Table of Contents

RiskVision Help 11
RiskVision Compliance Manager Guide 11
About Compliance Manager 11
About Compliance Manager 11
Other RiskVision Applications 12
Logging In 14
Logging in as a Delegate 15
Resetting Your Password 16
Resetting Your Password 16
Logging in With Your New Password 17
Compliance Dashboard 18
Compliance Dashboard Overview 18
Compliance Dashboard Charts & Data 19
Access & View the Compliance Dashboard 22
Getting Started 26
Getting Started 26
Navigating the RiskVision System 27
Navigating the RiskVision System 27
Using the Tree and Grid View 28
Using the Grid View 30
Using the Grid View 30
Sorting the Table 31
Refresh 32
Limiting the Number of Rows 33
Pagination 34
Changing the Grid Header Mode 35
Actions 36
Details 37
Customizing the Columns 38
Common Features 39
Common Features 39
Changing the Grid Header Mode 40
Advanced Searching 41
Documents 47
Controlling Object Visibility 50
Using Rich Text Editor 51
Actions 54
Batch Workflow Transitions 56
Visualizing Objects 59
Visualizing Objects 59
Moving the Layout 60
Bulk Exporting Evidence 61
Bulk Exporting Documents 62
Bulk Exporting Documents 62
Maximum Zip File Download Size 63
User Picker 64
About the Welcome Page 66
About Welcome Page 66

My Assessments 67
To-Do List 68
Message Center 69
My Findings 70
Using Quick Links 71
Understanding the Message Center 72
About Findings Page 73
About Findings Page 73
Creating a Finding 74
About Questionnaires Page 75
About Questionnaires Page 75
About Table Columns 76
About Action Options 77
About Submitted Questionnaires Page 78
About Tickets Page 79
About Tickets Page 79
Creating a New Ticket 80
Batch Edit Tickets 81
About Exception Requests Page 84
About Exception Requests Page 84
Request Global Exceptions 85
R6 Report License 88
Understanding Configurations 89
Understanding Configurations 89
Workflows 90
Workflows 90
Modifying Stage Settings 91
Modifying Stage Settings 91
Renaming The Stage 92
Configure Stage Transitions & Actions 93
Configuring Stakeholder Settings 97
Assigning Stakeholders 98
Allowing Stakeholders To Delegate 100
Allowing Stakeholders to Add Other Stakeholders 101
Send to Next Stage 102
Deleting Workflow Stages 103
Other Stage Options 106
Sending Escalations and Reminders to Stakeholders 108
Sending Escalations and Reminders to Stakeholders 108
Adding Escalations or Reminders 109
Editing Escalation and Reminder Settings 110
Deleting Escalations and Reminders 111
Sending Reminders and Escalations to Task-aware Stakeholders 112
Delegation & Delegation Revocation 113
Locking Answers in a Questionnaire 115
Forcing Stage Transition 116
Forcing Stage Transition 116
Determining Stage Transition Mode 117
Managing Workflow Escalation 118
Notifying Assessment Owner 119
Specifying Multiple Workflows 120

Specify Multiple Workflows 120
Defining More Complex Selection Conditions 121
Defining More Complex Selection Conditions 121
Specifying Sub-Conditions 122
Allowing Independent Stage Transitions 123
Allowing Independent Stage Transitions 123
Creating Workflows With Branching 124
Preferred Ownership 126
Preferred Ownership 126
About Preferred Ownership Options 127
Visualizing Workflows 128
Escalation 130
Escalation 130
Creating an Escalation Configuration 131
About Email Templates 132
About Email Templates 132
Default Email Templates 133
Configuring Email Templates 137
Configuring E-mail Templates 137
Updating Email Template 138
Adding a New Customized Email Template 139
Email Template Variables 140
Email Template Variables 140
Alert Email Templates 141
Assessment Email Templates 142
Analytics Email Templates 143
Control Email Templates 144
Exception Email Templates 145
Finding Email Templates 146
Incident Email Templates 147
Risk Email Templates 148
Ticket Email Templates 149
Vendor Email Templates 150
More Variables 151
Modifying a Variable Displaying Date 152
Adding Object Fields in Email Templates 153
Add Custom Attributes to Email Templates 154
Getting Familiar with Email Notifications 155
Filters 158
About Filter Data Types 158
About Comparison Operators 159
About Conjunctions 161
Adding a Filter 162
Modifying Filter Conditions 163
Removing a Filter 164
Grouping Filters 165
Grouping Filters 165
Creating a New Group 166
Deleting a Group 167
Understanding Complex Filters 168
User Variables 170

About Alert Rules 171
About Alert Rules 171
Creating an Alert Rule 172
Creating an Alert Rule 172
E-mail Templates 173
Modifying An Alert Rule 174
Deleting an Alert Rule 175
Configuring a Threshold Range for Calculating Vulnerability Scores 176
Understanding Questionnaire Presentation Options 178
Understanding Questionnaire Presentation Options 178
Setting up Questionnaire Presentation Options 179
Questionnaire Responder 180
Questions 181
Control Testing 182
Supporting Information 183
Actions 184
Evidence 185
Questionnaire Reviewer 186
About Ticket Management Preferences 187
Understanding, Setting up, and Managing Essential Objects 188
Entities 188
Entities 188
Entity Types 189
Create a New Entity 191
Creating a New Computer Type Entity 196
Setting the Name, Type, and Owner for an Entity 202
About Discovered Entities 203
Displaying Entity Details 204
Display Entity Details 204
Entity Details Tabs 206
About Ownership Types 208
About Ownership Types 208
Adding A New Ownership Type 209
Deleting an Ownership Type 210
Changing the Setting of an Ownership Type 211
Configuring Owners 212
Configuring Entity Compliance and Criticality Ranges 214
Setting the Criticality 216
About Entity Relationships 218
About Entity Relationships 218
Understanding Relationship Types 219
Understanding Relationship Types 219
Predefined Relationship Type 220
Defining Entity Relationships 221
Creating and Deleting Relationship Types 224
Importing Relationships 225
Propagation Overview 226
Propagation Overview 226
About Propagation Settings 227
Visualizing Relationships 229
Visualizing Relationships 229

Relationship Report 230
Relationship Explorer 231
Assigning Vulnerabilities 232
Operating Systems 235
Applications 237
Ports 239
Performing Entity Actions 240
Performing Entity Actions 240
Contextual Reports of Entities 241
Entity Attribute Screens 244
Using Entity Collections 247
About Entity Collections 247
Understanding Entity Collection Details 255
About Dynamic Groups 256
About Dynamic Groups 256
Default Dynamic Groups 257
Configuring the Dynamic Grouping 258
Configuring the Dynamic Grouping 258
Grouping Applications 259
Grouping Entities By Attributes 260
Grouping Computer And Network Devices 264
Configuring Dynamic Group Folders 267
Configuring Dynamic Group Folders 267
Setting the Name and Description 272
Setting Folder and Grouping Preferences 273
Understanding Organizational Hierarchy 274
Understanding Organizational Hierarchy 274
Organization Hierarchy Actions 275
Organization Hierarchy Actions 275
Enabling the Organization Hierarchy Selection 276
Defining a New Organization 277
Entity Management 278
About the Content Folders 279
About the Content Folders 279
Default Organization Content Folders 280
Content Actions Overview 281
About Controls 283
About Controls 283
About Controls and Questionnaires 286
About Controls and Questionnaires 286
Understanding Controls and Questionnaires 287
Control Objectives 288
Configuring Controls 290
Configuring Subcontrols 291
Create a New Control 292
Creating Questionnaires 294
Creating New Questions 302
Selecting Domain-Specific Controls 308
Configurable Control Testing 311
Configuring Default Manual Control Choices 312
Migrating Draft Content into Versioned Content 313

Grouping Content 316
Create a New Group 316
Adding a Tag to a Group 317
Creating a New Content Pack 318
Automated Controls 322
Automated Controls 322
Create an Automated Control 323
Setting the Input Parameters 324
Setting the General Information 325
Selecting a Check Template 326
Selecting the Check Parameters 327
About the Common Control Framework 328
About the Common Control Framework 328
Common Control Framework 329
Importing Data 335
Importing Data 335
Working with Excel 336
Working With Excel 336
Multi-Valued Attributes 338
Provided Excel Spreadsheets 339
Overview of Attributes 340
Overview of Attributes 340
Attribute Name 341
Attribute Types 342
Cardinality 343
Import Content from Excel 344
Understanding Attributes in RiskVision Templates 350
Entity Import Template 350
User Import Template 352
Finding Import Template 354
Control Import Template 356
Risk Assessment Import Template 358
Entity Relationship Import Template 359
Alternatives to Excel 360
Importing Entity Collections 361
About Target Selection Options 362
Creating a Control Target Profile 362
Creating a Control Target Profile 362
Deleting Profile Control Target Profiles 363
About Target Selection Options 364
Configuring Target Selection Options 366
Configuring Profile Variables 368
Risks 370
Creating a New Risk 370
Creating a New Risk 370
Associating Threats, Vulnerabilities And Controls With Risks 371
Understanding Risk Exposure 373
Creating a New Threat 375
Deleting a Risk 376
Exporting Risks 377
Importing Risks 378

Understanding Operational Vulnerabilities 379
Understanding Risk Catalogs 380
Risk Score Calculation Methods 381
Using the Document Repository 383
Using the Document Repository 383
Document Repository Structure 384
Document Repository Ownership 386
Modifying Ownership 387
Document Repository Actions 388
Document Repository Actions 388
Move 389
Delete 390
Data Feeds 391
About Data Feeds 391
Importing Data Feeds 392
Deleting Data Feeds 397
Setting up, Launching and Managing Assessments 398
Programs 398
Assessing Compliance 398
Understanding Programs 399
About the Program Wizard 400
New Program Wizard Buttons 401
Checklist for Creating a Program 402
Naming the Program and Assigning Owners 403
About Questionnaire Types 405
Selecting Controls and Questionnaires 406
Selecting Controls and Questionnaires 406
Assigning Content 407
Selecting Workflow 409
Understanding Recurrence 410
Understanding Recurrence 410
Reassessing All Entities on the Same Schedule 411
Reassessing All Entities On the Same Schedule 411
Reassessing Entities Based on Criticality 412
Reassessing Entities Based On Criticality 412
Security Requirement 413
Selecting the Questionnaire Option For Reassessment 414
Setting Additional Program Options 415
Setting Control Response Options 417
Sending Notifications to Stakeholders 420
Sending Notifications to Stakeholders 420
Checklist For Notifying Stakeholders Only When There Are Questionnaires 421
Notifications Behavior 422
Assigning Risk Assessment Questionnaires 423
Assessments 424
Checklist for Creating an Assessment 424
Controlling Dynamic Group Visibility in Assessment Creation 425
Controlling the Visibility of Propagation Tab 427
Creating an Entity Assessment 428
Importing Answers to Questionnaires 430

Creating an Entity Collection Assessment 432
Choosing Entities 434
Launching the Assessment 435
Removing an Entity Collection Assessment 436
Removing an Entity Collection Assessment 436
Managing Entity Collections 437
Assessment Actions Overview 438
Restart Assessments 439
Participating in Assessments 445
About the Questionnaire Answering Interface 445
Reviewing Assessment Results 448
Viewing Program Details 448
View Program Details 448
Synchronizing the Changes in a Program 449
Synchronizing the Changes in a Program 449
Synchronizing the Workflow 450
Updating Content 451
Viewing Content Version 452
Viewing Assessments Based on Group Definitions 453
Viewing Assessment Details 454
Viewing Assessment Details 454
Adjusting Assessment Due Dates 455
Monitoring Assessment Progress 456
Understanding Assessment Propagation Details 457
Understanding Assessment Propagation Details 457
Overriding Inherited Controls 458
Exception Requests 460
Create an Exception Request - Assessment 460
Exception Request Basic Details 462
Exception Request Attachments 463
Default Exception Workflow 464
Edit an Exception 465
Transition Exception Requests 466
Control Results 467
Control Results Grid 467
Control/Test Details 468
Findings 471
About Findings 471
Creating a Finding - Assessment 472
Deleting a Finding 474
Importing Findings 475
Finding Analysis 479
Responses 480
Create a Response 480
Update a Response 481
Delete a Response 482
Tickets 483
Tickets 483
Understanding Ticket Flow 484
Creating a Ticket - Assessment 486
Link a Ticket to an Entity 487

Starting and Transitioning the Ticket Process 488
Changing the Default Ticket Workflow 489
Assigning a Ticket to Another User 490
Delegating an Object to Another User 491
Setting General Ticket Information 493
Deleting a Ticket 495
Automatic Ticket Archiving 496
Compensating Controls 497
About Compliance and Simple Risk Scoring 498
About Compliance and Simple Risk Scoring 498
Assessment, Control, and Subcontrol Compliance Scores 499
Risk Scoring 500
Security Risk Score 501
Configuring Compliance Score Settings 502
Configuring Subcontrol Scoring 502
Configuring Control Scoring 503

About Compliance Manager

Compliance Manager enables an organization to effectively manage and measure compliance programs across multiple regulations, standards, and frameworks. Compliance Manager automates the compliance process through general computer controls (GCC) and questionnaires, the evidences and control results can be automatically collected via connectors or questionnaire results from business users. Compliance Manager enables data classification, ownership configuration, compliance assessment, mitigation, and reporting. It supports popular frameworks, standards, and regulations such as ISO 27002, CIS, HIPAA and PCI, and many others. Compliance Manager improves process efficiency and integrity as well as data quality and reliability.

Other RiskVision Applications

Other RiskVision applications are listed in the table below:

ICON	APPLICATION	DESCRIPTION
	Enterprise Risk Manager	Enterprise Risk Manager is a comprehensive risk lifecycle management solution. Organizations can use this application to identify, assess, and mitigate risks using an appropriate risk treatment plan. Its flexible risk model supports both qualitative and quantitative methodologies, including the calculation of inherent risk, current risk, and residual risk within the context of mitigating controls. It features rich reports and dashboards, as well as easy to use risk assessment tools and will help your orgnization understand and monitor its enterprise risk posture. Enterprise Risk Manager includes out-of-the-box support for popular risk methodologies, such as COSO, AZ/NZS 4360 and ISO.
	Vendor Risk Manager	Vendor Risk Manager helps organizations audit and manage third-party risks, as mandated by regulations and standards, such as ISO 27001, PCI, and FISMA. This application classifies, assesses, and reports on third-party risk, based on the standard control framework from shared assessment programs, or an organization's custom control framework. Vendor Risk Manager provides a portal where vendors participate in assessments and the results are retrieved by an organization's risk analysts. Vendors are classified automatically into appropriate tiers and applicable controls are applied based on the vendor tier. Powerful delegated administration and automation features allow Vendor Risk Manager to scale to large numbers of vendors.
	Threat and Vulnerability Manager	Threat and Vulnerability Manager will help you consolidate your threat and vulnerability programs onto a single platform. It integrates with vulnerability and early warning data feeds from iDefense and National Vulnerability, and correlates these feeds with vulnerability scanner results to eliminate false positives and report incidents. Inferred scans are performed by correlating the vulnerability data feeds to a company's RiskVision asset database, mitigating risks for assets not reachable by vulnerability scanners. Once detected, vulnerabilities are assessed and remediated using the system's workflow for true closed-loop vulnerability management.
	Policy Manager	Policy Manager enables the management of enterprise policies on a single centralized platform. Organizations can enforce policy and process standards across different locations, departments, and programs. It supports simultaneous policy editing across multiple stakeholders using a rich WYSIWYG user interface. An organization can automate processes for policy authoring, reviewing and approval. Policy templates help enforce consistent formatting and structure. It has a highly configurable workflow enabling an organization to enforce change control and maintain accountability and it supports policy awareness campaigns with policy distribution, attestation, and comprehension testing tools.
	Incident Manager	Incident Manager helps organizations collect, classify, and manage multiple IT and non-IT incidents. It is a single collection point for all incidents that are manually and automatically reported. It imports incidents reported from most monitoring systems and scanners, as well as Security Incident Management (SIM) solutions. All incidents, including business, operational, and environmental, can be reported using the incident-reporting portal. Incidents are assessed based on configurable workflows and automatically created and classified based on rules that are tracked throughout the incident's lifecycle. Incidents are tied to controls, policies, and risk to provide closed-loop feedback for policy and control assessment and risk monitoring. Incidents are rated based on their criticality

		so that organizations can respond based on the impact to the business.

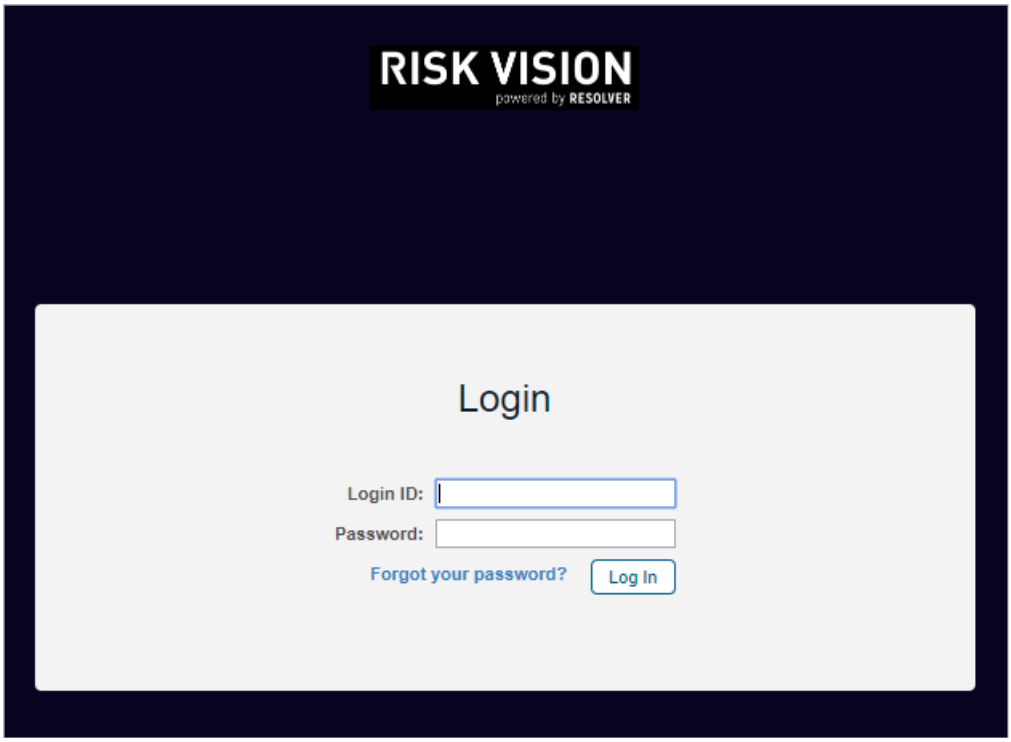
Logging In

Your login account may be identical to your Active Directory credentials, or a new ID may have been created for you within the RiskVision Enterprise Risk Manager. Contact your Administrator for your credential information.

For more information on default accounts, please refer to the Installation & Configuration Guide or contact your Resolver Customer Support representative.

To access the application using a web browser:

1. Open a browser and enter the RiskVision URL.



The RiskVision login screen.

2. For example, https://RISKVISION, where RISKVISION is the hostname or IP address for the Resolver RiskVision Server.

   Depending on your browser, you may see a message like "Web site certified by an unknown authority." To avoid seeing these types of messages in future sessions, accept the certificate permanently.

3. Enter the user name or e-mail and password that is specific to your domain, select a domain if the **Domain** drop-down list is available, and then click **Log In**.

   The first time you log in, the *License Agreement* is displayed.

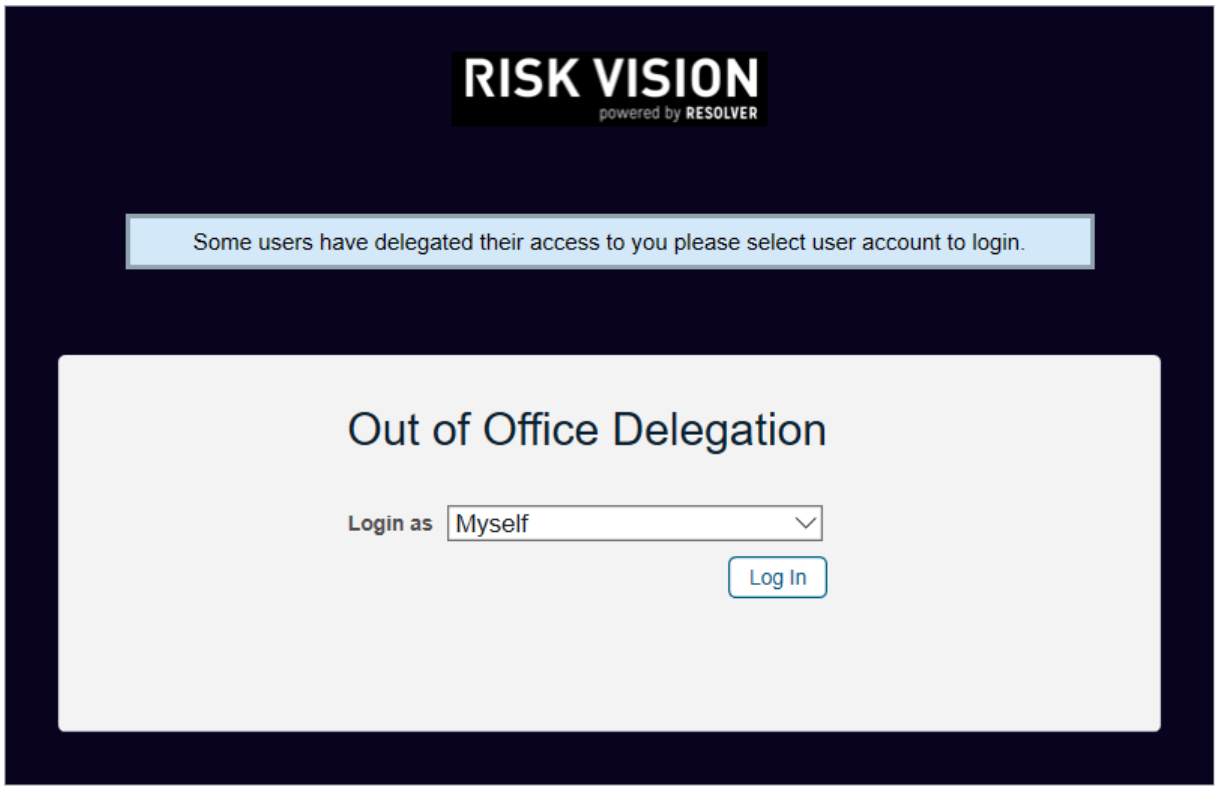
4. Click **Accept** to continue. The **Welcome** page is displayed.

Logging in as a Delegate

You can log into the account of another user if that user or a RiskVision administrator nominates you to access the delegation. To learn how to delegate your RiskVision user account, see Delegating Your RiskVision User Account.

To access a delegated user account:

1. Open a browser and enter the RiskVision server URL.
2. Enter your **Login ID** and **Password**, then click **Log In**.
3. Click **Login as** and select a user account other than **Myself**, then click **Log In**. **Myself** will log you in to your user account.



The Out of Office Delegation screen.

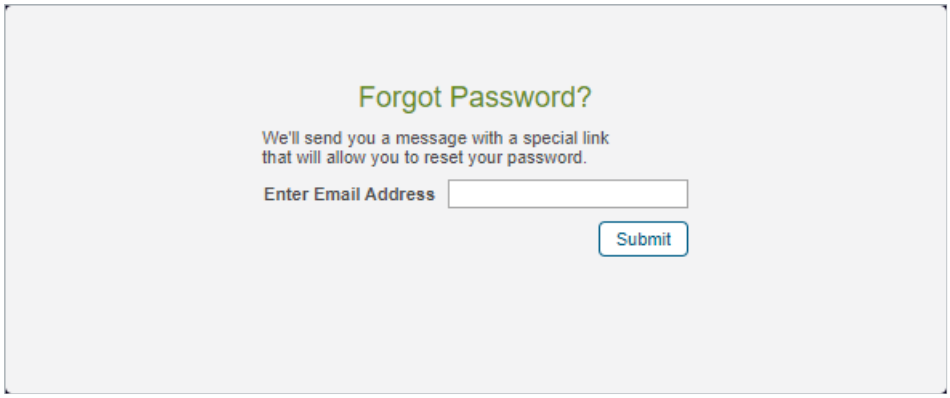
When you are logged into a delegated user account, you can perform any task permitted by that user's account permissions on behalf of that user. When the delegated user logs into RiskVision, the **Current User** will appear as **Logged in as: delegated by [username]**.

Resetting Your Password

If you've forgotten your password, you can set a new one right away with no assistance required from your RiskVision administrator.

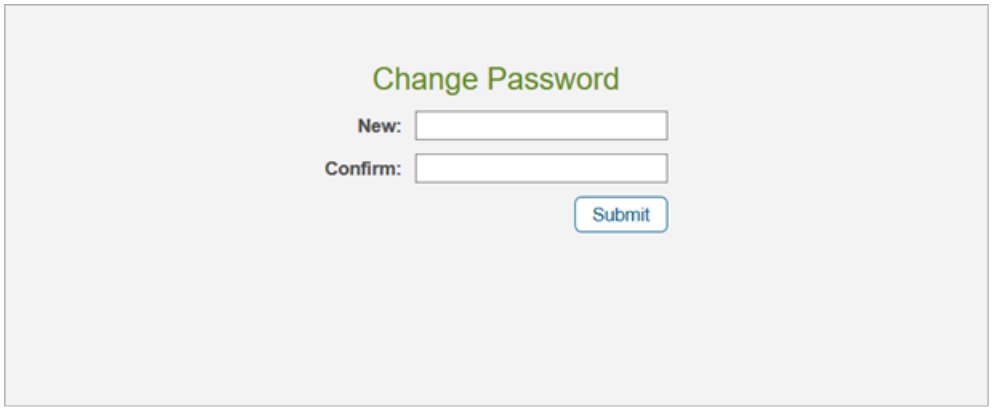
To reset your password:

1. Open the login page.
2. Click the **Forgot your Password** link.
3. Enter the email address that has been registered in the RiskVision Server in the **Enter Email Address** field.



The Forgot Password page.

4. Click **Submit**. An email containing the link to reset your password will be sent to your mail box.
5. Click the link in the email to open the **Change Password** page.



The Change Password page.

6. Enter a new password in the **New** and **Confirm** fields.
7. Click **Submit**.

To log on with your new password, see Logging in With Your New Password.

Logging in With Your New Password

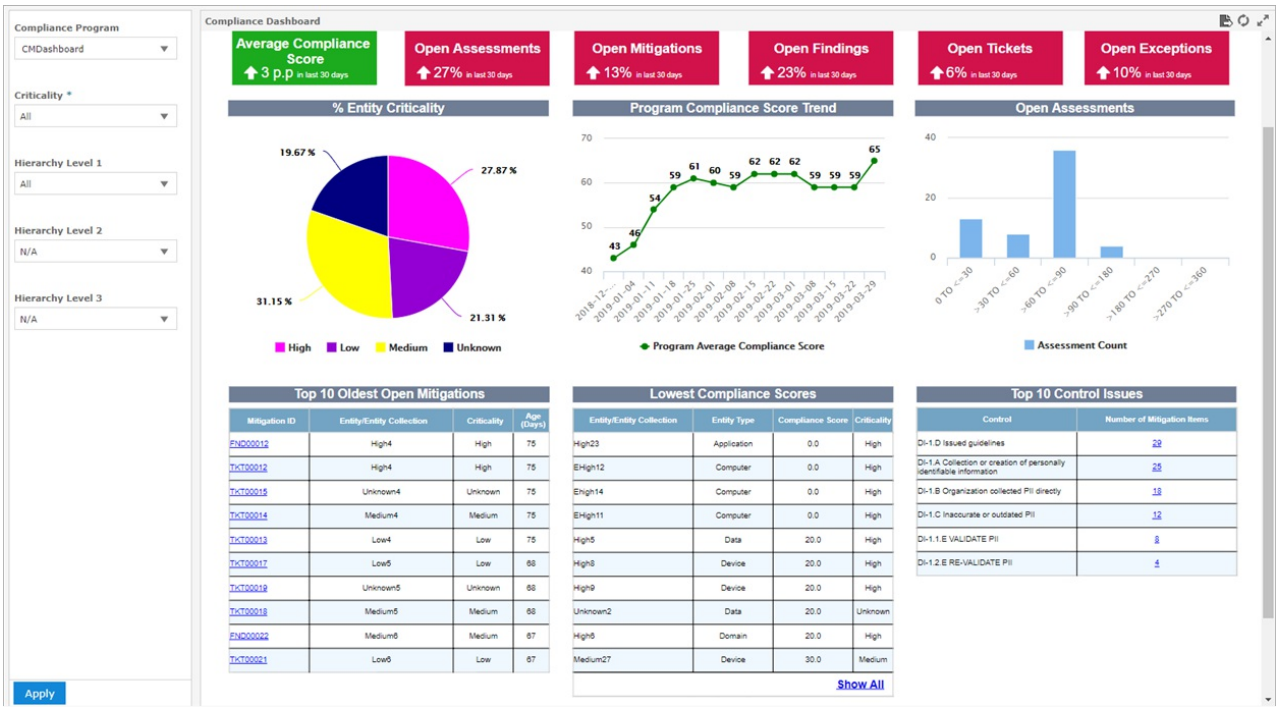
After you reset your password using the **Forgot Your Password** link on the login page, you can now log in with your new password. Make sure that you close all your browser windows and then launch the RiskVision application in a new browser window.

Compliance Dashboard Overview

The **Compliance Dashboard** was designed to allow executives, information security officers, and security and compliance teams to easily monitor, track, and review compliance and remediation statuses and scorecards for relevant business units or groups within a program.

Charts include average, lowest, and trending compliance scores, the number of open assessments and mitigations, and more. For details on the charts and data displayed on this dashboard, see the Compliance Dashboard Charts & Data article. For information on viewing the dashboard, see the Access & View the Compliance Dashboard article.

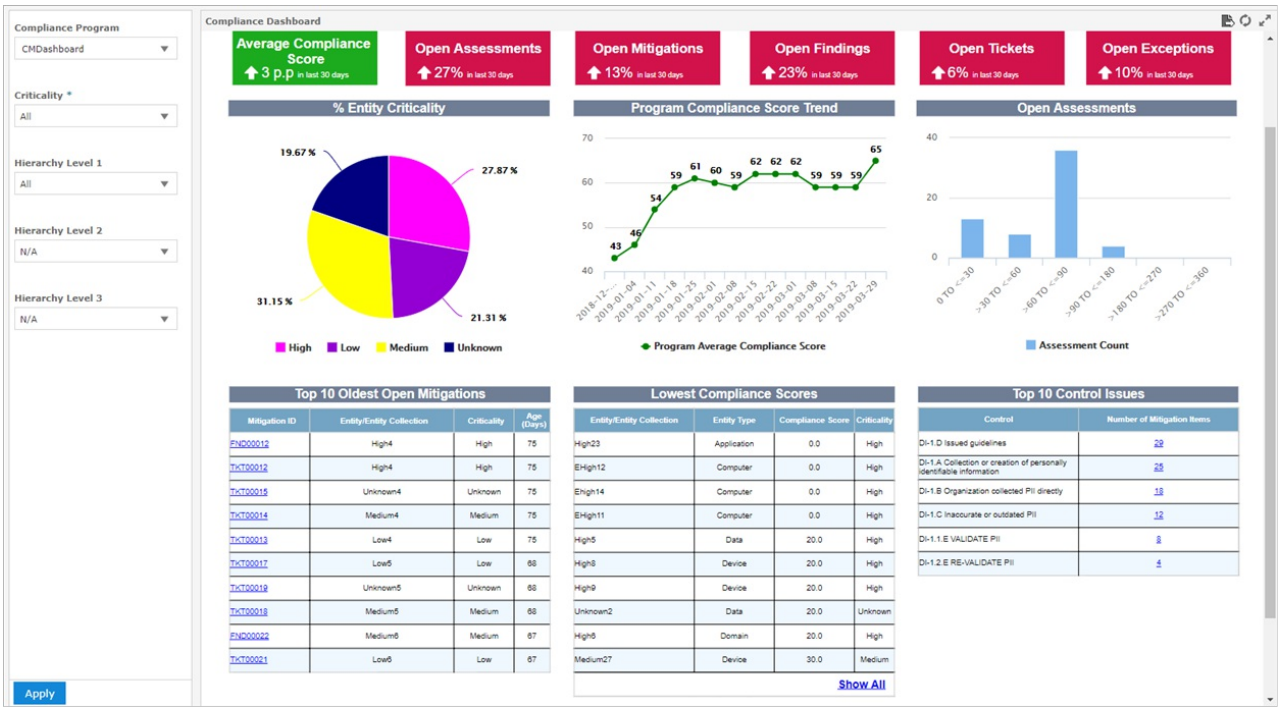
> The **Compliance Dashboard** data is updated via the **Report Summary Builder** (which must be run first) and **Trending Data Collection for CM dashboards** scheduled jobs. See Manage Jobs for more information.



The Compliance Dashboard.

Compliance Dashboard Charts & Data

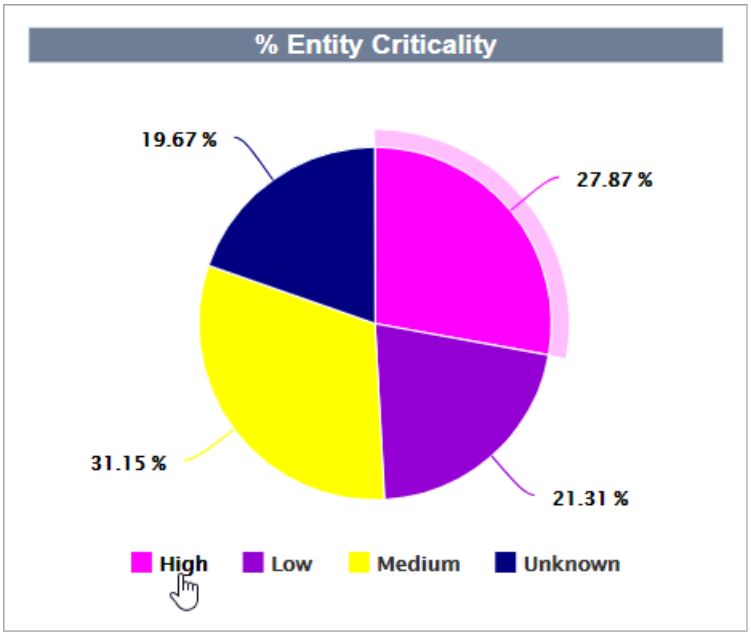
This article provides details on the charts displayed on the **Compliance Dashboard**. For information on accessing it, see the Access & View the Compliance Dashboard article.



The Compliance Dashboard.

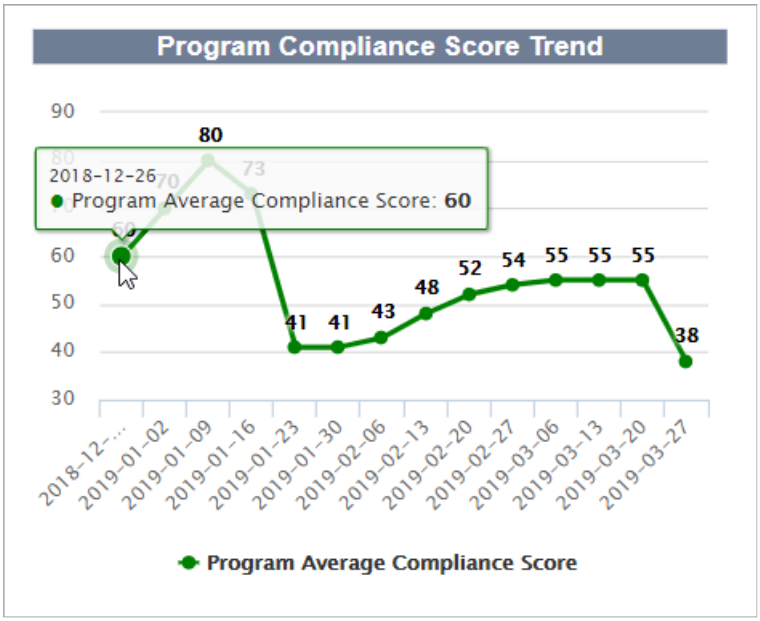
This dashboard displays the following data for the currently selected program:

- **Average Compliance Score:** Displays the current score and comparison data from the last 30 days. If the score has increased in the last 30 days, it'll be displayed with an up arrow and a green background. If the score has decreased in the last 30 days, it'll be displayed with a down arrow and a red background.
- **Open Assessments:** Displays the current number of open assessments. If the number of assessments has decreased in the last 30 days, it'll be displayed with a down arrow and a green background. If that number has increased, it'll be displayed with an up arrow and a red background.
- **Open Mitigations:** Displays the current number of assessments with open mitigations, which consist of tickets and findings. If the number of mitigations has decreased in the last 30 days, it'll be displayed with a down arrow and a green background. If that number has increased, it'll be displayed with an up arrow and a red background.
- **Open Findings/Open Tickets/Open Exceptions:** Displays the current number of open findings, tickets, or exceptions. If the number of these objects have decreased in the last 30 days, each will be displayed with a down arrow and a green background. If that number has increased, each will be displayed with an up arrow and a read background.
- **% Entity Criticality:** A pie chart that represents, in percentages, the criticality assigned to the entities in the program. Clicking a portion of the chart will open a new tab with an **Entity Compliance Detail Report** for the selected criticality level. Clicking a criticality level below the pie chart (e.g. High, Low, Medium, or Unknown), will hide that data from the chart.



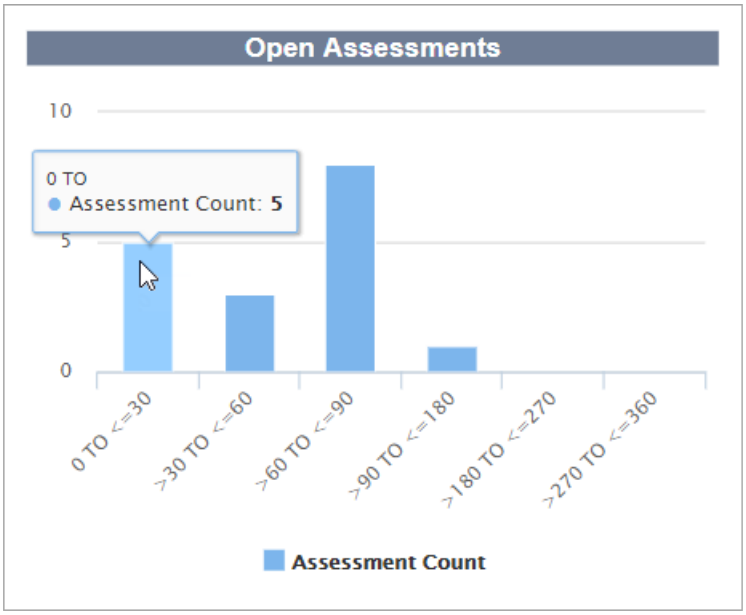
The % Entity Criticality pie chart. Clicking a criticality level will hide it from the chart, while clicking a section in the chart will open an Entity Compliance Detail report in a new tab.

- **Program Compliance Score Trend:** Displays the average compliance score for the selected program. Hovering your cursor over a point in this chart will display the score and its date. Clicking **Program Average Compliance Score** below the chart will hide its data.



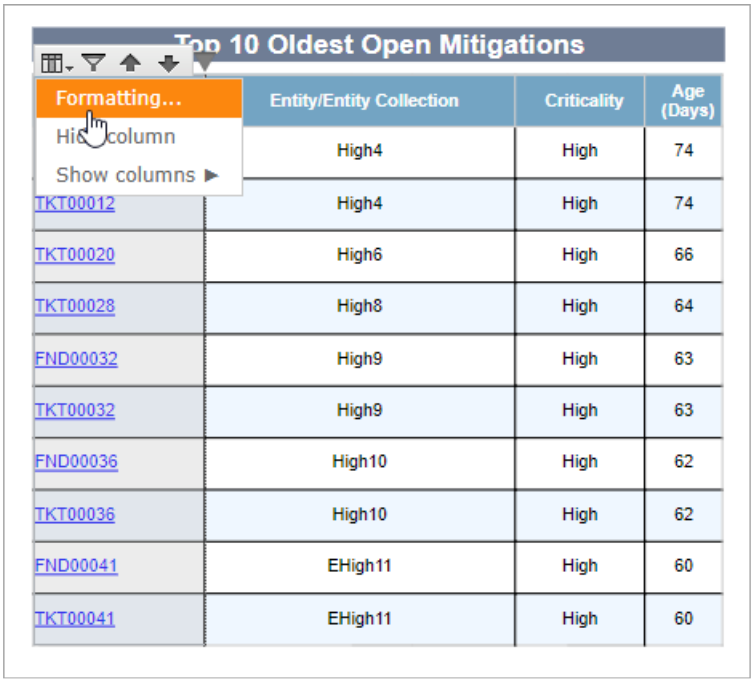
The Program Average Compliance Score chart.

- **Open Assessments:** Displays the number of open assessments grouped days open (e.g. **> 30 to <=60** [more than 30 but less than 60]). Hovering your cursor over a bar in this chart will display the date range and the number of assessments. Clicking **Assessment Count** below the chart will hide its data.



The Open Assessments chart.

- **Top 10 Oldest Mitigations:** Displays a list of ten oldest tickets and findings, along with their mitigation IDs, entity or entity collection, criticality, and age in days. Clicking a mitigation ID will open the ticket or finding in a new tab. Clicking a column will display the chart options, including table formatting, show/hide columns, filters, sorting, and resizing.



The Top 10 Oldest Mitigations chart. Clicking a column will display the chart options.

- **Lowest Compliance Scores:** Displays the entities or entity collections with the lowest compliance scores, along with their entity types, compliance score, and criticality. Clicking a column will display the chart options, including table formatting, show/hide columns, filters, sorting, and resizing. Clicking **Show All** will open the **Assessment Compliance Score Details** report in a new tab.
- **Top 10 Control Issues:** Displays the controls with the highest number of total open and closed mitigation items linked to open and closed (but not archived) assessments. Clicking a column will display the chart options, including table formatting, show/hide columns, filters, sorting, and resizing. Clicking a number in the **Number of Mitigation Items** column will open a **Control Mitigation Details** report in a new tab.

Access & View the Compliance Dashboard

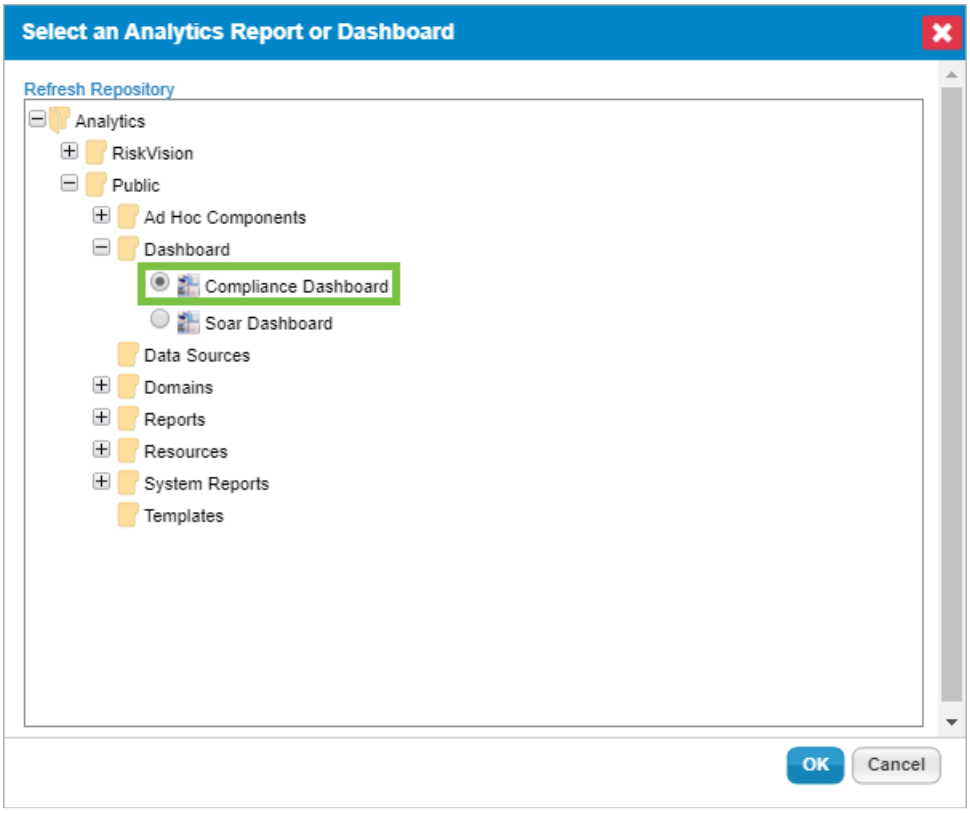
For information on the data displayed on the dashboard, see the Compliance Dashboard Charts & Data article.

The **Compliance Dashboard** data is updated via the **Report Summary Builder** (which must be run first) and **Trending Data Collection for CM dashboards** scheduled jobs. See Manage Jobs for more information.

This article provides information for individual users and users within a role to access the dashboard. Should your organization wish to select the **Compliance Dashboard** as the default dashboard/home page for every user accessing the application, contact Resolver Support.

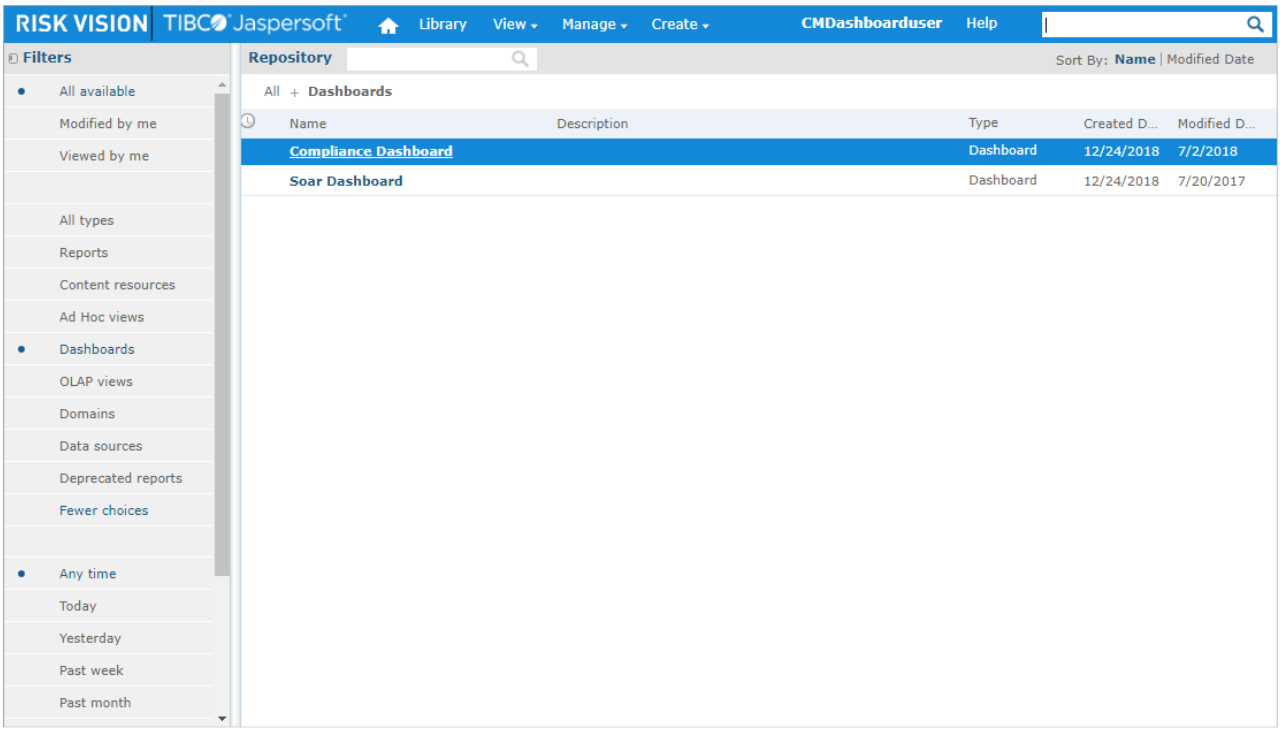
Accessing the Dashboard

The dashboard can be added to your **Welcome** page by selecting it as your default dashboard in the **User Settings** or if an administrator selected it as the default for your role. See the Select a Default Dashboard article (for end-users) or step 6 of the Create a New Role article (for administrators) for more information. For both of these options, ensure the **Compliance Dashboard** option in the **Analytics > Public > Dashboard** repository is selected.



The Compliance Dashboard in the repository when selecting a default dashboard or home page.

The dashboard can also be accessed through Jaspersoft by hovering your cursor over **Analytics** at the top of the page, then clicking **Analytics and Reporting > View list** in the **Dashboards** section **> Compliance Dashboard**.

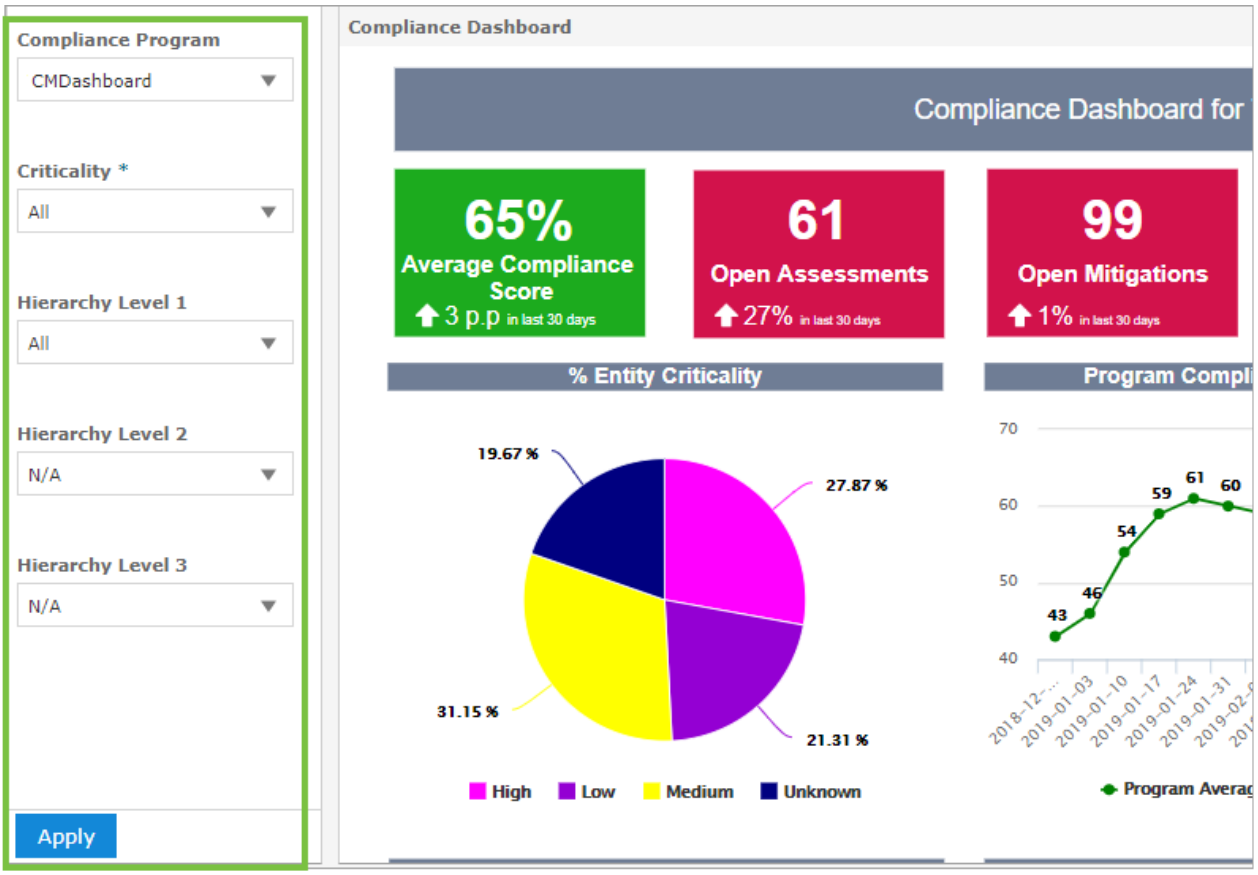


The Compliance Dashboard in the Jaspersoft repository.

Compliance Dashboard Filters

When viewing the dashboard, you can apply filters to refine the data. Filters include **Compliance Program**, **Criticality**, and **Hierarchy Levels 1** through **3**, which provide a business perspective to the dashboard by allowing users to see compliance for the entire organization, a division, or a department.

Clicking **Apply** will apply the filters and save the selections for the currently logged in user, preventing the need to reapply the filters each time the dashboard is viewed.



The Compliance Dashboard filters.

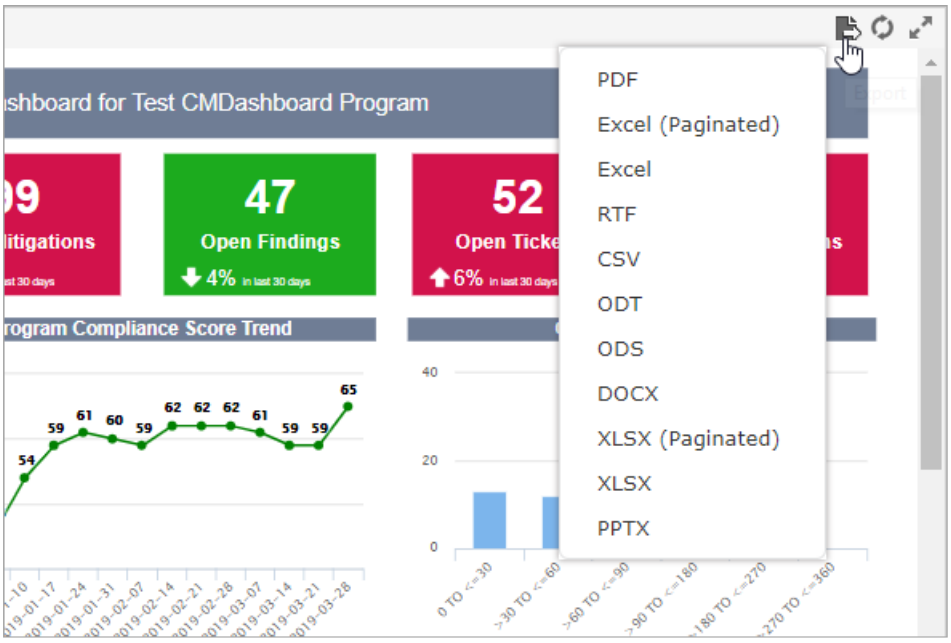
Export, Refresh & Maximize

The **Export**, **Refresh**, and **Maximize** options are accessible at the top-right of the dashboard.

Export file type options include:

- PDF
- Excel (Paginated)
- Excel
- RTF
- CSV
- ODT
- ODS
- DOCX
- XLSX (Paginated)
- XLSX

To export the dashboard, hover your cursor over the **Export** icon, then click a file option to initiate the download.



The Export file type options.

To display the latest data, click the **Refresh** icon. To hide the filters on the left of the page, click the icon.

Getting Started

All logged in users of any RiskVision application are directed to the **Welcome** page, on the **Home** menu. The **Welcome** page contains active tasks and messages which require your attention. The tasks are divided into categories and displayed as sections with links. If you are not a stakeholder in any task, you will not see any links in the sections. By default, each section will show up to five items you might own more tasks. By clicking the **"Go to..."** link below the section, you will be navigated to the respective page of that section, on the **Home** menu, to view the exhaustive list of items. Besides accessing sections, the **Welcome** page also provides **Quicklinks** to pages so that you can be directed to the desired area instead of having to manually navigate trough the RiskVision applications.

Here's the complete list of pages on the **Home** menu, which appear based on your role and the RiskVision application:

- Welcome
- Message Center
- Findings
- Questionnaire
- Submitted Questionnaires
- Tickets
- Exception Requests

The pages as discussed above will help you to view, edit, or update the list of do able items, and these operations can also be accomplished from other points in RiskVision applications. Typically, the stakeholders who will not need their extreme participation in ITGRC projects are provisioned to access the pages on the Home menu. The user interface of each page can be customized to fit the needs of your business goal.

Before you move on to understand the purpose of these pages, RiskVision recommends to familiarizing yourself with the navigation, tree and grid, actions, user settings, and the advance search. For more information, see Navigating in RiskVision.

Navigating the RiskVision System

RiskVision pages use a consistent interface, shown below, to navigate easily wherever you are in the application.

The navigation ribbon in Compliance Manager.

Selecting a different application changes the menus. The specific menus and submenu choices available depends on the current application and the permissions assigned to your user role.

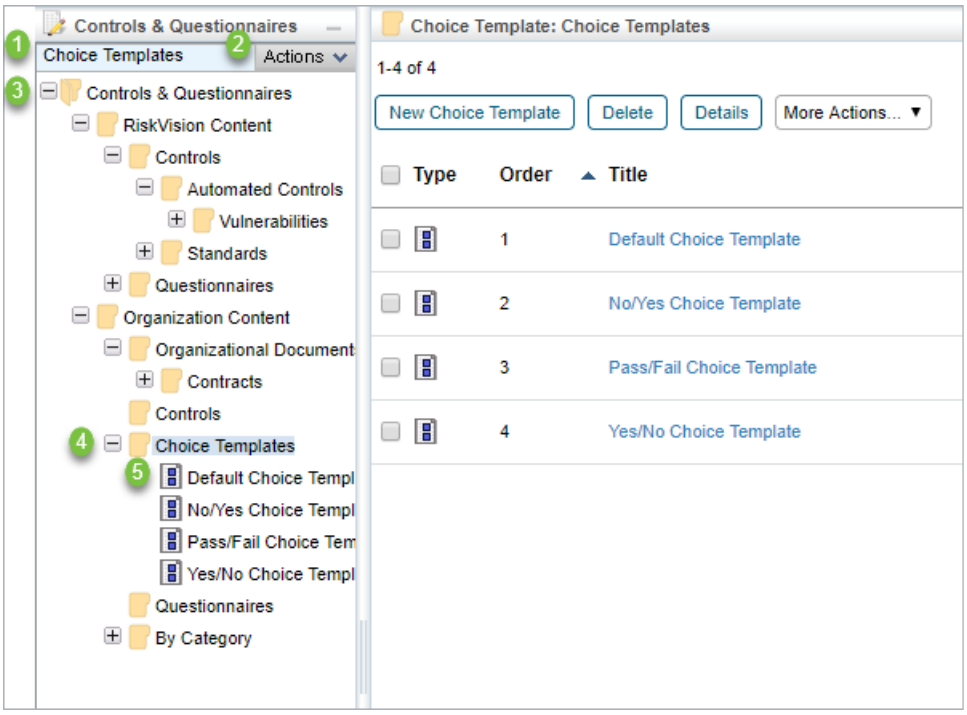
Moving the mouse hover a menu, such as "Home," displays a pull-down submenu of items. You can quickly view a snapshot of the available pages by moving the mouse over each menu.

Clicking the menu selects it and displays as many submenu items as possible under the menus. If your browser window is narrow, there may be more submenu items under the menu than what appears.

Using the Tree and Grid View

Many pages in the RiskVision solution display a hierarchical tree on the left and a tabular grid on the right side of the screen. The tree and grid function in the familiar way that files and folders are shown in Operating Systems like Microsoft Windows.

For more information about the grid side of the tree and grid view, see Using the Grid View.



The Tree and Grid view.

1. Selected node
2. Actions pulldown
3. Root node
4. Folder
5. Object

To adjust the width of the tree view, click the splitter, the vertical bar between the panes, and drag it to right or left. To hide the entire tree view, move the splitter all the way to the left, or click the minimize button at the top of the tree pane. To view the tree again after it has been minimized, click the splitter—parked on the left edge of the window—and drag it to the right.

Clicking on an item in the tree pane will display its name in the **Selected Node** window. Clicking the **Actions** will bring up a list of actions that can be performed on the selected item, such as refreshing, copying, or deleting it. The contents of the tree pane vary considerably. Some pages use the tree to differentiate read-only content from read-write Organization content, for example. Some trees group the objects you own--My Dashboards, for instance--separately from shared objects and archived objects.

Certain trees include objects. When you click on an object in the tree, the detail pane for that object replaces the grid pane. In other cases, the tree only includes folders. Clicking on a folder or a dynamic group usually displays the objects it contains in the grid pane.

Selecting different nodes of the tree have different effects:

Target	Description
Root / Initial view	May display a grid view showing all objects, or may display a landing page (such as Analytics> Dashboards). The initial view is usually similar to selecting the root of the tree. Selecting the root of the Entities tree is special: it displays a details view for all entities, summarizing the set and providing a convenient place for manually creating an Entity.
Folder	The contents of the folder appear in the grid.

Target	Description
Object	The details view for the selected object replaces the grid view.

Certain root or initial view pages include action buttons, such as the **Import Content (XML)** button on the **Content** > **Controls and Questionnaires** page the **Import Policies (XML)** button on the **Content**> **Policies** page.

Using the Grid View

The grid view is used throughout the RiskVision solution to display a table of objects (users, programs, connectors, and so on) and their attributes. Each row in the table represents an object, and the columns reflect some of the object's attributes. In some cases, you can customize the columns and how they display particular attributes.

Sorting the Table

To sort the table by any visible attribute, click that attribute's column heading. To reverse the sort (ascending order instead of descending), click the column heading again. To make a hidden attribute visible, see Customizing the Columns in the following sections.

Refresh

The table represents a snapshot of the underlying data at the time it was first displayed. Some data, such as Charts in Progress, are more dynamic, but all objects can change over time. To update the display with the latest data, click the **Refresh** button.

Limiting the Number of Rows

The grid view may show all objects of a particular kind, such as Ownership Types, or it may show only the contents of the selected dynamic group.

Filtering the grid.

Enable Focus

To focus on objects of interest:

1. Click the **Filter by** dropdown and select an object attribute.
2. Enter a value. Press **Enter**. For text attributes, the value is a case-insensitive, "begins with" query.

To remove the filter and show all rows, select **Show all** from the filter pull down list, or clear the value and hit **Enter**.

Enable Grids

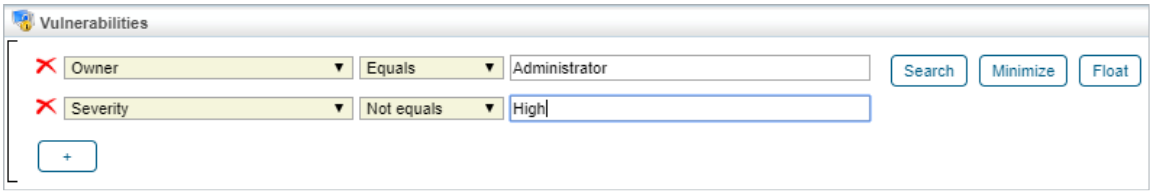
Certain grids, such as Entities, Vendors, and all grids on the Vulnerabilities menu, contain the Advanced Filter to help you locate the objects using one or more advanced search conditions.

To enable the advance search feature in a grid:

1. Select **Advanced Filter** in the **Filter by** dropdown list or click the icon next to the **Filter by** drop-down list. You can also click **Float** to perform a search in the **Search** dialog.
2. **Optional**: Click **+** to add more search conditions. You can add a maximum of six conditions. Depending on the field selected, comparison operators and search input varies, and appears in their respective dropdown lists. The search value must be either entered in the text box or selected from the dropdown list.

   Example: To search computer entities owned by a user named Administrator:

   1. Select **Primary Owner** in the first dropdown list.
   2. Select **Equals** in the second drop-down list.
   3. Select **Administrator** in the third drop-down list.
   4. Select '**Type**' '**Equals**' '**Computer**,' and click **Search**.
   5. **Optional**: If you're performing a search in the Search dialog, click **OK** after the selecting the search conditions. The results matching the search conditions are displayed in the grid.



The Advanced Search filter.

   6. Click **Minimize**.
   7. **Optional**: To re-expand the **Advanced Filter**, click .

Pagination

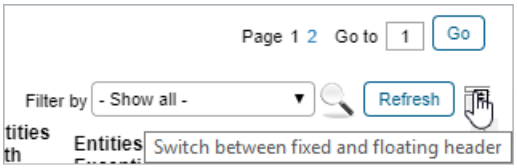
Large numbers of rows are shown in pages at a time. When the grid view is not displaying all rows of a table, the following pagination controls appear.

RiskVision's pagination controls.

The controls on the left adjust how many rows are displayed per page (between a minimum of 5 and a maximum of 500). The controls on the right allow for page navigation. The currently selected page is displayed in the text box. To navigate to another page, click the desired page number or the right and left arrow keys (for more than 5 pages). If the desired page number is not visible, type the number into the text box and click **Go** to navigate to that page.

Changing the Grid Header Mode

A RiskVision object grid can have various numbers of rows on any page. When you scroll down to view objects in the grid, the grid header row moves with the other rows, which may make it difficult to interpret the data correctly.



The Grid Header Mode icon.

Click the icon next to the **Refresh** button to prevent the header row from moving.

Actions

Grid views often have buttons such as **New**, **Details**, or **Delete**. The appearance of these buttons depends on the context, the current application, and your user privileges. If you are allowed to create objects here, for example, the **New** button will be shown. To delete one or more objects, check the box to select the rows to remove and click **Delete**.

The **More Actions...** pull down list offers other, context-specific actions, such as import, export, copy to, or move to. Actions such as **Import** are general, but most actions require selecting one or more rows. In the **Home > Questionnaires** view, each row has an **Actions** pull-down.

Details

Displaying and updating the attributes of a single object requires showing the object's details which can be accomplished in several ways. From the grid view, check the box to select the desired object and then click **Details**. In some cases, the **Details** action is found in the **More Actions...** pull-down list. In many grid views, the object's name or title is a link that serves as a shortcut to the details.

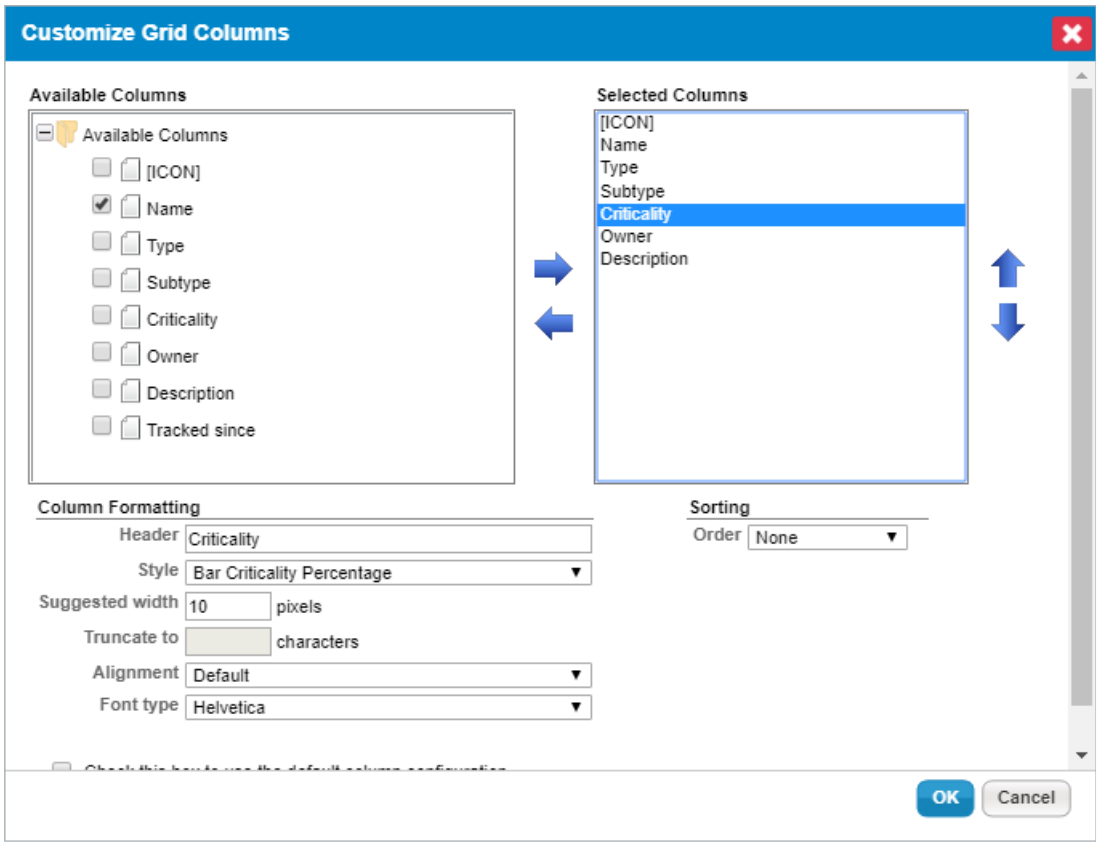
Some kinds of objects do not have details. Some, such as the **Home** > **Questionnaires** view, have links to more than one kind of object (in this case, entities and questionnaires). Details can be displayed in the lower half of the grid view in a popup window, or the details view can replace the entire grid view. Click **Back** to return to the grid view from the details view.

Customizing the Columns

In most grid views, you can specify exactly which attributes must be displayed as columns in a given grid view, and you can choose whether attributes must be shown graphically or as text or other options.

To customize the columns:

1. Open the **More Actions...** dropdown list.
2. Click **Customize**.



The Customize Grid Columns dialogue.

In the **Customize Grid Columns** dialogue, the object attributes that can be used as grid columns are listed in the **Available Columns** box. The current columns are listed in display order in the **Selected Columns** list.

3. **Optional**:
    a. Add a column to the **Selected Columns** list:
        i. Check the box next to a column in the **Available Columns** list.
        ii. Click the right arrow pointing from the **Available Columns** to the **Selected Columns** list.
    b. Remove a column from the **Selected Columns** list:
        i. Select a column in the **Selected Columns** list by clicking on it.
        ii. Click the left arrow that points from the **Selected Columns** back to the **Available Columns** list.
    c. Specify the format details of a column:
        i. Click a column name to select it in the **Selected Columns** list.
        ii. **Optional**: Edit the **Format > Header** field to change the column name.
        iii. **Optional**: Click the up or down arrow to change the order.

Customizing Grid Columns has no effect on the underlying data.

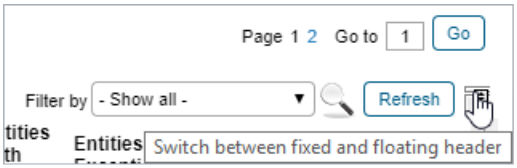
Common Features

A number of common features can be seen in many objects, throughout the RiskVision application. Here is a list of common features you must know before you begin to learn the features in RiskVision application:

- User Settings
- Delegation
- Advanced Searching
- Documents
- Applications
- Rich Text Editor
- Actions
- Visualization

Changing the Grid Header Mode

A RiskVision object grid can have various numbers of rows on any page. When you scroll down to view objects in the grid, the grid header row moves with the other rows, which may make it difficult to interpret the data correctly.



The Grid Header Mode icon.

Click the icon next to the **Refresh** button to prevent the header row from moving.

Advanced Searching

The search box can be used to search for simple terms as well as for more structured queries. This section describes the syntax for advanced queries.

An advanced query consists of terms and operators. Terms can be single words (such as "test" or "hello"), or a phrase enclosed in double quotes (such as "hello dolly"). Single terms (but not phrases) can include wildcards, * and ?, anywhere except the start of a term.

In addition to terms and operators, queries can refer to specific fields, such as "assetType:computer."

There are more esoteric search facilities. For example, a term that ends with a tilde (~) is a proximity search. Fielded range searches, such as likelihood:[1 TO 4], are supported. When searching for more than one term, a query can "boost" the relevance of a particular term.

Terms are combined with Boolean operators to form more complex queries.

Search Type	Example
Basic	server
Phrase	"cvss score"
Wildcard	serv* (matches server, serving, serves) te?t (matches test, text)
Fielded	assetType:computer
Boolean Operators	The following Boolean operators are supported: ▪ *term1* **AND** *term2* ▪ +*term1* *term2* (+ indicates that term1 must exist to match) ▪ *term1* **NOT** *term2* ▪ *term1* -*term2*
Fuzzy	server~ (matches server, swerver, fever, fervor, etc.)
Fielded range	impact:[1 TO 4] (inclusive--matches impact 1, 2, 3, or 4) impact:{1 TO 4} (exclusive--matches impact 2 or 3)

Additional Information

For more information about the advanced searching features built in to RiskVision, see http://lucene.apache.org/core/2_9_4/queryparsersyntax.html.

Using special characters to search objects might not return correct results. Instead, you can use the Advance Filter in the Filter by drop-down list if you have to perform a multi-criteria search.

Supported Fields

The following fields can be used to narrow the scope of a search to a particular field for certain objects. In the context of a grid of Policy objects, for example, you can search for specific policy types:

policyType:

Asset/Entity

- assetType
- assetSubtype
- name
- organization
- division
- subDivision
- assetNumber

- address.name
- address.address
- address.physicalPosition
- address.floor
- address.building
- address.city
- address.state
- address.region
- address.postalCode
- address.country
- assetTags.name
- assetTags.category
- assetTags.description
- assetTags.createdBy
- assetTags.createdTime
- assetTags.displayName
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1

Computer System

Kind of Asset/Entity; adds:

- applicationLinks.cpe.description
- applicationLinks.cpe.title
- applicationLinks.cpe.part
- applicationLinks.cpe.vendor
- applicationLinks.cpe.version
- operatingSystems.cpe.description
- operatingSystems.cpe.title
- operatingSystems.cpe.part
- operatingSystems.cpe.vendor
- operatingSystems.cpe.version

Exception Request

- name
- justification
- startDate
- nextReviewDate
- requestedBy
- approvedBy
- status
- restart
- reEnd
- risk

- gap.createdBy
- gap.creationTime
- gap.name
- gap.status
- gap.priority
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.date1 (to) customAttributes.date3
- customAttributes.boolean1 (to) customAttributes.boolean5
- customAttributes.long1 (to) customAttributes.long3
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1 (to) .string25
- customAttributes.extendedCustomAttributes.text1 (to) .text2
- customAttributes.extendedCustomAttributes.date1 (to) .date3
- customAttributes.extendedCustomAttributes.boolean1 (to) .boolean5
- customAttributes.extendedCustomAttributes.long1 (to) .long3

Incident

- title
- description
- timeStarted
- timeDetected
- timeReceived
- uiIncidentId
- incidentNumber
- currentWorkflowStageName
- incidentType.typeName
- incidentType.typeDescription
- incidentSubtype.subtypeName
- incidentSubtype.subtypeDescription
- incidentDetail.severity
- incidentDetail.priority
- incidentDetail.status
- incidentDetail.preventiveMeasures
- incidentDetail.causeAnalysis
- incidentDetail.confidentialityAffected
- incidentDetail.integrityAffected
- incidentDetail.availabilityAffected
- incidentDetail.businessCriticality
- incidentSubmitter.caption
- attachements.name [Note misspelling]
- attachements.pathId [Note misspelling]
- attachements.url [Note misspelling]
- attachements.version [Note misspelling]
- customAttributes.string1 (to) customAttributes.string25

- customAttributes.text1 (to) customAttributes.text2
- customAttributes.date1 (to) customAttributes.date3
- customAttributes.boolean1 (to) customAttributes.boolean5
- customAttributes.long1 (to) customAttributes.long3
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1 (to) .string25
- customAttributes.extendedCustomAttributes.text1 (to) .text2
- customAttributes.extendedCustomAttributes.date1 (to) .date3
- customAttributes.extendedCustomAttributes.boolean1 (to) .boolean5
- customAttributes.extendedCustomAttributes.long1 (to) .long3

Policy Set

- title
- description
- descriptor
- definitions
- scope
- purpose
- audience
- supportingInformation
- keyPoints
- policysetType
- policysetSubtype
- parentPolicySetIds
- policySetCategoryIds
- currentWorkflowStageName
- workflowUserDefinedStatus
- tags.name
- tags.category
- tags.description
- tags.createdBy
- tags.createdTime
- tags.displayName
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1

Policy

- title
- description
- descriptor
- policyType
- checkFunction
- parameters
- checkType

- checkDescription
- organization
- parentPolicySetIds
- policySetCategoryIds
- tags.name
- tags.category
- tags.description
- tags.createdBy
- tags.createdTime
- tags.displayName
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1

Report

- name
- displayName
- description
- reportOn
- reportFocus
- reportType
- reportChartType
- reportCreationType

Ticket

- name
- description
- plannedStartDate
- startDate
- owner
- priority
- createdBy
- updatedBy
- exceptionExpireTime
- incident.title
- submitter.userid
- attachements.name [Note misspelling]
- attachements.pathId [Note misspelling]
- attachements.url [Note misspelling]
- attachements.version [Note misspelling]
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.date1 (to) customAttributes.date3
- customAttributes.boolean1 (to) customAttributes.boolean5
- customAttributes.long1 (to) customAttributes.long3

- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1 (to) .string25
- customAttributes.extendedCustomAttributes.text1 (to) .text2
- customAttributes.extendedCustomAttributes.date1 (to) .date3
- customAttributes.extendedCustomAttributes.boolean1 (to) .boolean5
- customAttributes.extendedCustomAttributes.long1 (to) .long3

Vulnerability ID

- captionDB (vulnerability title)
- identifier (use title if available)
- description
- abstractText
- analysis
- recovery
- defaultSeverity
- cvssVector (matches value to first ':')
- likelihood
- source
- sourceFlags (string from int; for example, 3 is 'nvdbidefense')
- assessmentCheckSystem
- assessmentCheckName
- assessmentCheckHref
- recordType
- vulnerableProducts.description
- vulnerableProducts.title
- vulnerableProducts.vendor
- vulnerableProducts.version
- data.data
- tags.name
- tags.description
- tags.type
- tags.referenceType

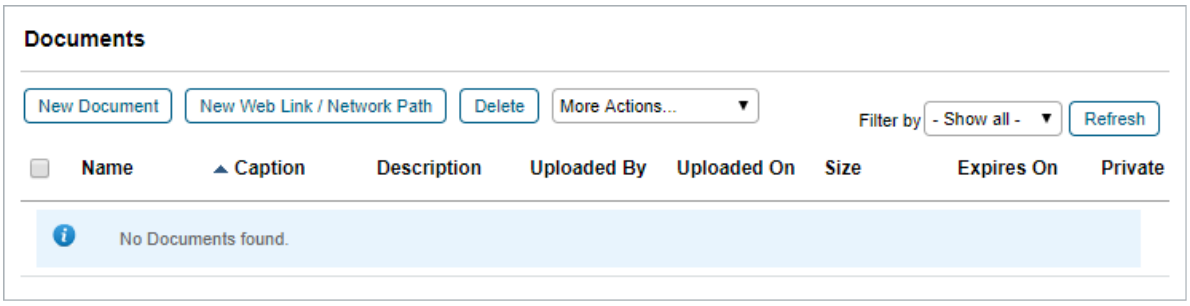
Vendor ID

Kind of Asset/Entity; adds:

- vendor.vendorType
- vendor.vendorTier
- vendor.vendorStatus
- vendor.vendorPreviousName

Documents

The **Documents** tab allows you to attach entity-related documents, such as service contracts. You can attach documents from your local system or document repository, or provide a web link or network link to external information as a reference. The **Documents** tab can be found in the details page of an object, such as an entity, entity collection, program, or control. Note that shared documents cannot be added to all objects.

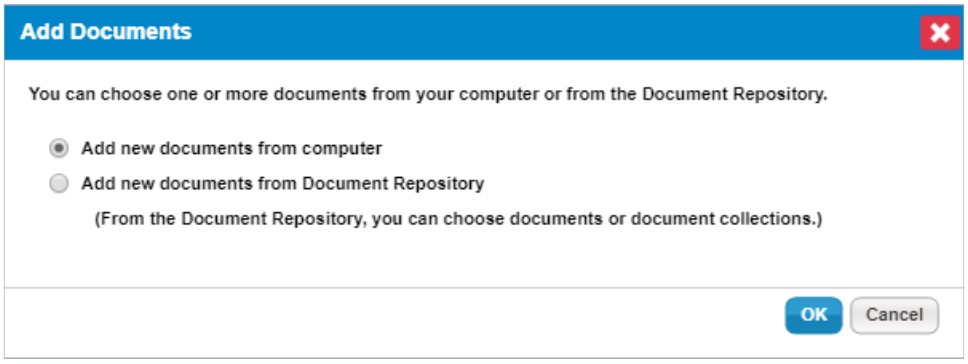


The Documents window.

Other resources allow the attachment of documents in order to document findings, tickets, exception requests, and for other needs. For example, the **Findings** option supports attaching documents in the context of a questionnaire.

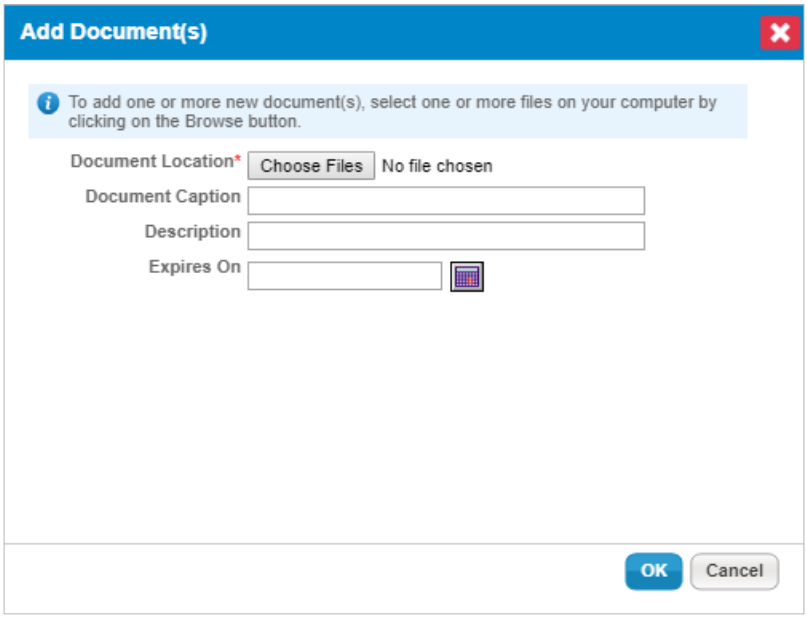
To attach a document:

1. Select an object to open its details page, then click the **Documents** tab.
2. Click **New Document**. Select one of the following options:



The Add Documents window.

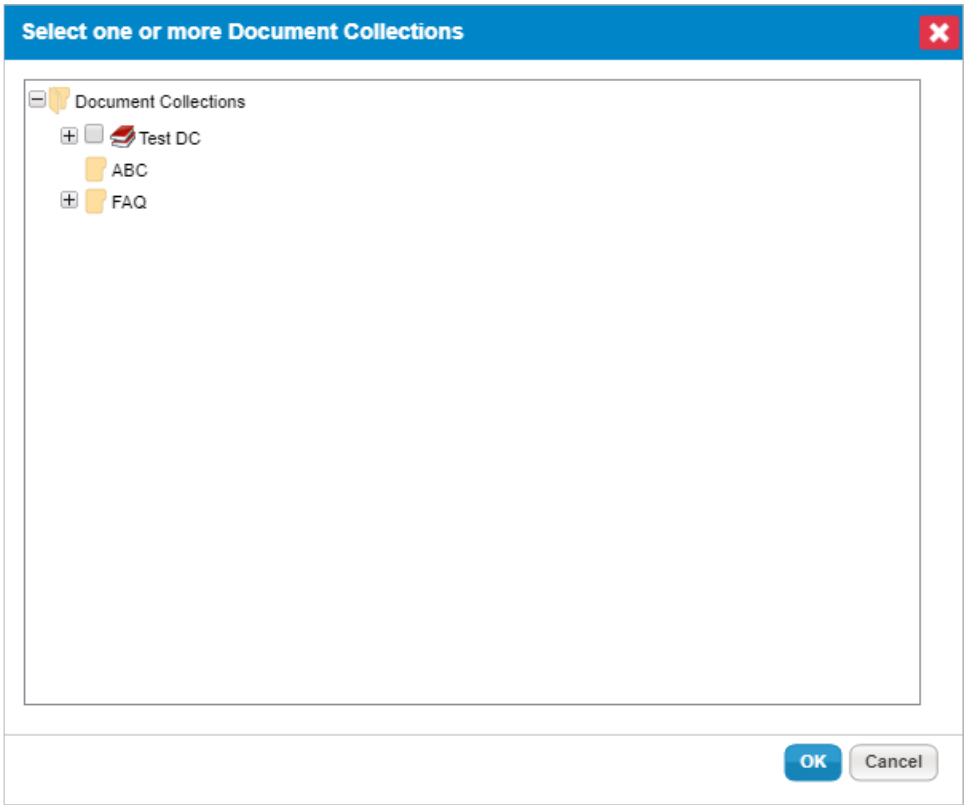
- **Add new document from Computer**.
  - Click **OK**.
  - Fill out all fields, including **Document Caption**, **Description**, and **Expires On**.



The Add new documents from computer window.

- Click **OK**.

- **Add new document from Document Repository**.
  - Click **OK**.
  - Select the required document collection.



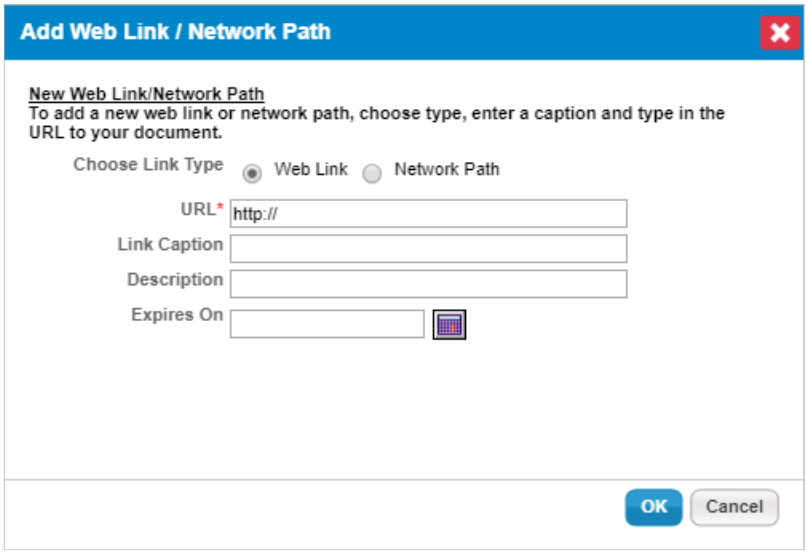
The Add new documents from Document Repository window.

- Click **OK**.

To attach a web link or network path:

1. Select an object, then click the **Documents** tab.

2. Click **New Web Link/Network Path**.



The Add Web Link/Network Path window.

3. Click the **URL** field and type the complete URL or Network Path.
4. **Optional**: Enter a **Link Caption** and **Description**, and click the calendar icon to set the **Expires On** field.
5. Click **OK**.

To delete a document, web link or network path:

1. Select an object, then click the **Documents** tab, or go to the user interface area where documents are located.
2. Check the box next to document(s) and web link(s) you want to delete.
3. Click **Delete**.
4. Click **OK**.

The UNC path will display in all browsers but is only be clickable in Internet Explorer because other browsers block direct connection to the UNC path for security reasons. If you're using another browser you will need to manually navigate to the appropriate location on the external file system.

Controlling Object Visibility

Many default and user-defined objects contain the **Applications** tab in their details page to help you control the visibility of an object in the RiskVision applications. Though you possess sufficient permissions to access the application and the menu item, the object will not be visible to you if the application is not selected in the details page of that object.

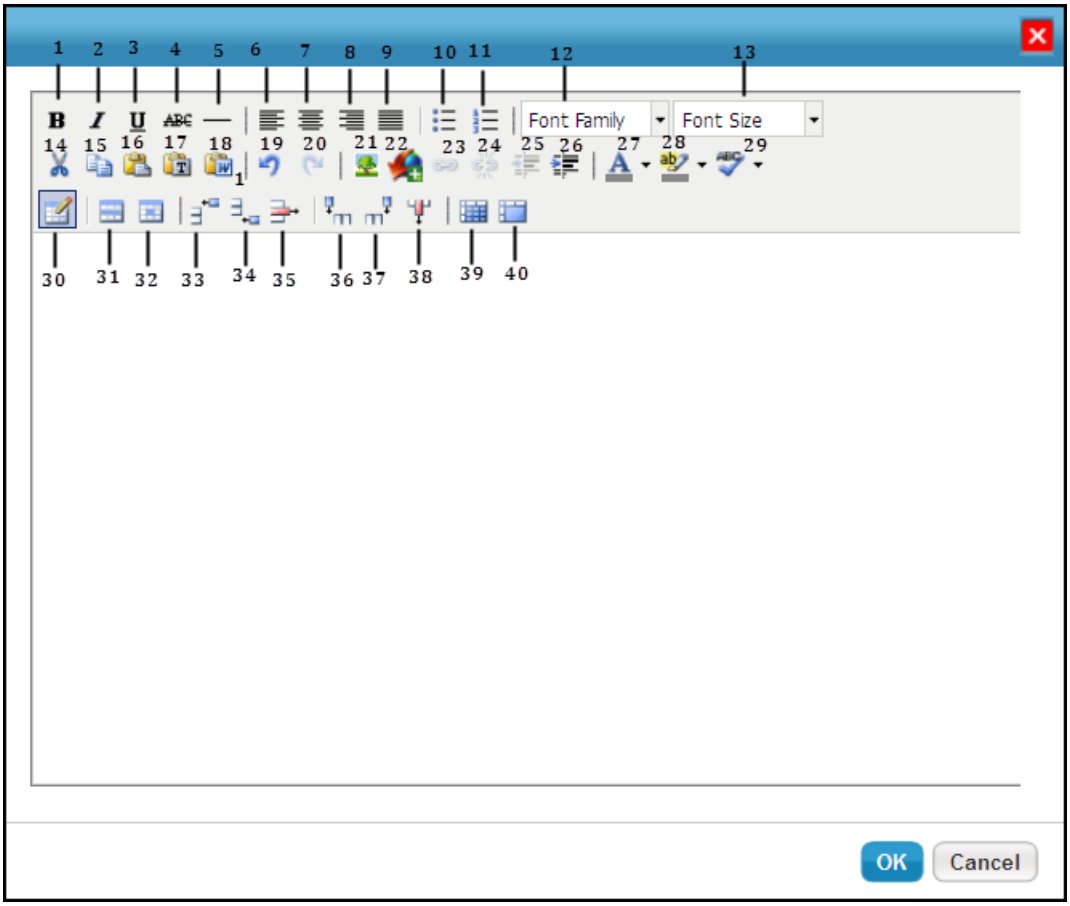
To control an object's visibility:

1. In the RiskVision application, select the object containing the **Applications** tab.
2. Click the **Applications** tab.
3. Click **Edit** and select boxes next to application(s).
4. Click **Save**. The object is now visible in the application(s) you have selected in the previous step.

Using Rich Text Editor

The Rich Text editor is similar to word processing applications in that it allows users to enter text, and contains options to format the text, such as bold, align, indent, lists, font color, font size, text highlight, and more. The Rich Text editor is found throughout the RiskVision application in locations where more than simple text entry is required, such as when explaining an answer choice in a questionnaire, and drafting a questionnaire, content pack or policy. Typically, the Rich Text editor is available for use in the fields of objects that show the "Click to enter text" informational message. When working with the Rich Text editor, you will notice that not all of the options appear for each field. For example, the table options mainly appear only in fields of the questionnaire object.

The following graphic illustrates the Rich Text editor.



The following table lists all the options available in the Rich Text editor.

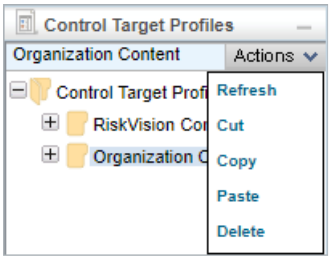
Option	Description
1	Makes the selected text bold. Use Ctrl + B as short-cut key.
2	Makes the selected text italic. Use Ctrl + I as short-cut key.
3	Underlines the selected text. Use Ctrl + U as short-cut key.
4	Draws a line through the middle of the selected text.
5	Draws a horizontal line at the cursor position.
6	Aligns the text to the left.
7	Aligns the text to the center.
8	Aligns the text to the right.

Option	Description
9	Justifies the left and right alignments.
10	Makes the text a bulleted list.
11	Makes the text a numbered list.
12	Choose the font family for the selected text.
13	Choose the font size for the selected text.
14	Cut the selected text. Use Ctrl + X as short-cut key.
15	Copy the selected text. Use Ctrl + B as short-cut key.
16	Paste the text that is cut or copied. Use Ctrl + V as short-cut key.
17	Paste the text without any formatting.
18	Paste the text which is copied in the Microsoft Word application.
19	Revert the changes. Use Ctrl + Z as short-cut key.
20	Reverse undo changes. Use Ctrl + Y as short-cut key.
21	Insert or edit an image. Allows modification of image properties, such as dimension, space, border, and more.
22	Allows you to upload an image from your computer.
23	Allows you to embed the link to the selected text.
24	Allows you to deactivate working links.
25	Adds space between the margin and the beginning of the text on a line.
26	Removes space in the indented line.
27	Allows choosing the text color.
28	Highlights the selected text.
29	Checks the spelling and grammar of the text.
30	Inserts a table in the editor. Use the General tab to specify the number of rows and columns, alignment, padding, border, and more. Use the Advanced tab to set the advanced properties.
31	Updates the current, odd, even, or all rows in a table.
32	Updates the current cell, all cells of a row, all cells of a column, or all cells in a table.
33	Inserts a row before the cursor position.

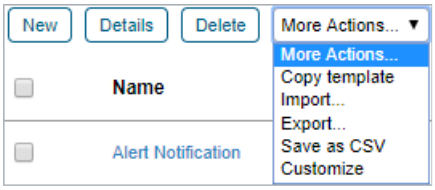
Option	Description
34	Inserts a row after the cursor position.
35	Deletes a row
36	Inserts a column before the cursor position.
37	Inserts a column after the cursor position.
38	Deletes a column.
39	Splits the merged cells.
40	Merges the cells.

Actions

This section covers the most common options available in the **Actions** or **More Actions** drop-down list, seen throughout RiskVision. These drop-down lists are sensitive to the page and the current selection. They can be seen in the tree on the left side of a page, in the center of a page, in the details pane of a page, or at the top-right corner of a page.



The Actions menu.



The More Actions menu.

This article covers how to perform the following actions:

- Refreshing the data;
- Cutting, copying, and pasting;
- Saving the grid as a CSV file; and
- Importing and exporting the data to an XML file.

For information on transitioning bulk findings, tickets, exceptions, or incidents in a workflow, see theBatch Workflow Transitions article.

To refresh the tree view:

1. In the page where a tree view is available, select the folder. The **Actions** menu appears.
2. Click **Actions** and select **Refresh**. The tree is updated.

To cut the selection:

1. In the page where a tree view is available, expand the tree and select the object of interest. The **Actions** menu appears.
2. Click **Actions** and select **Cut**. The object is now ready for paste action.

To copy the selection:

1. In the page where a tree view is available, expand the tree and select the folder of interest. The **Actions** menu appears.
2. Click **Actions** and select **Copy**. The object is copied.

To paste the cut or copied action:

1. In the page where a tree view is available, expand the tree and select the folder of interest. The **Actions** menu appears.
2. Click **Actions** and select **Paste**. The object is pasted.

To delete the selection:

1. In the page where a tree view is available, expand the tree and select the folder of interest. The **Actions** menu appears.
2. Click **Actions** and select **Delete**. The object is deleted.

To save fewer rows in the grid or the complete grid in CSV format:

1. Open the page of interest in which the **More Actions** drop-down list containing the **Save as CSV** option is available.
2. Do one of the following:
    - To save the complete grid, select **Save as CSV** in the More Actions drop-down list.
    - To save the row(s) in grid, select the row(s) of interest and select **Save as CSV** in the More Actions drop-down list.
3. A dialog appears, displaying the options to open or save the file. Follow the instructions displayed by your browser to save the file.

To import a file in XML format:

1. Open the page of interest in which the More Actions drop-down list containing the **Import** option is available.
2. Select **Import** in the More Actions drop-down list. An import dialog sensitive to the object type appears. For example, if you are importing an email template, the **Import Email Templates** dialog will be seen.
3. Click **Browse** to select the file.
4. Click **OK** on the dialog after the file is selected. The dialog is exited and the object(s) is imported.

To export the object(s) or the complete grid in XML format:

1. Open the page of interest in which the More Actions drop-down list containing the **Export** option is available.
2. Do one of the following:
    - Select **Export** in the More Actions drop-down list to export the complete grid.
    - Select the row(s) of interest and select **Export** in the More Actions drop-down list to export the row(s) in grid.
3. A dialog appears, displaying the options to open or save the file. Follow the instructions displayed by your browser to save the file.

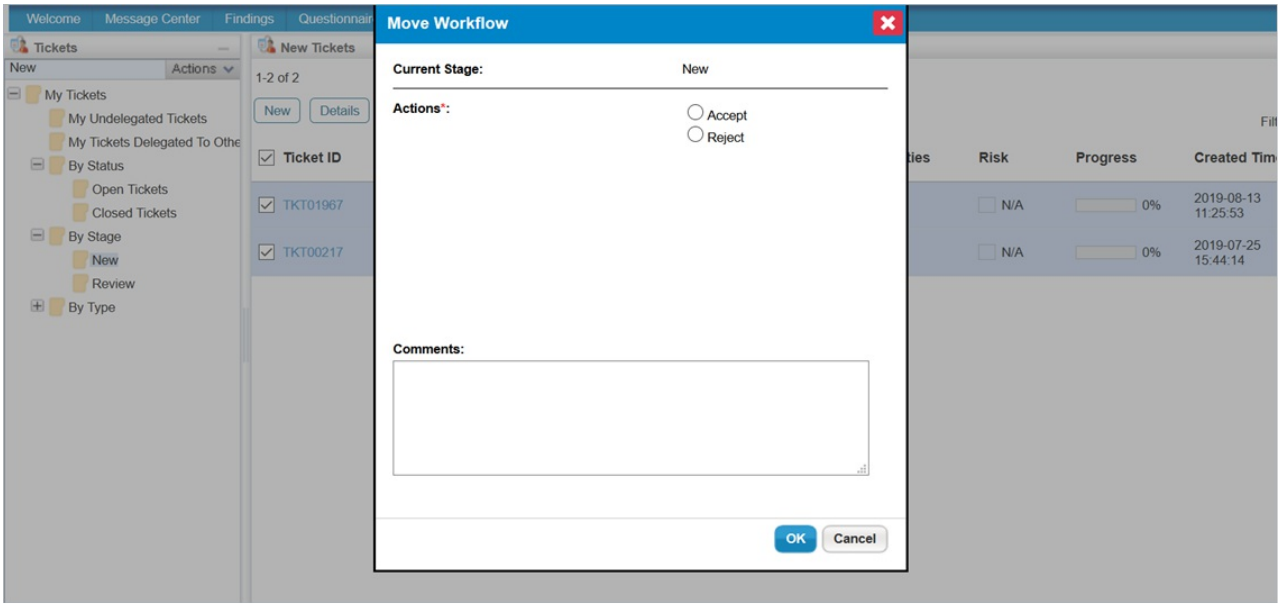
Batch Workflow Transitions

The **Batch Workflow Transition** action makes it possible for users to move multiple objects to another workflow state in bulk. Once objects have successfully transitioned, entries are recorded in each object's **Workflow History**, but a single entry is logged for each bulk-transition on the **Events** page in **Administration**. Depending on the application you're currently working in, these objects include:

- Findings;
- Tickets;
- Exceptions Requests; and
- Incidents.

When using this action, note that:

- Up to 50 objects can be bulk-transitioned at one time.
- Only objects in the same stage from the same workflow can be transitioned in bulk, which are grouped and selected in the **By Stage** folder and its sub-folders. If needed, the workflow settings can be modified in **Configuration > Workflows.**
- If one or more objects cannot be transitioned due to an error, the transition will fail.
- Bulk transitions cannot be performed on closed or terminal objects. Reopening objects in bulk is not supported.
- Only users with **View** and **Update** permissions on the objects can perform this action.



The Move Workflow window, which allows you to transition multiple objects at once.

Batch workflow transitioning supports the use of the Groovy programming language. If you wish to use Groovy for bulk-transitioning workflows, contact Resolver Support.

In order to support batch workflow transitioning, users upgrading to RiskVision version 9.3 or higher must include the following method signature in the **DetailPane** Groovy file of the desired object: `public boolean isTransitionActionAllowedForBatch(String transitionAction, String toStage, boolean forceTransition, List payloads).`

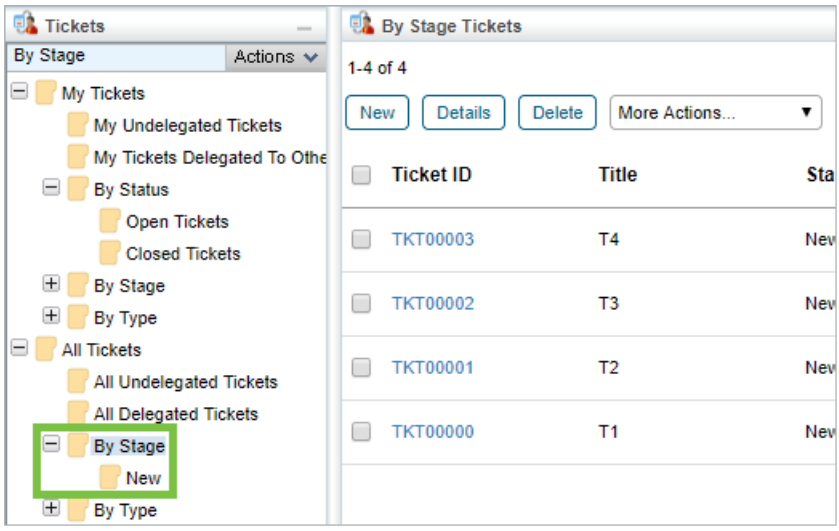
`In addition, any Groovy customization files that implement PayloadScriptAction must provide implementation for isTransitionActionAllowedForBatch() in the DetailPane Groovy file.`

To bulk-transition objects:

1. Click **Home**, then navigate to the object you wish to perform the action on (i.e., **Findings**, **Tickets**,

Exceptions, or **Incidents**).

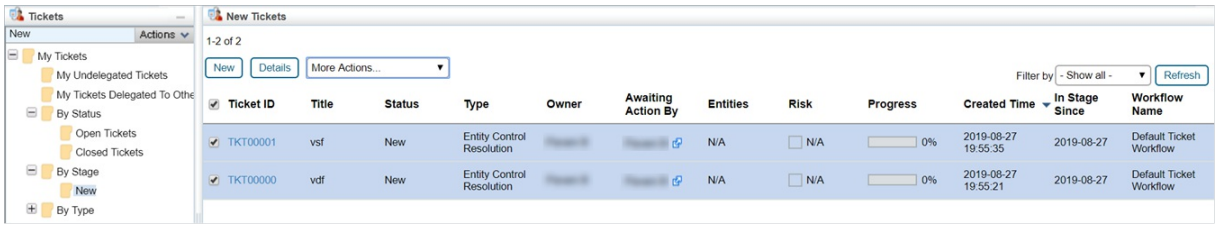
2. Click the **+** icon beside the **By Stage** folder in the tree view to display its sub-folders.



The By Stage folder in the tree view.

3. Click a sub-folder under **By Stage** to display objects in the grid based on their current stage.

4. Select the checkboxes beside the appropriate objects or select the checkbox in the far-left of the grid's header to select all objects.

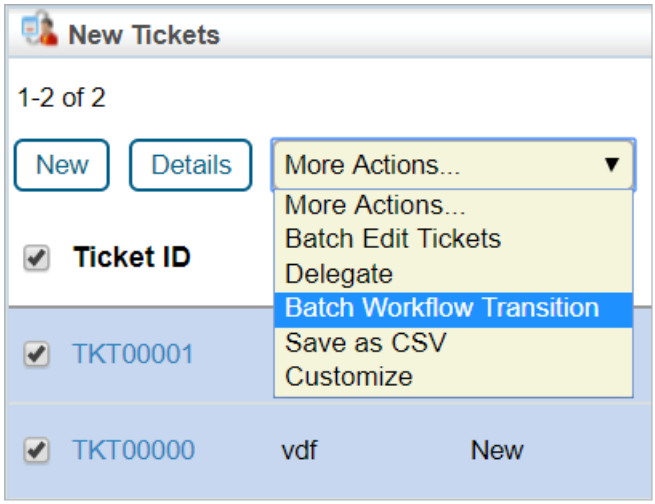


Selected objects in the New sub-folder.

> When selecting objects in bulk, review the **Workflow Name** column on the far-right of the grid to ensure all objects belong to the same workflow definition. If a workflow's name was recently modified, the workflow must be synchronized before it will display its current name in the column.

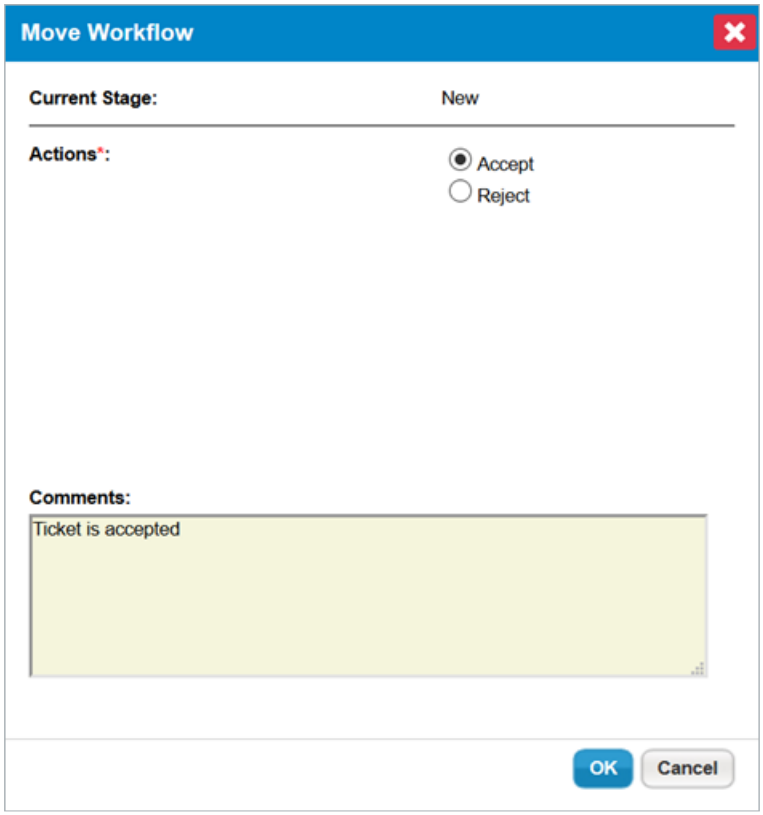
> A maximum of 50 objects can be selected for a single bulk transition. Closed objects cannot be selected.

5. Click the **More Actions...** dropdown menu, then click **Batch Workflow Transition** to display the **Move Workflow** window.



The Batch Workflow Transition option in the More Actions... dropdown menu.

6. Select an option in the **Actions** section to transition the objects to another state.
7. Enter any notes in the **Comments** text box as required.



The Move Workflow window.

8. Click **OK** to complete the transition and refresh your browser to see your changes.

Visualizing Objects

The primary goal of this section is to provide an overview of visualization and to discuss the tool options available for navigational purposes. For case-specific information about how the RiskVision visualization tool helps understand the pattern with respect to workflows and relationships, please read the sections, Visualizing Relationships and Visualizing Workflows.

RiskVision has integrated a visualization tool in the objects of entities, entity collections, and workflows to help users visualize relationships between entities, entity collections, and workflow stages. This tool has been incorporated as a separate tab on the details page of the respective objects - the Relationships tab for entities and entity collections and the Stages tab for Workflows. A default graphical layout is displayed by clicking on the Relationships tab and then selecting "Relationship Report" for entities and entity collections, it is also displayed by clicking on Stages tab for workflows.

This tool has different layouts that allow you to choose the representation that is easiest to understand for you. In addition, it contains options to zoom and to move around the graph when there are many nodes in a layout.

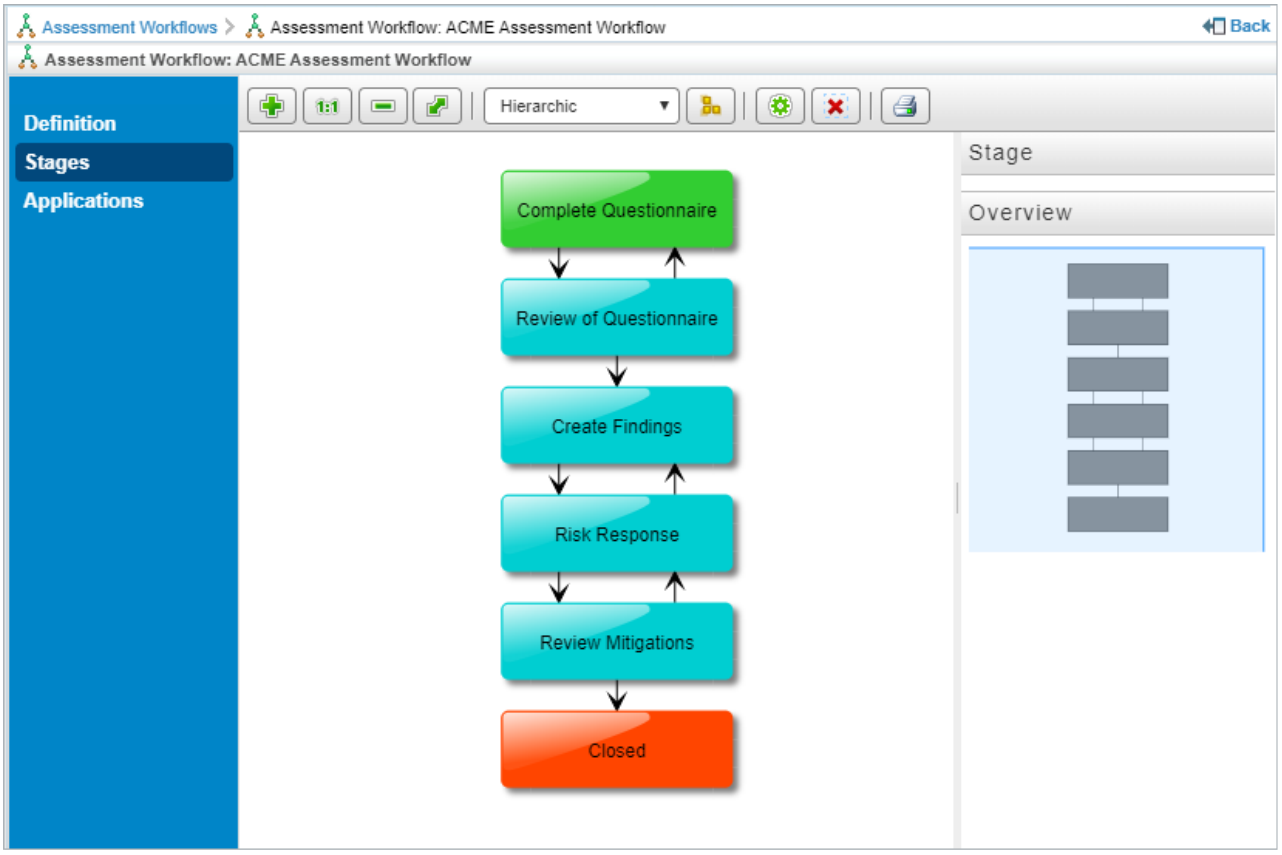
The following tool options are available to enhance your visual experience:

Option	Description
	Click to magnify the layout. Continue selecting this icon until you have achieved the desired magnification level.
	Click once to revert the layout to its original size.
	Click to reduce the size of the layout. Continue selecting this icon until you have achieved the desired magnification level.
	Click once to make the content fit in the layout.
Selecting layout	Select a desired layout option in the drop-down list at the top of the window.
	Click once to revert the layout to its original size and to properly align the layout.
	Click once to show the labels.
	Click once to hide the labels.
	Click to open the layout in a new browser tab for printing purposes.
	Click to reload the graph with changes you have applied.

For visualizing workflows in RiskVision, you need a web browser with HTML5 support.

Moving the Layout

When a layout contains several nodes, you may want to zoom in on the layout to clearly read the nodes. However, this action limits the number of nodes in views. In order to view the other nodes with same zoom in level, use the **Overview** pane to move the layout.



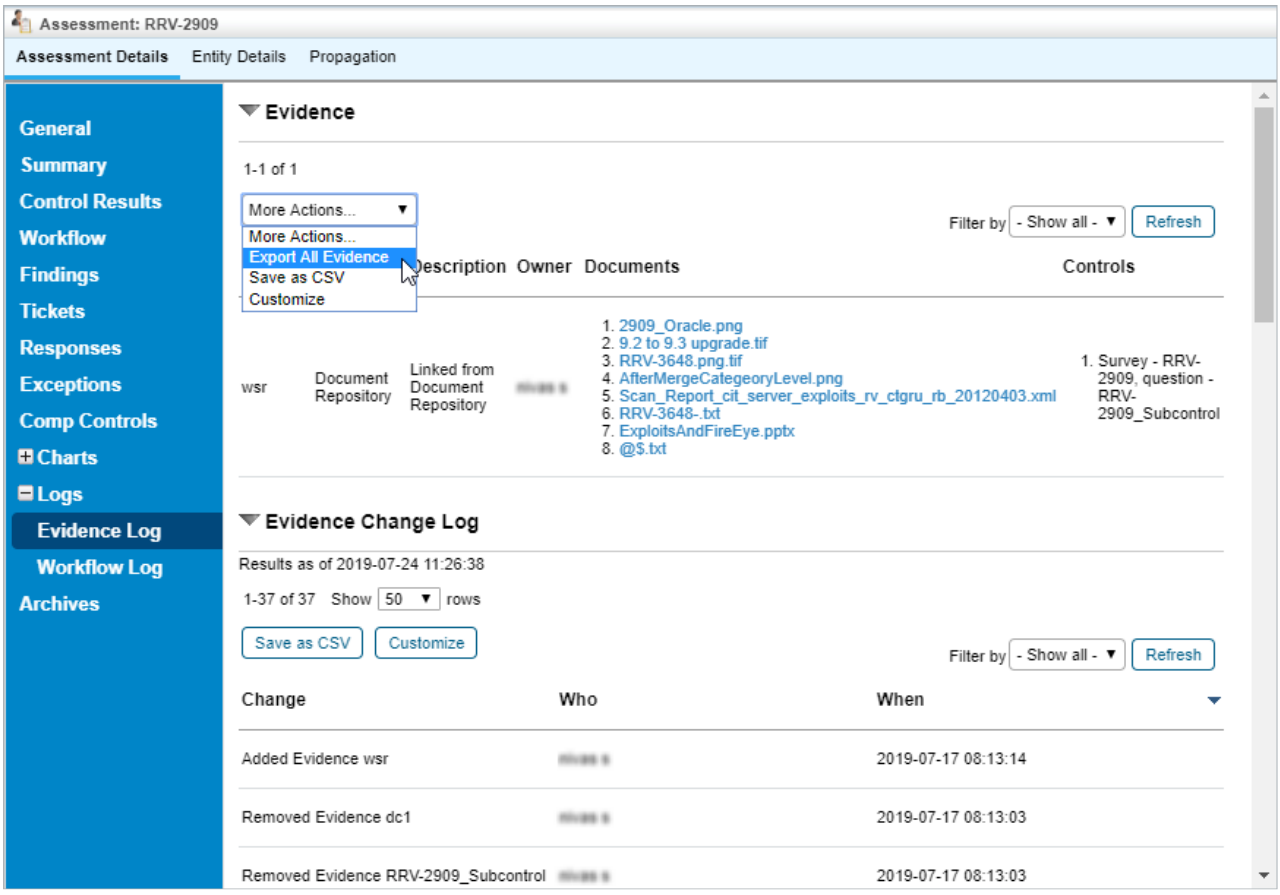
The Workflow Stage layout.

To move the layout:

- In the zoomed layout, move the cursor into the rectangular shaded region of the**Overview** pane at the right-hand side of the window. Hold the left button of the mouse, and move the mouse in the required directions.
- Use the vertical and horizontal scroll-bars around the layout which appears when you expand the layout beyond the best fit.

Bulk Exporting Evidence

RiskVision allows users with the Assessment Manage permission to bulk export evidence from assessments. To perform the bulk export, click**More Actions > Export All Evidence**. This option is visible in the **Assessments Details** page > **Evidence Log** tab.



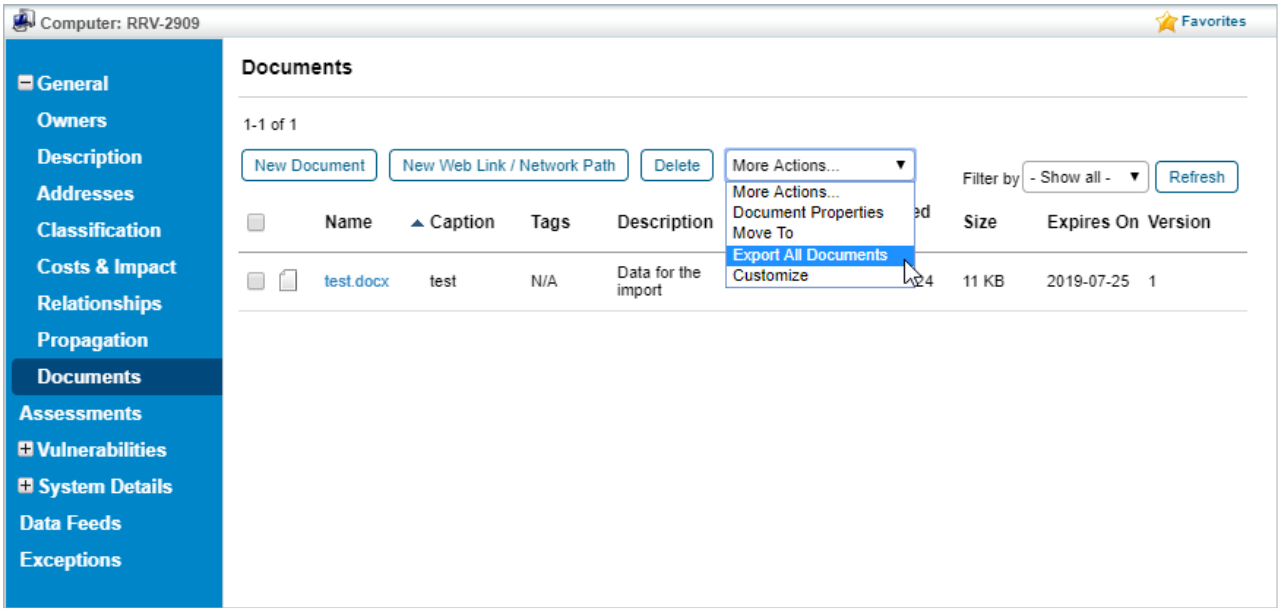
The Evidence Log tab on the Assessment Details page.

When you perform a bulk export of evidence, you will get a single downloaded zip file. For assessments, the zip file name shall be Program - Assessment Name.zip. This zip file will contain multiple folders, one for each question.

If a document is used as evidence for more than one question within that assessment, all the documents are downloaded where user can open and save all the documents.

Bulk Exporting Documents

Users can also export documents attached to entities, findings, and tickets using **More Actions > Export All Documents**. This feature requires object Manage permissions for the object you performing a bulk export from. You can access the bulk export option in the object's **Documents** tab.



Accessing the Export All Documents option on an object's Documents tab.

This option is located in a similar position on the Findings and Tickets **Documents** tabs. Bulk exporting of documents results in a single zip file. The name of the zip file depends on the object from which the files have been exported. For entities, the zip file is the entity name, for findings the file name is Finding ID - Finding Name - Entity Name.zip, and for tickets, the file name is Ticket ID - Ticket Name.zip. The Bulk Export Documents feature applies to documents, but not to network paths and web links.

Maximum Zip File Download Size

By default, downloaded zip files for both evidence and documents cannot exceed 200 MB in size.

The maximum file size can be adjusted through the `attachments.export.maxAllowedSize` property. For example, to change the maximum file size to 1 GB, you would set the property as follows: `attachments.export.maxAllowedSize=1024`.

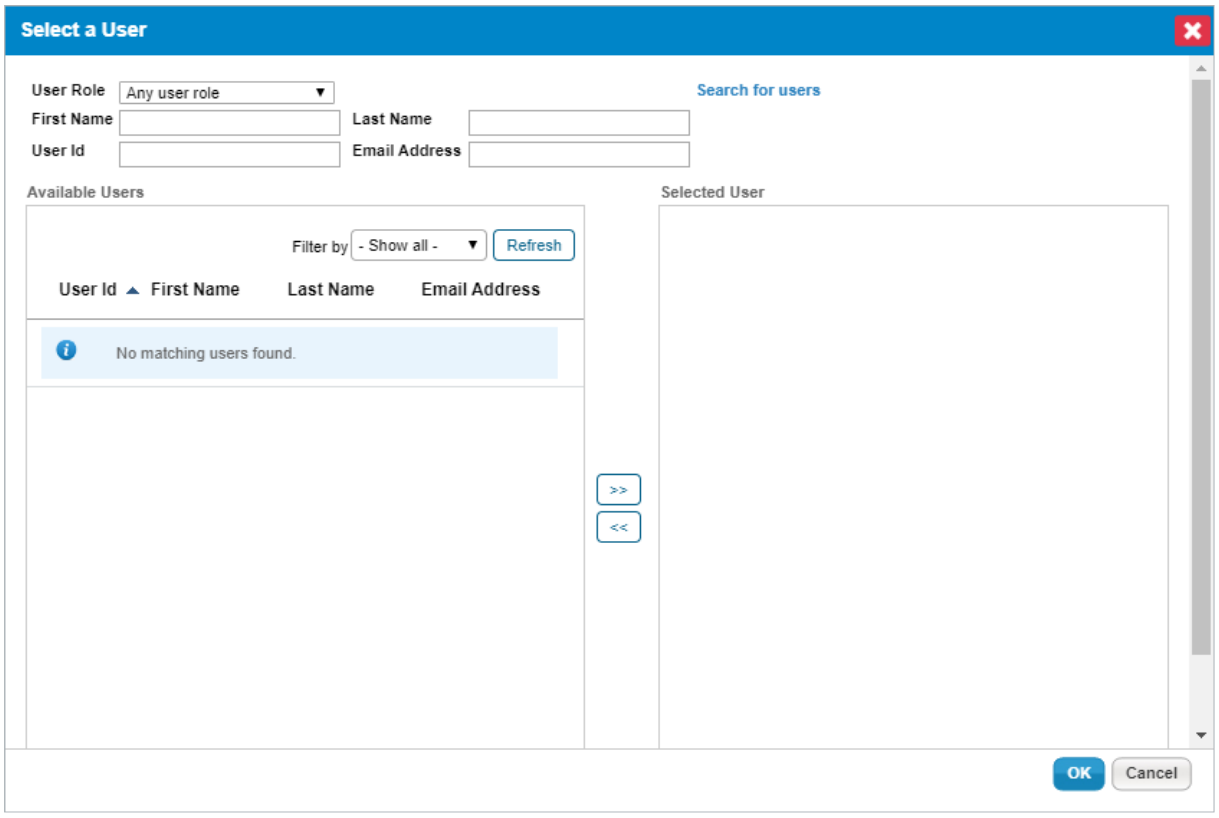
User Picker

You can add users as owners to objects such as entities, tickets, and findings using the **User Picker** window to search for users. This feature allows you to search for users by Source, User Role, First Name, Last Name, User ID, and Email Address. Each search will return a maximum of 200 user records.

The **Source** dropdown menu appears in the **User Picker** window when the `com.agiliance.security.agluserintegration.label=Search External Users` property is enabled, which allows importing users from the Authentication Connector, which connects to your LDAP directories, into RiskVision.

To search for users:

1. Open a page of interest in which the owner or primary owner must be added. Click the + icon to open the **User Picker** window.
2. Pick the appropriate source, if the property is enabled.
3. Enter the search criteria.



The User Picker window.

4. Click **Search for users**. The result appears in the **Available Users** list.
5. Add a user to the **Selected User** list by selecting the user in the **Available Users** list and clicking the right arrow pointing from the **Available Users** to the **Selected User** list. To remove a user from the **Selected User** list, select it in the **Selected User** list by clicking on it, then click the left arrow that points from the **Selected User** list back to the **Available Users** list.

If the user selected from Authentication Connector does not exist in RiskVision, the new user account is created within the application before assigning them to the object.

Using Search Criteria

1. Search results are filtered using an AND condition between the fields
2. Depending on the Source selected internal users or LDAP users, the use of the wildcard character is different:

   - For Internal Users, the search field supports a single word in which the wildcard of "*" can be used before and/or after the search term. For example: *test* , *test, test * and test
   - For LDAP users search, the search field supports a single word that includes the wildcard of "*" at the beginning and/or end of the search terms as well as anywhere within the search term. For example: *test, test*, tes*t, te*t, and t*est

- Note: If you are not making a wildcard search, your search terms will be exact match terms for each of the terms you are using.

About Welcome Page

Each RiskVision application has a **Welcome** page that can be customized for each individual user and their specific roles. The components of this page change based on the selected application.

When you log in, a summary of items assigned to you, such as questionnaires, tickets, exceptions, and notifications, will be displayed. Clicking on any of these items on the **Welcome** page opens a navigation pane with details specific to your selection.

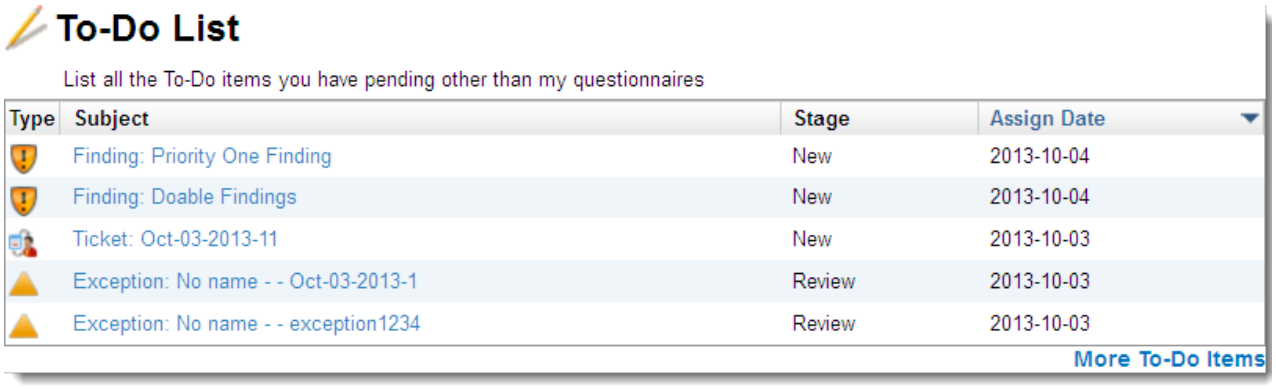
Users can also configure their **Welcome** page to display a specific dashboard or report, including the Compliance Dashboard. For information on customizing the **Welcome** page, see the Select a Default Dashboard article.

My Assessments

The **My Assessments** section in the **Welcome** page provides a glimpse of questionnaires that were recently assigned to you, because the assessment workflow has entered the stage in which you are a stakeholder. Based on the due date of a questionnaire, click the subject to begin answering a questionnaire instantly without requiring you to search for the questionnaire in the Questionnaires page. Clicking the **Go to Assessments** link at the bottom of the section will direct you to the **Questionnaires** page on the **Home** menu, where questionnaires with relevant action options are shown in a grid.

To-Do List

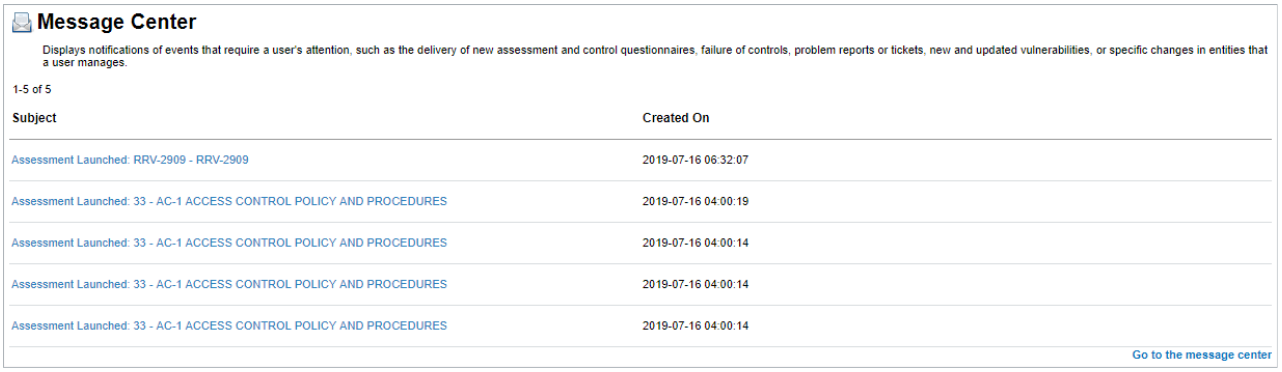
The **To-Do List** is a component of the Welcome page that displays exception requests, tickets, findings, and other requests for action (except assessments and questionnaires). The items displayed depend on your role, the current status of the system, and the selected application.



Click on an item to see more detail. Click **More To-Do Items** to see all to-do items. As with other grids or tabular displays in RiskVision, click on a column heading to sort by that column.

Message Center

The **Message Center** is a short summary of your most recent notifications, and is displayed on the **Welcome** page.



The Message Center.

To view a message:

1. Click a message to open the **Alert** window with the message's contents.
2. Click one of the following buttons:
    - **Archive & Close**: Dismiss the window and remove the message from the **Message Center**.
    - **Cancel**: Keep the message in the **Message Center**.
3. **Optional**: To view all messages, click **Go to the message center** or go to **Home** > **Message Center**.

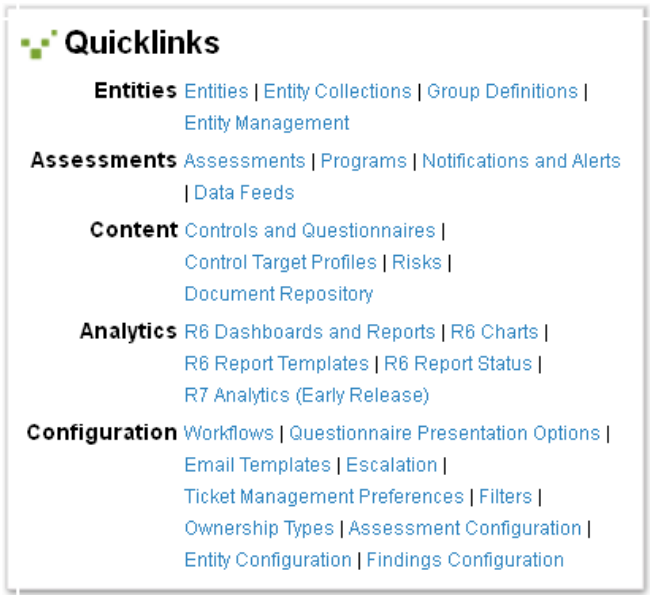
For more information, see Understanding the Message Center.

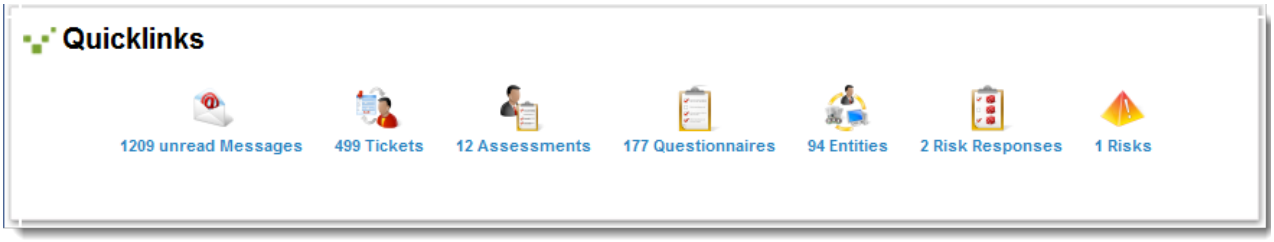
My Findings

The **My Findings** section in the **Welcome** page provides a glimpse of the recent five findings you have reported. To view and monitor the progress of all your reported findings, click **Go to Findings** at the bottom of the section so that you are directed to the Findings page on the Home menu.

Using Quick Links

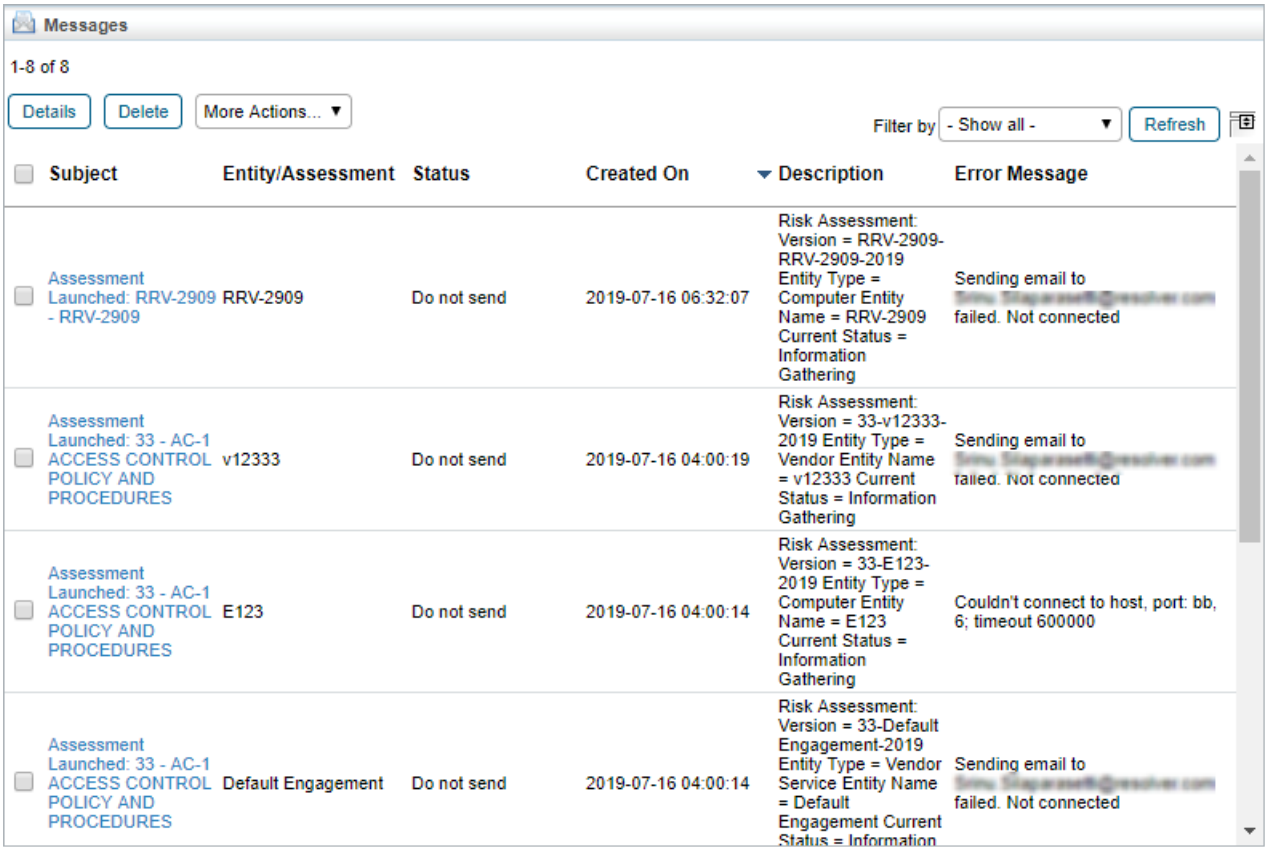
Quicklinks is a component of the Welcome page that provides a categorized set of links to other pages in the RiskVision system. The set of links change depending on the selected application (such as the RiskVision Application) and your user account's role.





Understanding the Message Center

The **Message Center** is a page that displays notifications, such as an alert that a workflow has advanced to the next stage. The notifications in the **Message Center** page are always relevant, because of certain criteria. For example, the system only sends alerts to the stakeholders of a particular workflow stage.



The Message Center page.

In the **Message Center** page, you can perform the following tasks:

- Clicking the subject of a message will help you view the details in a pane below the grid.
- Simultaneous deletion or archiving of multiple messages is possible.

About Findings Page

Findings are associated with controls that are non-compliant in an assessment. The **Findings** page is a grid comprising of findings that are created for controls or questionnaire in the Questionnaire window as well as those created in the grid using the New button. In the **Findings** page, you can create a finding for an entity. You can work on findings only if you are a stakeholder or findings administrator. To respond to a finding, you must use response, exception or ticket that are available in the **Findings** details page. In order to work on exception and ticket, you need the set of permissions required by those objects; since the permissions related to a finding will allow only to modify the general, risk assessment, response, and attachments.

The following are the actions/option Findings in the grid helps you manage a finding:

Actions	Description
New	Creates a new finding.
Details	Displays the finding details so you can edit, update the general, risk assessment and response settings, or add or manage objects associated with a finding.
Delete	Allows deletion of findings.
Import Audit Findings	Allows importing of findings for an entity. For more information, see Importing Findings.
Add Finding Response	Allows adding a response to a finding
Show Finding Responses	Displays responses, if any, for the selected finding.
New Exception	Creates an exception to the selected finding. Use an exception to override the finding's score. For information about how to create an exception, see Requesting Global Exceptions.
New Ticket	Creates a ticket to the selected finding.
Synchronize Workflow	Incorporates workflow changes into the selected finding. The moment you apply this action the finding will advance using the latest changes.
Delegate	Bulk delegation can be done by stakeholders of a workflow or Users with Manage permission by checking the check boxes next to one or more findings and choose **Delegate** option to bring up the **User Picker**. The users can then delegate to any user or team.
Revoke Delegation	When a user chooses the bulk action of **Revoke Delegation** under the **More Actions** menu, then the delegation shall be revoked for all objects that have been delegated.

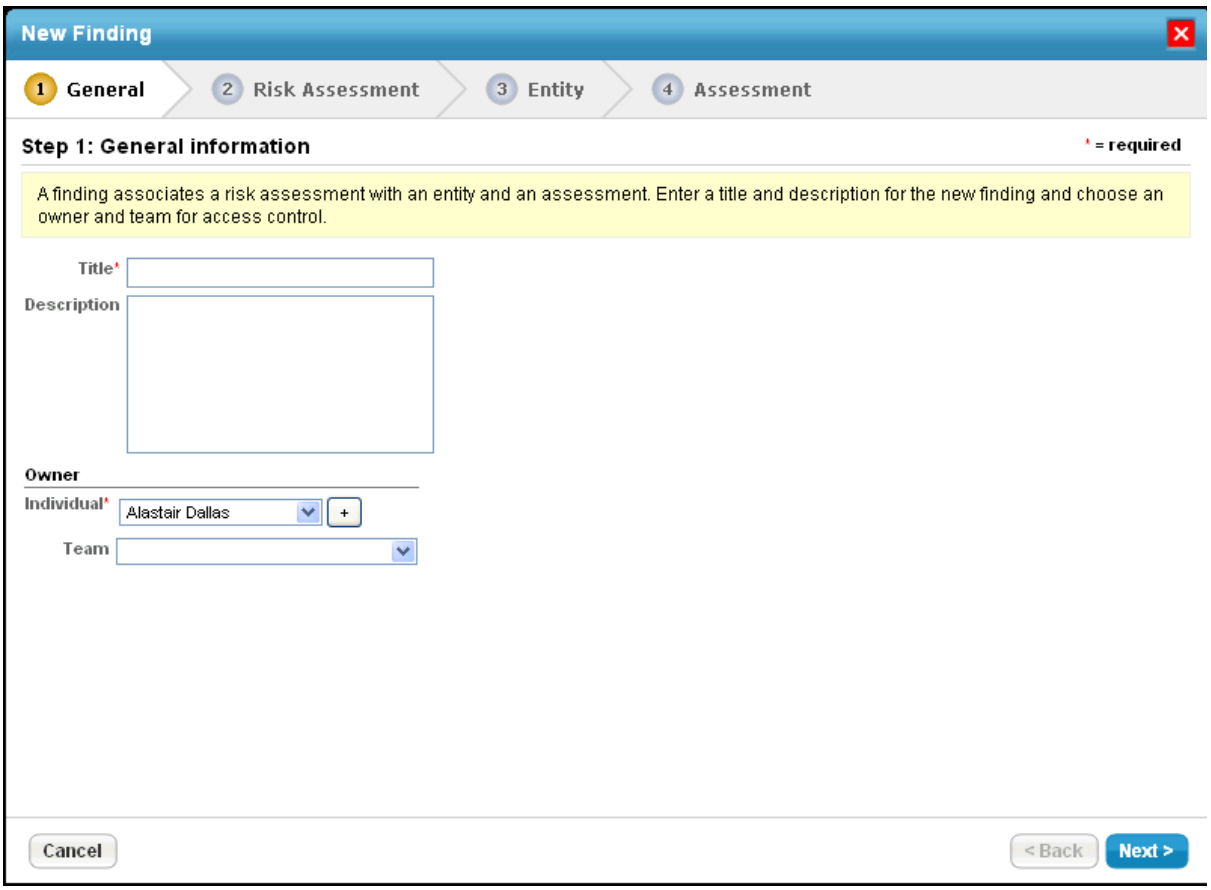
Creating a Finding

You can create a finding for an entity, a failed control or any control that does not achieve the desired compliance. Findings for a failed control can be created on the **Control Results** tab of **Assessment Details** page, whereas findings for an entity can be created on the **Findings** tab of **Assessment Details** page or on the **Home** > **Findings** page. At a minimum, findings allow you to perform the risk assessment when created. However, it is the responsibility of the program owner to provide a way for the workflow stage stakeholders to respond to a finding using multiple response mechanisms. For information about how to configure a response mechanism to a finding, see Setting Control Response Options.

Findings are associated with specific assessments, but the wizard allows you to either select an existing assessment or create a new one. You can also create a new entity to associate with the new finding. In this case, you must also create an assessment.

To create a finding:

1. Go to the **Home** > **Findings** page and click **New**. The **New Finding** wizard appears, and displays the **General** wizard page.



2. In the **General** wizard page. Enter **Title, and Description, and select Owner** and **Team. Click Next to continue.**

3. In the **Risk Assessment** wizard page, assess the risk of this Finding by choosing a likelihood and an impact. Select Impact, Likelihood, residual Impact, and residual Likelihoodvalues. Click **Next** to continue.

4. In the **Entity** wizard page, select an existing entity, or create a new entity, which will be the subject of this finding. Click **Next** to continue.

5. In the **Assessment** wizard page Select an existing assessment, or create a new assessment to associate with the new finding. To create a new assessment, select an existing program.

6. Click **Finish** to save the new finding, or click **Cancel** to quit without saving. Note that creating a new finding can take some time.

About Questionnaires Page

The **Home** > **Questionnaires** page lists all of the questionnaires assigned to you in a grid where actions specific to the state of the assessment appear in that questionnaire's row.

About Table Columns

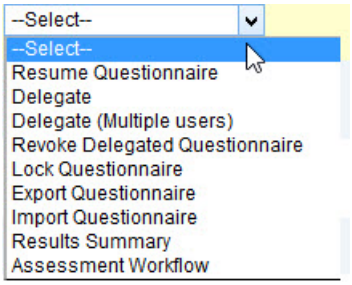
The table columns display the following questionnaire-specific information:

Column	Description
Program	Displays the program name.
Assessment	Displays the assessment name.
Questionnaire	Displays the content name assigned to the entity for evaluation in the program. Tool tip displays the path to the content on the Controls and Questionnaires page.
Status	Displays the stage name.
Complete By	Displays the questionnaire due date.
Progress	Shows the percent complete of the stage.
Delegate To	Shows the user name to whom you have assigned the questionnaire.
Delegated By	Shows the name of the stakeholder who delegated the questionnaire.
Actions	Drop-down that allows you to initiate an action. See below.
Action Items	Shows icons that indicate action items set for the questionnaire questions, such as exception requests, and identifies questionnaires with attachments.

About Action Options

Actions are questionnaire preferences chosen by the Program Owner. An option may be available for one questionnaire but not another. Also, the action options corresponding to each questionnaire do not appear by default in the drop-down list after the Questionnaires are rendered in the grid. Selecting the **Select** option in the drop-down list followed by clicking the drop-down list makes the actions visible in the drop-down list of the corresponding questionnaire.

The following table describes all the actions that could be available:

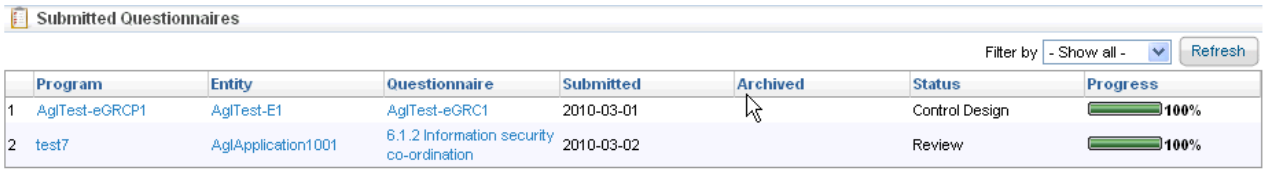


Option	Description
Work on this Questionnaire	Opens the questionnaire and allows you to answer and delegate questions. Only displays when no questions have been answered.
Resume Questionnaire	Opens the questionnaire and allows you to answer and delegate questions. Only displays if one or more questions are answered.
Delegate	Transfers the responsibility of providing answers to another user or a team. The questionnaire disappears from stakeholders list and it is forwarded to the new user with the answers that you have already provided (if any).
Delegate (Multiple users)	Transfers the responsibility of providing answers to multiple users and/or team when the control contains multiple questionnaires.
Revoke Delegated Questionnaire	Stakeholders or users with revoke delegation permission can revoke the responsibility of a user and/or team from answering the questionnaire. The delegated questionnaire disappears from your list and is forwarded to the stakeholder with the answers that the delegated user or team has already provided (if any).
Lock/Unlock Questionnaire	When locked, prevents users from changing the answers. When unlocked, allows any user to open the questionnaire and change answers without first unlocking the questionnaire.
Export Questionnaire	Creates an Excel spreadsheet with the questions and corresponding choices.
Import Questionnaire	Allows you to import answers from an Excel spreadsheet.
Results Summary	Shows the risk and compliance scores based on the questionnaire answers provided.
Assessments Workflow	Displays the assessment's current workflow stage, allowing you to move the workflow to next stage.

The Revoke Delegated Questionnaire option appears when the Questionnaire is delegated to a user or team.

About Submitted Questionnaires Page

The **Submitted Questionnaires** page displays questionnaires in which you were a stakeholder, but which are no longer active, typically because you have completed the questionnaire and advanced it to the next workflow stage, which is often Review. This page allows you to follow the progress of completed questionnaires. You will not be able to view the **Submitted Questionnaires** page on the Home menu unless you have the Questionnaire View Submitted Questionnaires permission.



	Program	Entity	Questionnaire	Submitted	Archived	Status	Progress
1	AglTest-eGRCP1	AglTest-E1	AglTest-eGRC1	2010-03-01		Control Design	100%
2	test7	AglApplication1001	6.1.2 Information security co-ordination	2010-03-02		Review	100%

See also Using the Grid View

About Tickets Page

The **Tickets** page is a grid consisting of tickets in which you are a stakeholder. If you own the responsibility of managing the tickets in your organization, you can view all of the tickets irrespective of the ownership. Depending on the permissions, you can use the **Tickets** page to perform one or more tasks as described below:

- Create a new ticket
- Open a ticket to view the details and to perform the following tasks:
  - Update the general information
  - Transition the workflow
  - Add comments
  - Manage attachments
  - Link or detach entities and vulnerabilities
  - View workflow history and changes
  - Synchronize the changes made to the ticket workflow
  - Delete a ticket

When you access the **Tickets** page, you can view all the tickets that needs your attention as well as the closed ones. For your convenience, the tickets can be segregated using the groups: **By Status, Stage, Type** and **My Tickets Delegated To Others** so that you can view the relevant tickets in one view. For example, you can click the Review group under the Tickets tree to work on the tickets that entered the review stage.

The groups under By Stage appear only when tickets enter a particular stage. For example, if there are tickets in the "New" and "Assigned" stages, only those stage groups appear to the stakeholder.

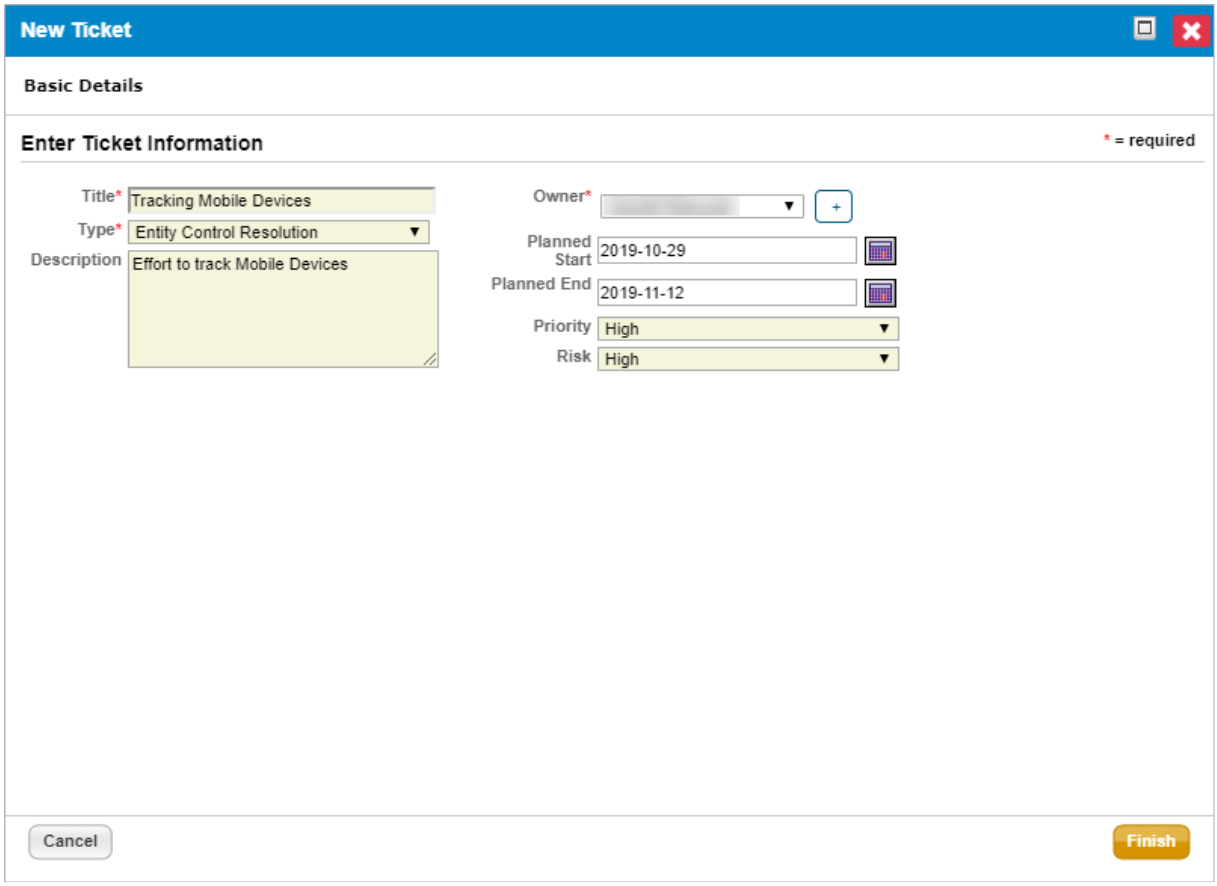
Creating a New Ticket

Use tickets to assign tasks to system users and track progress. Create a ticket for each item that you want to track. For each task, the RiskVision solution creates a single ticket and sends the notification to all stakeholders of the initial stage. Each person views, modifies, and transitions the same ticket. Creating a new ticket requires you to have the Ticket View, Create or Manage permissions.

By default, all tickets use the Default Ticket Workflow template.

To create a new ticket:

1. Go to **Home > Tickets**.
2. Select the **My Tickets** folder.
3. Click **New**. The New Ticket window displays.



The New Ticket window.

4. Enter Title and Description. Select Type, Owner, Priority, and Risk. Also, specify Planned Start and Planned End dates. For information about the description of the fields in the **New Ticket** wizard, see Setting General Ticket Information.
5. Click **OK**.

A new ticket is created and displays in the My Tickets folder. Next, link the ticket to an entity.

You can create a ticket for a finding using the **Tickets** tab on the finding details page, and for a vulnerability using the **Affected Entities** tab on the vulnerabilities details page, and for an incident using the **Actions** and **Tickets** tab on the incidents details page. Creating a ticket manually, automatically marks the vulnerability as acknowledged. If the system (Affected Entities Notification Sender job) creates the ticket automatically, an unacknowledged vulnerability remains unacknowledged.

Batch Edit Tickets

The **Batch Edit Tickets** action makes it possible for users to edit most of the fields in multiple tickets at one time. The fields that **cannot** be edited include:

- Name;
- Status;
- Export Status;
- Submitted By;
- Ticket ID;
- Created Time; and
- Ticket Age.

Once the tickets have been successfully modified, the logged event will include the **Ticket IDs** of the modified tickets, the user who performed the action, records of the modified fields, and the time and date of the action.

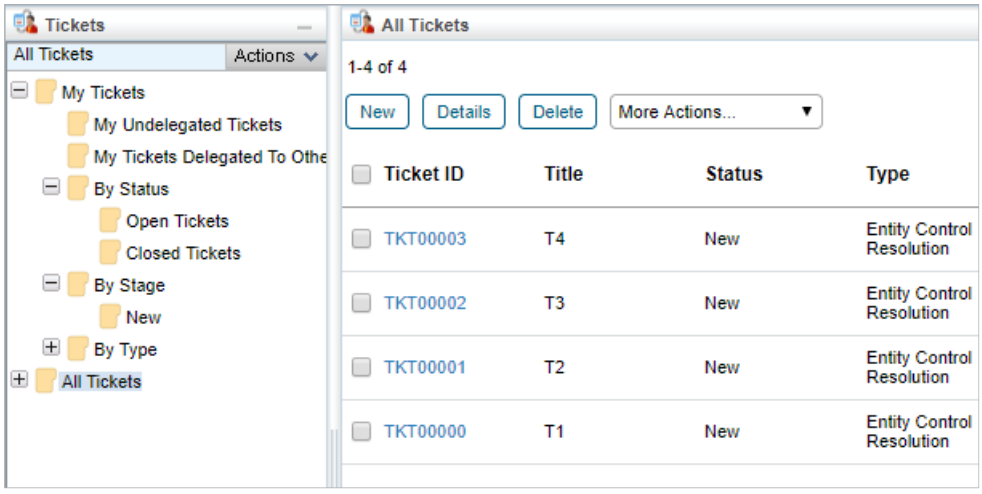
When using this action, note that:

- Up to 50 tickets can be bulk-edited at one time.
- Batch edits cannot be performed on closed or terminal tickets. Reopening tickets in bulk is not supported.
- Only users with **View** and **Update** permissions on tickets can perform this action.

> Batch ticket editing supports the use of the Groovy programming language. If you wish to use Groovy for bulk-editing tickets, contact Resolver Support.

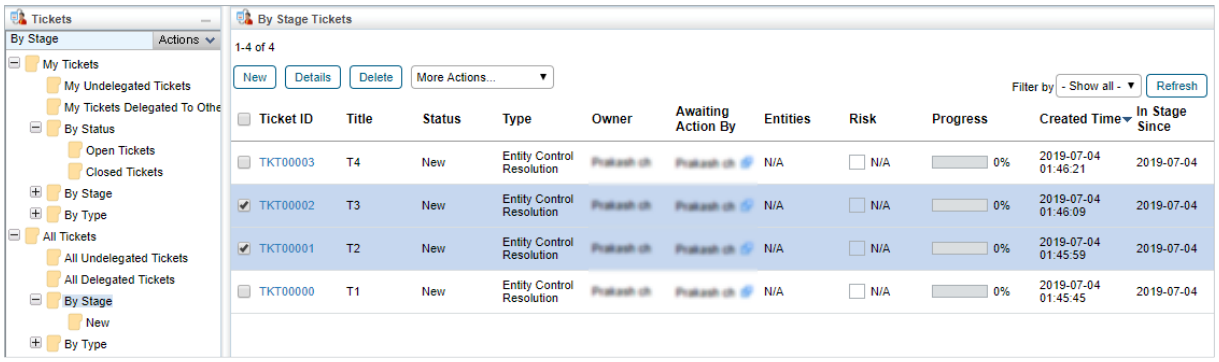
To bulk-edit tickets:

1. Click **Home** > **Tickets**.
2. Click a folder in the tree view to view the tickets in the grid.



Existing tickets.

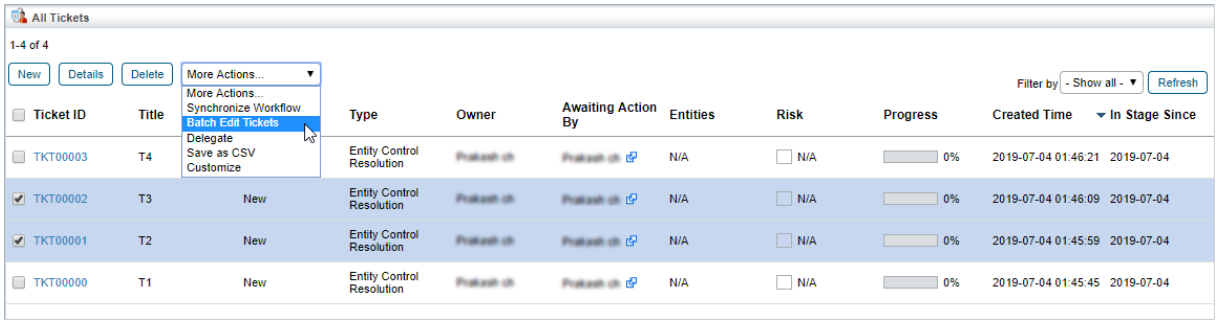
3. Select the checkboxes beside the appropriate objects or select the checkbox in the far-left of the grid's header to select all objects.



Selected tickets.

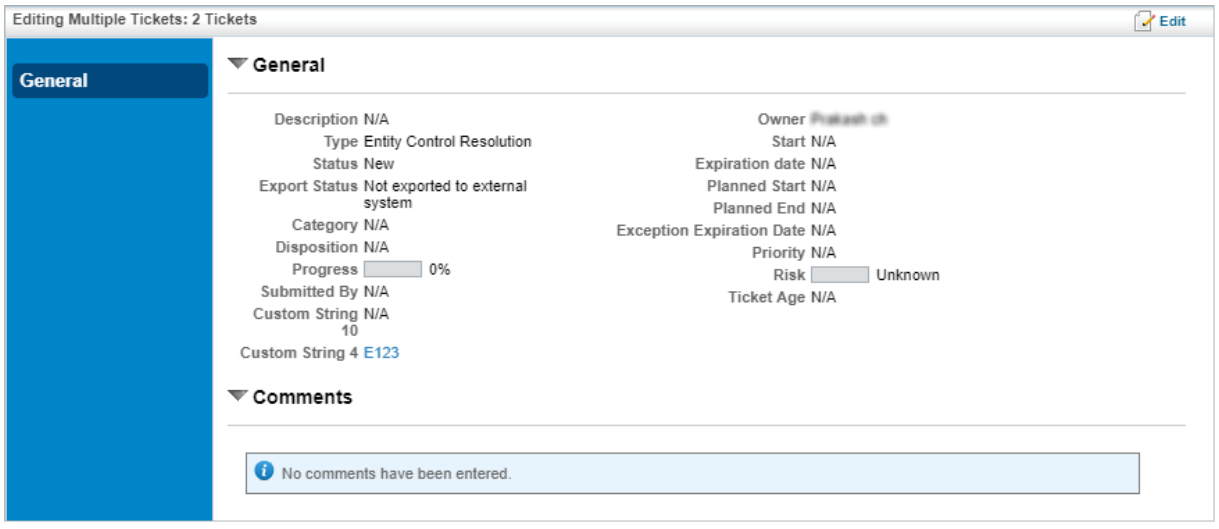
A maximum of 50 tickets can be selected for a batch edit.

4. Click the **More Actions...** dropdown menu, then click **Batch Edit Tickets** to open the **Editing Multiple Tickets** window.



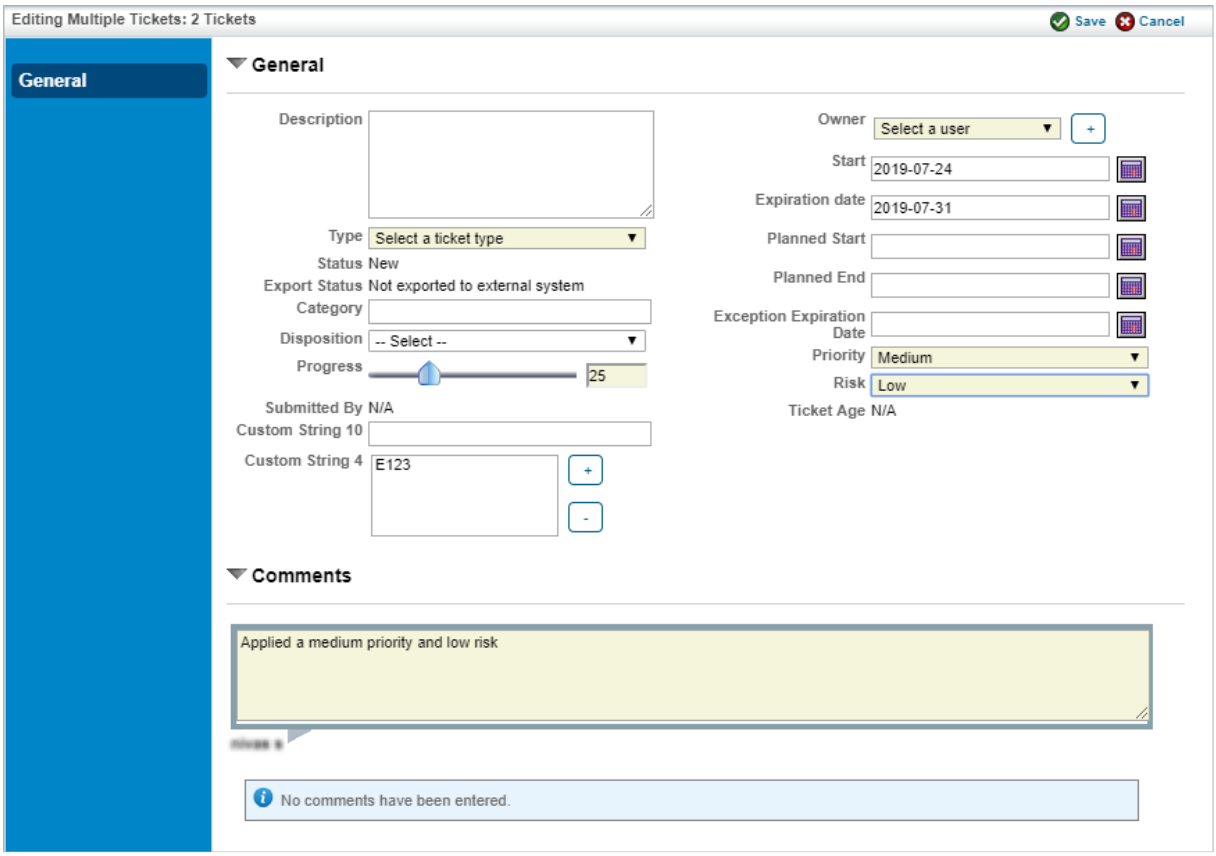
The Batch Edit Tickets option in the More Actions... dropdown menu.

5. Click **Edit** in the top-right corner of the window.



The Editing Multiple Tickets window.

6. Make changes to the fields and add comments as required.
7. Click **Save** when finished and refresh your browser to see your changes.



Editing the fields of multiple tickets.

About Exception Requests Page

The **Exception Requests** page is a grid consisting of both local and global exceptions in which you are a stakeholder. The operations that you perform in this grid depends on the permissions assigned to your role. You can use the **Exception Requests** page to perform one or more tasks as described below:

- Create a global exception
- Update the general information
- Transition the workflow
- View workflow history
- Enter additional comments in addition to the comments that you enter while transitioning the workflow
- Manage attachments
- Synchronize the changes made to the workflow of an exception
- Delete an exception

Local exceptions can be created in the Questionnaire window or Control Results tab of Assessment Details page. For more information, refer to *Questionnaire Responder's Guide*.

Request Global Exceptions

This section explains how to request global exceptions for entities that are out-of-compliance with a control or subcontrol and you want to override the questionnaire and check results in the compliance and risk scores. The RiskVision solution applies the exception to all assessments with the entity-subcontrol pair. Setting an exception at the control level propagates the override to the subcontrols. If the questionnaire contained a subcontrol only, the global exception applies. You can also create an exception for a finding to override the finding's risk score. In order to request an exception, you must have Exception View and Exception Request permissions.

To request Local exceptions, that is, exceptions for a particular assessment, use the questionnaire. Stakeholders can access the questionnaire from

Folder	Sub-Folder	
My Exceptions	By Stage	Review Sign-Off Closed
	By Type	Control Vulnerability
	My Exceptions Delegated To Others	
	My Undelegated Exceptions	
All Exception	By Stage	Review Sign Off Closed
	By Type	Control Vulnerability
	All Delegated Exceptions	
	All Undelegated Exceptions	

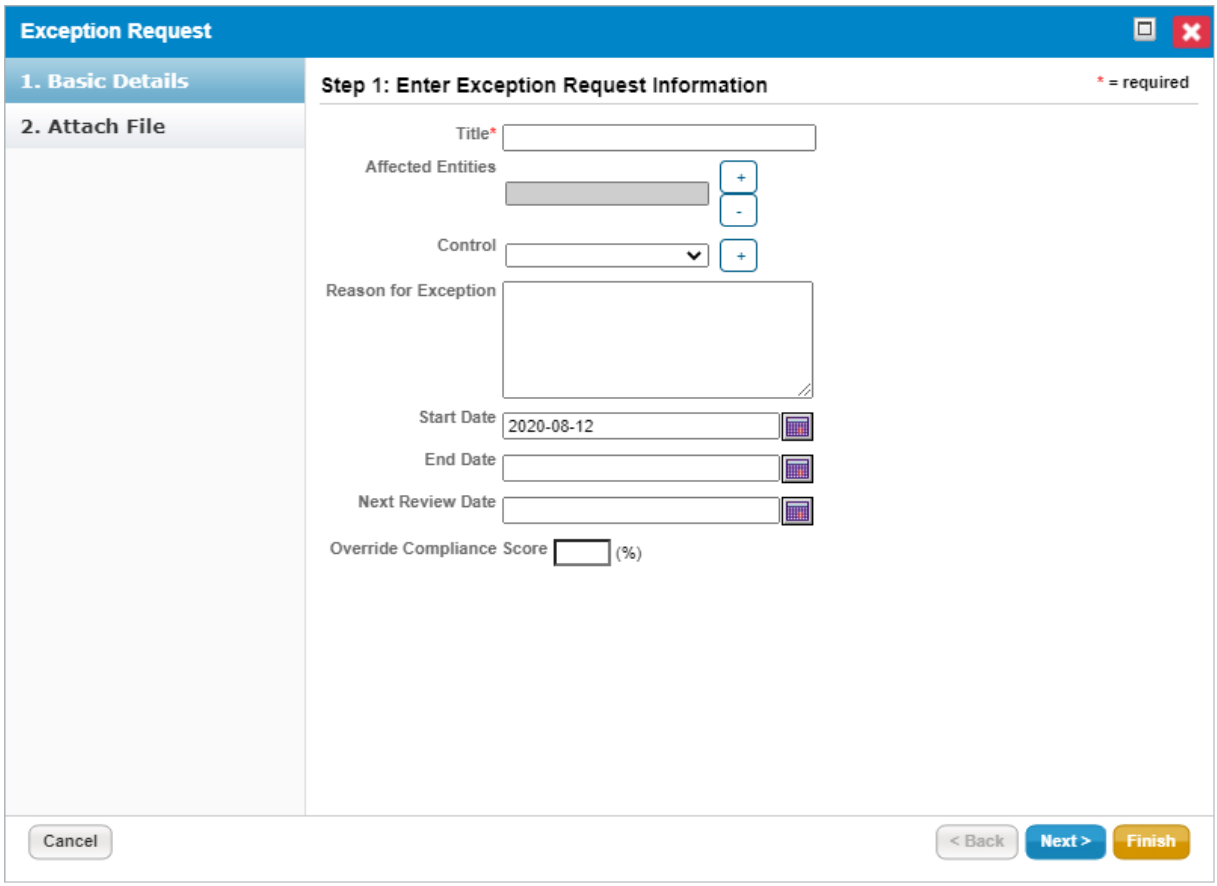
Note:

1. The folder name under the **By Stage** depends on the workflow stage names

2. All Exception folders are available only if users have the object Mange permission privilege.

To request an exception:

1. Go to **Home** > **Exception Requests.**
2. Click **New**. The **Exception Request** wizard appears.

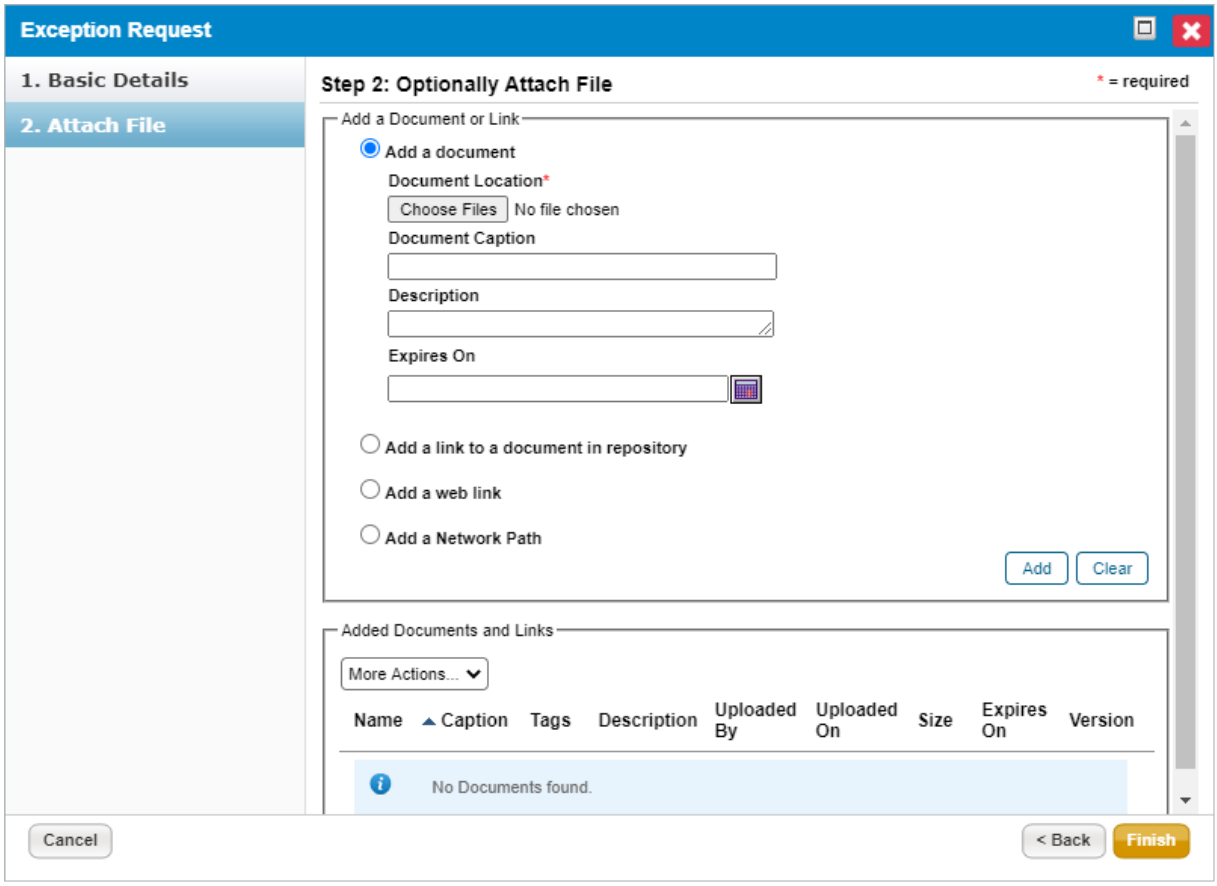


The Exception Request wizard.

3. In the **Basic Details** wizard page, enter the exception information. For more information, see Exception Request Basic Details.

4. Click **Next** to continue.

5. **Optional:** Add a document from your desktop, link to a document in the repository, or URL. For more information, see Exception Request Attachments.



The Attach File section of the Exception Request wizard.

If you cancel the attachment, it will appear to cancel the entire exception request. Wait a few moments and the exception request will appear without the attachment.

6. Click **Finish** to exit the wizard and to add an exception on **Home** > **Exceptions** page.

The exception has been created, but not requested. Go to the workflow page and submit the exception request. See Managing Your Exception Requests

R6 Report License

Resolver is preserving R6 Reporting for long-time RiskVision customers who have legacy reports in R6 Reporting that they have not been able to transition to RiskVision's JasperReports Server. As of Version 9.0, customers will need to request a license key with R6 Reporting enabled from Resolver Support.

The following table shows the differences in RiskVision's behavior when the R6 license is enabled:

FEATURE	WITH R6 LICENSE	WITHOUT R6 LICENSE
Menus Available in the Analytics Tab	• Analytics and Reporting • R6 Dashboards and Reports • R6 Charts • R6 Report Templates • R6 Report Status	• Analytics and Reporting
Configure UI Permission	Required for creating an R6 Custom Query chart.	Required to view and create R6 charts. Only table-type charts with custom queries can be created.
Enabled Properties	• To create R6 Charts, enable allowNewReport=true • To create R6 Dashboards and Reports, enable allowNewDashboard=true	• To create R6 table-type charts with custom queries, enable allowNewReport=true
Viewing R6 Charts, Dashboards, and Reports	Users can access R6 Dashboards and Reports, R6 Report Templates, and R6 Report Status.	• To view archived R6 Charts, enable showArchivedReports=true • To view archived R6 Dashboards and Reports, enable showDashboardPage=true
New Group and **Export Group** Actions	Users can select **New Group** and **Export Group** under **My Charts** and **My Dashboards**.	Users cannot execute **New Group** or **Export Group**.

The Analytics tab with an R6 License.

The Analytics tab without an R6 License.

Understanding Configurations

Any assessments you run in the RiskVision application involve various objects available on the **Configuration** menu. You must carefully examine each object to decide up to what extent you will need it and then configure only the required options to meet the essence of your assessment because you may want to choose a different strategy for each assessment. The below list describes the objects you will want to configure before the assessments are launched:

- **Workflows** - Choosing an appropriate workflow other than the default workflows is possible through the user interface of assessment and policy creation wizards. If you want an exception, ticket, finding, and incident to follow a different workflow pattern, other than the default workflows, you must configure the selection criteria within those workflows. For more information on workflows, see the following topics:
  - About Workflows
  - Modifying Stage Settings
  - Specifying Multiple Workflows
- **Escalation** - Escalations are meant for tickets that are left unattended past thier due date so that the requestor, owner manager, or both can be made aware of the situation. For more information, see Creating an Escalation Configuration and Managing Escalation Configurations.
- **Email Templates** - The objects that notify stakeholders of a particular event typically use an email template. Several default email templates are available for selection or are already in-place to handle the notifications. If your organization prefers to follow the standard procedure for all its internal communications, you must design an email template. For more information, see Configuring E-mail Templates.
- **Filters** - A filter contains a set of conditions used by reports to match records, and dynamic groups to limit membership, and to limit user access, among other things. Filter types include Assessment, Dynamic Group, Entity, Exception Request, Incident, Program, Response, Risk, and more. For more information, see About Filters.
- **Ownership Types** - Ownership types link workflow stage stakeholders to the system users who are assigned to an entity or policy. This allows processes such as programs, tickets, and policy pack approval to run automatically. You can restrict which user can be assigned as a type of owner based on the user's role assignment. For more information, see About Ownership Types.
- **Assessment Configuration, Entity Configuration, Findings Configuration, Vulnerability Risk Configuration, and Incident Configuration** - Depending on the RiskVision application, a common threshold range criteria can be established for assessment, finding, vulnerability, risk or incident objects. When assessments are run, the risk, vulnerability and incident scores are derived according to the default range. Before you run any assessment, ensure that the threshold range is configured according to the assessment objective and meets auditing guidelines and policies. For more information, see Configuring a Threshold Range for Risk, Vulnerability and Incident Scores.
- **Questionnaire Presentation Options** - Instead of provisioning too many options in the questionnaire UI, you may want to consider creating a new questionnaire presentation option so that responders quickly get rid of the questionnaire without bothering with the options which might be of no worth for an assessment type. For more information, see Setting Questionnaire Presentation Options.
- **Ticket Management Preferences** - Usually, tickets are escalated when they pass the due date. You can add a disposition to avoid sending the escalation. For more information on setting the ticket preferences, see About Ticket Management Preferences.

Workflows

A workflow divides compliance, risk and other related business processes into stages and allows you to pre-assign participants (stakeholders), define requirements for transitioning between stages, and automate run-time process controls and activities, such as sending e-mail notifications and updating status.

The workflow initiator, such as a program owner, manages their own workflow and performs actions like reassigning, adding stakeholders, and forcing a transition to another stage. To view workflows on the **Configuration** menu, you must have the Workflow View permission to create, update or modify a workflow stage, you must have the Workflow Update permission.

The following table lists the RiskVision default workflows. The type of workflow that you see on the **Configuration** > **Workflows** menu depends on the RiskVision application.

Type	Object	Description
Exception	Entities and/or Controls	Specifies the stages of approving or rejecting an exception to a control that is requested by a user taking a questionnaire or from the **Exceptions** page.
Assessment	Entities	Specifies the stages in the process of evaluating compliance of an entity or group of entities against a set of controls or gathering risk related information. Successfully launching a program initiates the workflow. Advanced: Workflow can allow questionnaires to advance workflow stages independently.
Ticket	Entities	Specifies the stages for reporting and tracking various types of required actions. Initiate the ticket workflow from an incident using the Remedy connector, and by manually creating one on the Ticket page.
Finding	Controls or Entities	Specifies the stages to perform the risk assessment to respond to a finding. Creating a finding on the **Home > Findings** page or on the **Control Results** tab or **Findings** tab of **Assessment Detail** page will launch the workflow.

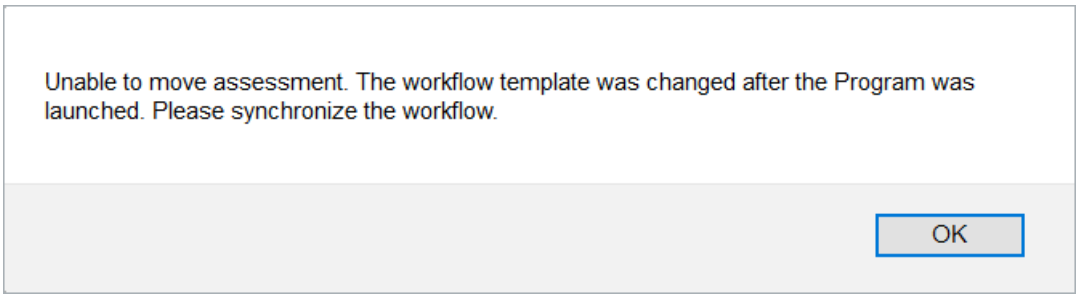
Modifying Stage Settings

This section explains workflow stage options. When you start a new process, such as an assessment or content pack development, RiskVision copies the selected workflow and creates a separate workflow instance that belongs to the process. Instances and workflow templates are related but require synchronization in order to have instances that are related to templates reflect the latest template modifications.

Users can modify templates if they have Workflow View and Workflow Update permissions.

For assessments, any change to the template alerts the program owner by displaying an informational message on the assessment details page. The owner can synchronize the workflow settings with the assessment workflow instances. This overwrites the instance settings with the new workflow settings.

For example, if the template has changed after an assessment has launched, the user will be unable to advance the workflow and will see the following message displayed:



Renaming The Stage

The stage name is displayed on the workflow pages of an assessment, policy, exception, ticket, incident, and so on. To change a stage name, select the stage and click **Edit**. Enter the new name and click **Save**.

- For assessment type workflows, you can only modify the stage name if there are no programs already in progress that use the workflow.
- For policies, exceptions, tickets, and incidents, the new workflow stage name appears if the process began after you completed the change.

Configure Stage Transitions & Actions

This article provides instructions on configuring the workflow transition and action options for the following objects:

- Tickets;
- Incidents;
- Exceptions;
- Findings; and
- Policies.

A stage transition moves the process from the current stage to another stage. The transition is typically associated with a user action, such as approve or reject. For Assessment workflows, the transition can also have questionnaire taking conditions. The stage transition options display as buttons on the workflow page.

By default, a workflow uses at least two actions in each stage. Since you may not need two actions on all occasions for each workflow stage, you may want to use the following properties so that actions can be selected depending on the context of need.

PROPERTY	DESCRIPTION
workflow.min.transitions=	Enter a number which specifies the actions in the workflow stage. If this property value is not set, the default value is 2, meaning there must be at least two transitions for every non-terminal stage.
workflow.max.transitions=	Enter a number so that you will have the choice to select more transitions when needed. By default the value is 4, meaning there can be no more than four transitions for every non-terminal stage.

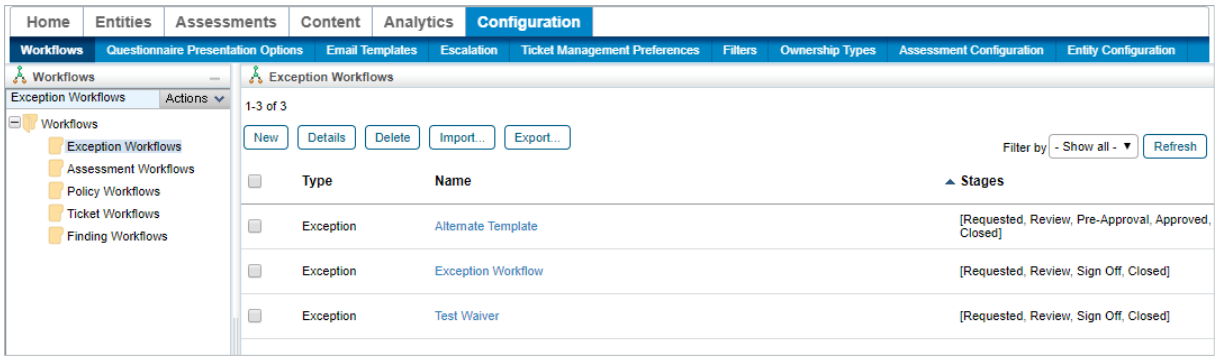
For example, if you need just one action in a workflow stage, you must set the `workflow.min.transition` property to 1 and `workflow.max.transitions` property to an appropriate value so that you can continue to select more actions in stages depending on the context of need.

Only users with **Workflow View** and **Workflow Update** permissions can modify workflows.

As of version 9.5, the `workflow.max.transitions` value for exception workflows will be the entered value plus 1. This extra transition will allow the workflow to expire.

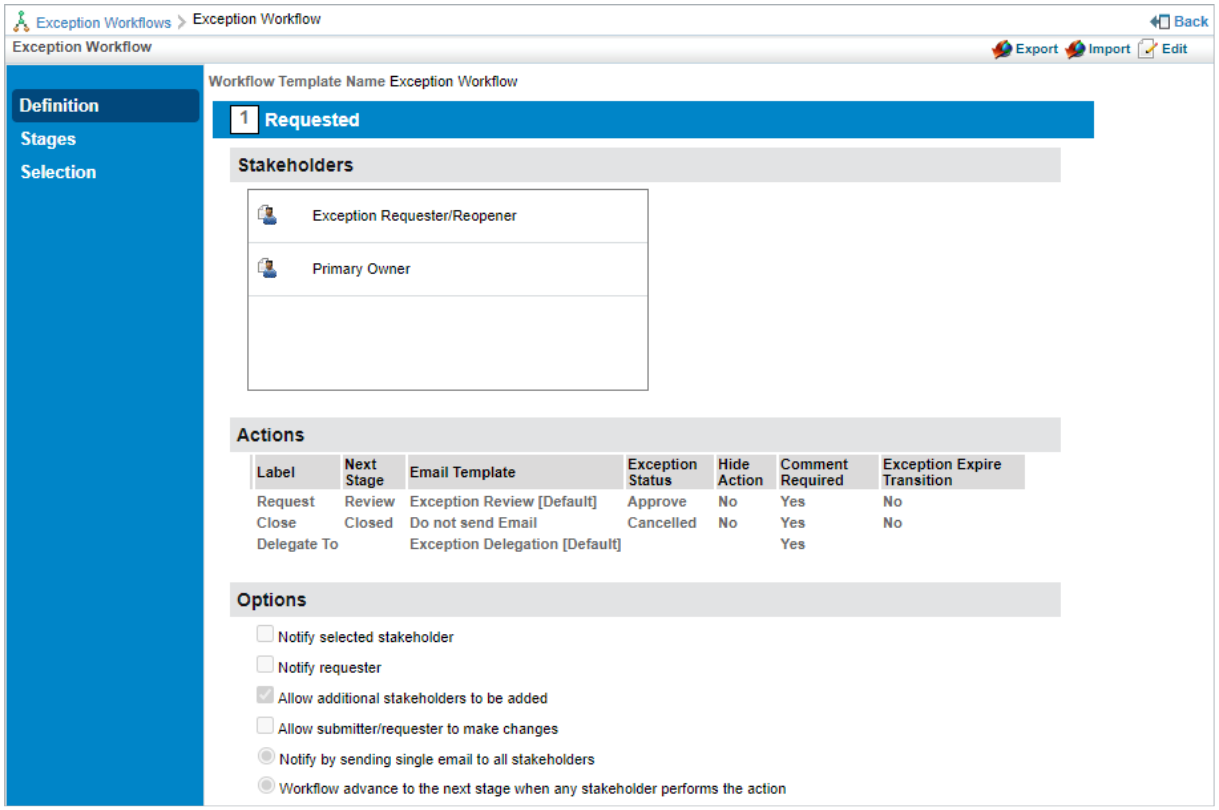
To configure a workflow's transitions and actions:

1. Click **Configuration > Workflows**.
2. Click a workflow on the grid to open the workflow settings. If needed, use the tree to the left or the filter dropdown menu on the far right to filter the results on the grid.



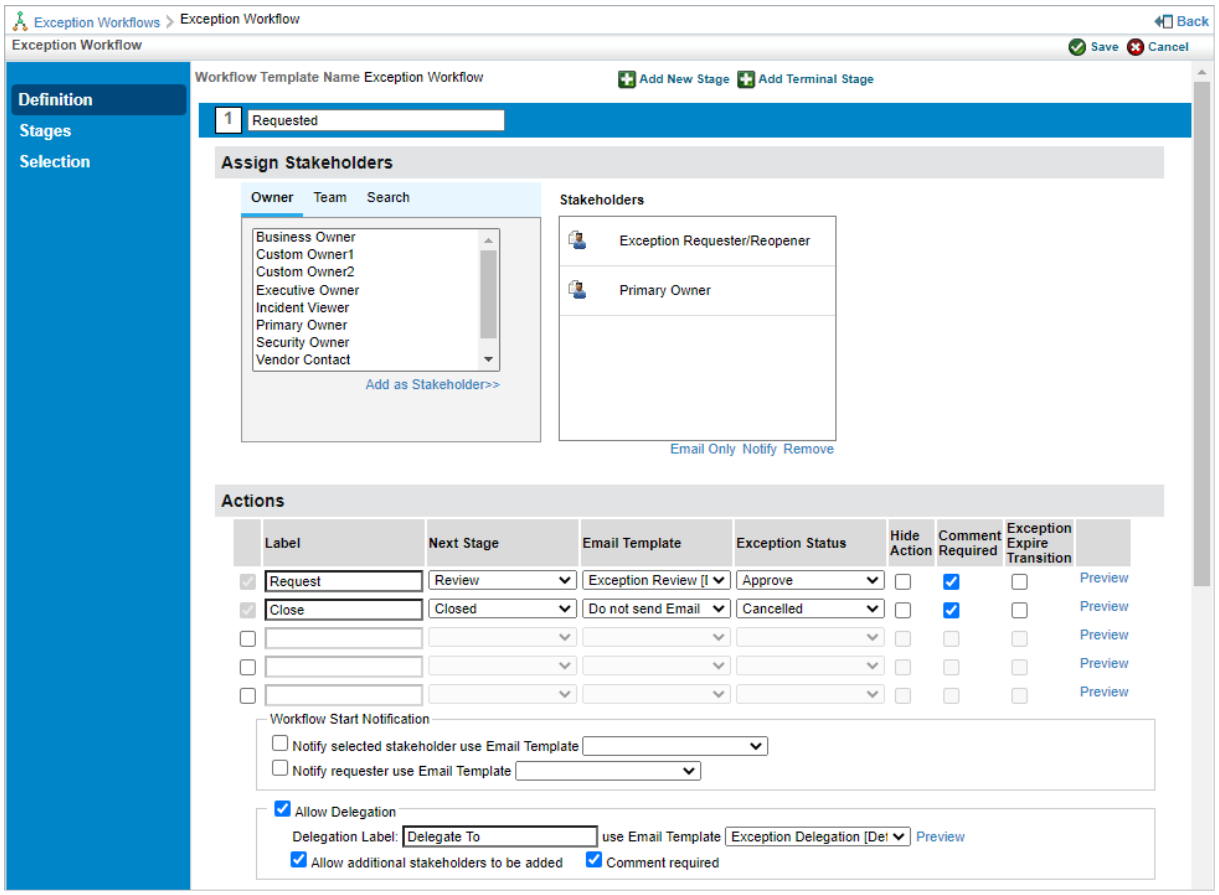
The Workflow settings in Configuration.

3. Click **Definition** in the pane to the left if it's not already selected.



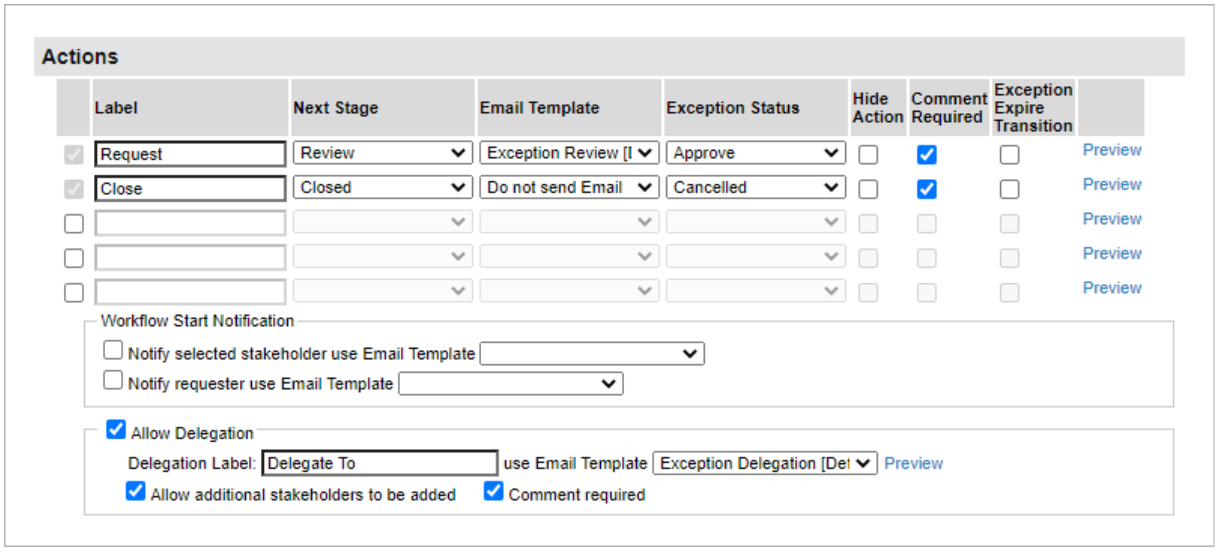
Workflow details.

4. Click **Edit** in the top-right of the workflow screen.



The Workflow edit screen.

5. Click a stage to display its **Actions** settings.
6. Enter a name for the stage in the **Label** text box. This is the label that will appear on the button that users click to move the object to another stage.

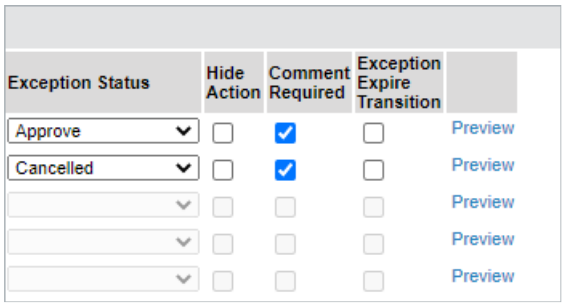


The Actions settings.

7. Select the stage the object will transition to from the **Next Stage** dropdown menu.
8. **Optional:** Select a template to define which email is sent to stakeholders when the notify settings are enabled. If you do not want an email sent, select **Do not send Email**
9. Enter a status for the object once it transitions in the **Status** field.

For exceptions, this field is a select list called the **Exception Status** field. Users will choose the appropriate status from a predefined list created on the Exception Management Preferences page. All other workflow types will have users enter in their own status values.

10. Select the **Hide Action** checkbox if the transition button should be hidden from end-users in the **Workflow** section of the object. This option is useful when the transition is automated and does not require any action from the user.
11. Deselect the **Comment Required** checkbox if the transition **does not** require end-users to enter comments in the **Workflow** tab before the object transitions. This checkbox is selected by default.



The Hide Action and Comment Required checkboxes.

12. **Optional:** Click **Preview** if you selected an email template in step 8 above and you wish to preview it.
13. Repeat steps 5 to 12 to modify the settings of additional stages as needed.
14. Click **Save** to save your changes.

Existing objects must be synchronized to reflect changes to the workflow settings. To synchronize, navigate to the objects (e.g. Home > Tickets) and select Synchronize Workflow from the More Actions... dropdown menu or open an individual object to synchronize it from the Workflow section.

Configuring Stakeholder Settings

A stakeholder is responsible for performing the actions defined in the workflow stage and can transition the process to another stage.

Assigning Stakeholders

You can include roles, specific users, and teams as stakeholders in every workflow stage.

Stakeholders assigned to workflow stages are classified into the following two categories:

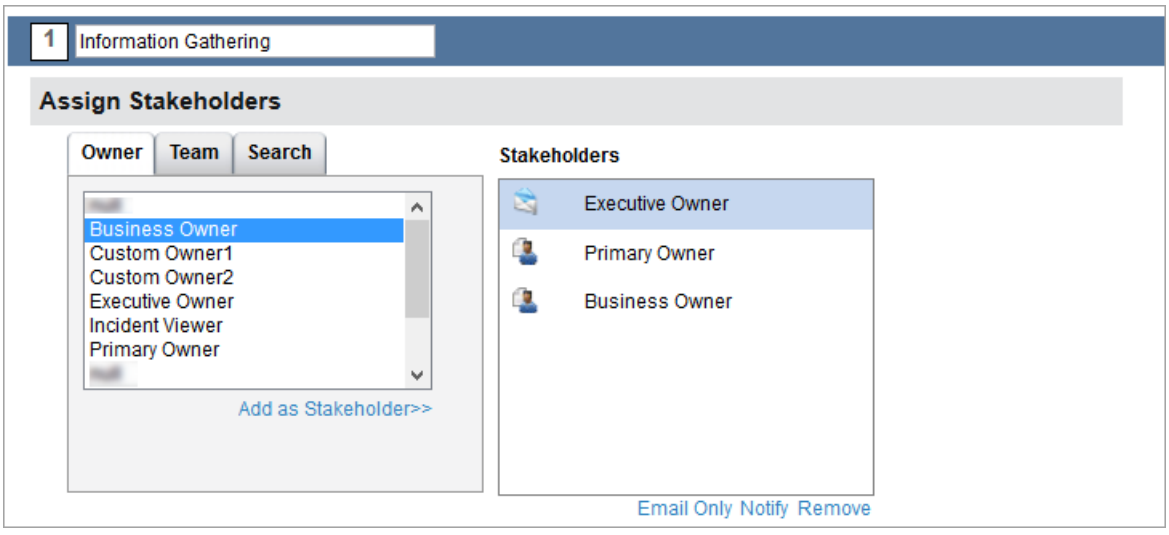
1. Task-performing stakeholders
2. Task-aware stakeholders

Task-performing stakeholders: This type of stakeholder performs different actions when the workflow enters a stage. By default, the stakeholders assigned to a workflow stage are task-performing stakeholders and have the icon next to their name.

Task-aware stakeholders: This type of stakeholder cannot perform any action when the workflow enters the stage. Notifications are sent to this type of stakeholder so that they are aware of the workflow progress. To assign a user, team, or owner as task-aware stakeholder, add the user as stakeholder first, then select the stakeholder and click **Email Only**. Task-aware stakeholders have the icon next to their name.

You must assign at least one task-performing stakeholder to every workflow stage. However, you can assign more than one stakeholder depending on your use case. The following table describes the selection options for assigning stakeholders to workflow stages:

Option	Description
Owner	Provides a list of ownership types. When selected, the user assigned to the Entity or Policy with the selected ownership type is automatically assigned as a stakeholder for the workflow stage.
Team	Provides a list of available teams.
Search	Allows you to search the User Directory to select users.



For assessment workflows, the program must be re-synchronized in order to add a stakeholder.

To assign stakeholders:

1. Open RiskVision Policy Manager.

2. Go to **Configuration** > **Workflows**.
3. Click the name of a workflow to open.
4. Click **Edit** at the top-right corner of the workflow details page.
5. Click a stage.
6. Perform one of the following options:
    - To add an ownership type as a stakeholder, click an owner type on the **Owner** tab.
    - To add a team as a stakeholder, click a team on the **Team** tab.
    - To add a user as stakeholder, click the **Search** tab, enter the search criteria, and click **Search**. Under **Search Results**, select the user.
7. Click **Add as Stakeholder**. The assigned stakeholders are indicated with a user icon next to their name.

If you have to assign a team in each workflow stage, ensure that the number of stakeholders in a team is less than 200. Otherwise, it may not be possible to advance a workflow stage when the workflow is assigned to an object such as policy, program, and so on.

To remove a stakeholder:

1. Go to **Configuration** > **Workflows**.
2. Click the name of a workflow to open.
3. Click **Edit** at the top-right corner of the workflow details page.
4. Click the stage to open its details.
5. Under **Assign Stakeholders**, select the stakeholder, and click **Remove**. To remove multiple stakeholders within a stage, press and hold **CTRL** button on your keyboard, click the stakeholders to select them, and click **Remove**. The stakeholder(s) is removed.
6. Click **Save**.

Allowing Stakeholders To Delegate

For each stage, except the terminal stage (closed), you can allow stakeholders to delegate their responsibility to another user or team. The delegate action adds the delegatee as a stakeholder and notifies them of their new task. The delegatee then acts as the original stakeholder.

To allow delegation:

1. Open a workflow for editing.
2. Open the stage.
3. Select **Allow Delegation**.
4. To change the label, enter the new button name.

5. Click **Save**. New workflow instances will be created from the revised template.

The Delegate label displays in drop-downs, questionnaire taking windows, and other process related places.

Workflow instances that are already in progress are not changed.

Allowing Stakeholders to Add Other Stakeholders

You can allow users to add stakeholders. New stakeholders must perform the requirements defined by the workflow stage. For example, if a stakeholder is added to the information gathering stage of an assessment, a questionnaire will be sent to them.

Stakeholders can add other stakeholders to workflow definitions, depending on permissions, but not to workflow templates. Synchronizing a workflow definition with its original workflow template will remove any additional ad hoc stakeholders.

If stakeholders are added to an assessment workflow definition, they will be automatically included the next time the assessment runs.

To allow stakeholders to add stakeholders:

1. Open RiskVision Policy Manager.
2. Go to **Configuration** > **Workflows**.
3. Click a workflow name to open. Click Edit.
4. Click a workflow stage to open.
5. Click **Allow Additional Stakeholders to be added**
6. Optional: To send an email when a stakeholder is added, click the name of an email template from the Notification dropdown.
7. Click **Save**. New workflow definitions will be created from the revised template.

Workflow instances that are already in progress will not be changed unless they are synced.

Send to Next Stage

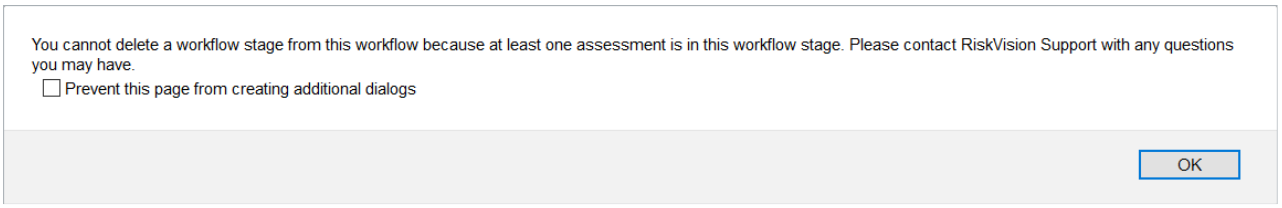
Assessment workflows have a 'Send to Next Stage' section with the following options:

Option	Description
Allow incomplete submission	Allow responders to submit the questionnaire even though all questions have not been answered.
Automatically move assessments to the next stage when all Questionnaires are complete	If checked, the workflow automatically advances to the next stage only when all the questionnaires have been completed and the user submits the questionnaire by clicking the 'Submit' link. This option works effectively when an assessment has only one questionnaire. In the case of multiple questionnaires, a workflow stage must have the branching capability.
Automatically submit Questionnaires that are answered by automated controls	If checked, automatically submits questionnaires that require no further input.

Deleting Workflow Stages

It is possible to delete a workflow's stage in the event it was created in error, or it is no longer needed. Once the stage has been deleted, it will no longer be possible to assign anything to that stage.

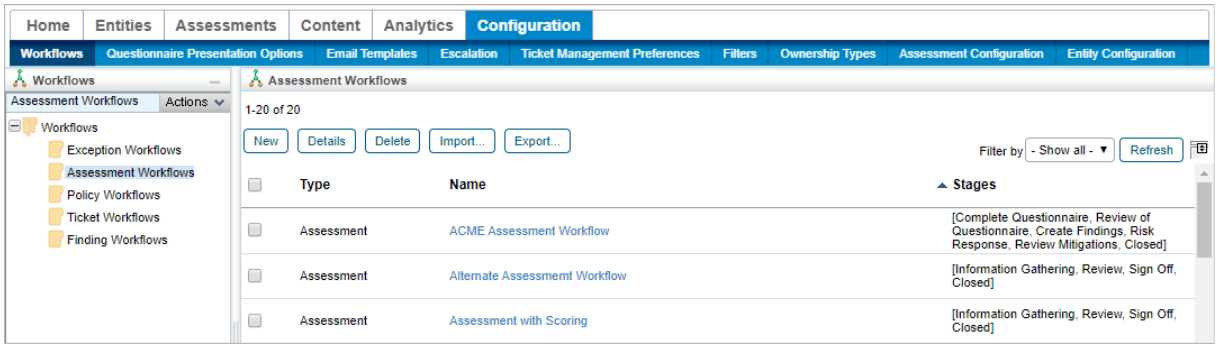
As of RiskVision version 9.3.5, assessment workflow stages can also be deleted. An assessment workflow stage can only be deleted if no assessments are currently assigned to it. Attempting to delete an occupied workflow will result in the following message being displayed: **"You cannot delete a workflow stage from this workflow because at least one assessment is in this workflow stage. Please contact RiskVision Support with any questions you may have."**



The error message displayed when a user attempts to delete a workflow stage with an assessment assigned to it.

To delete a workflow stage:

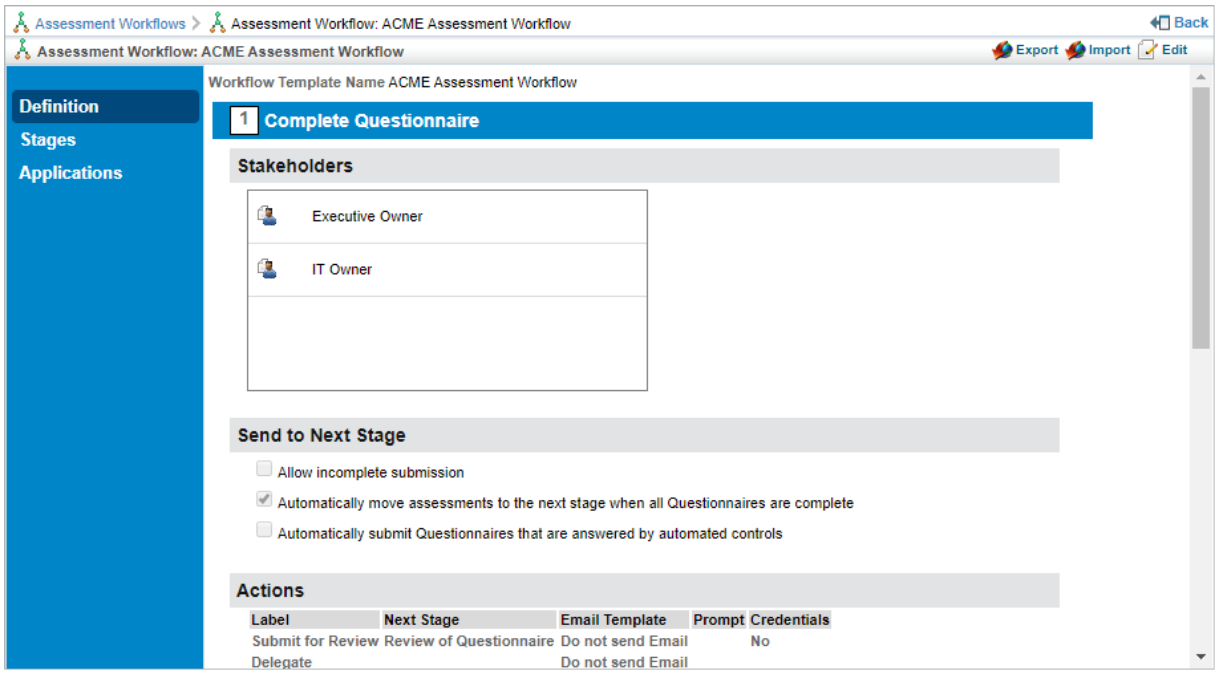
1. Navigate to **Configuration > Workflows**.



The Workflow settings in Configuration.

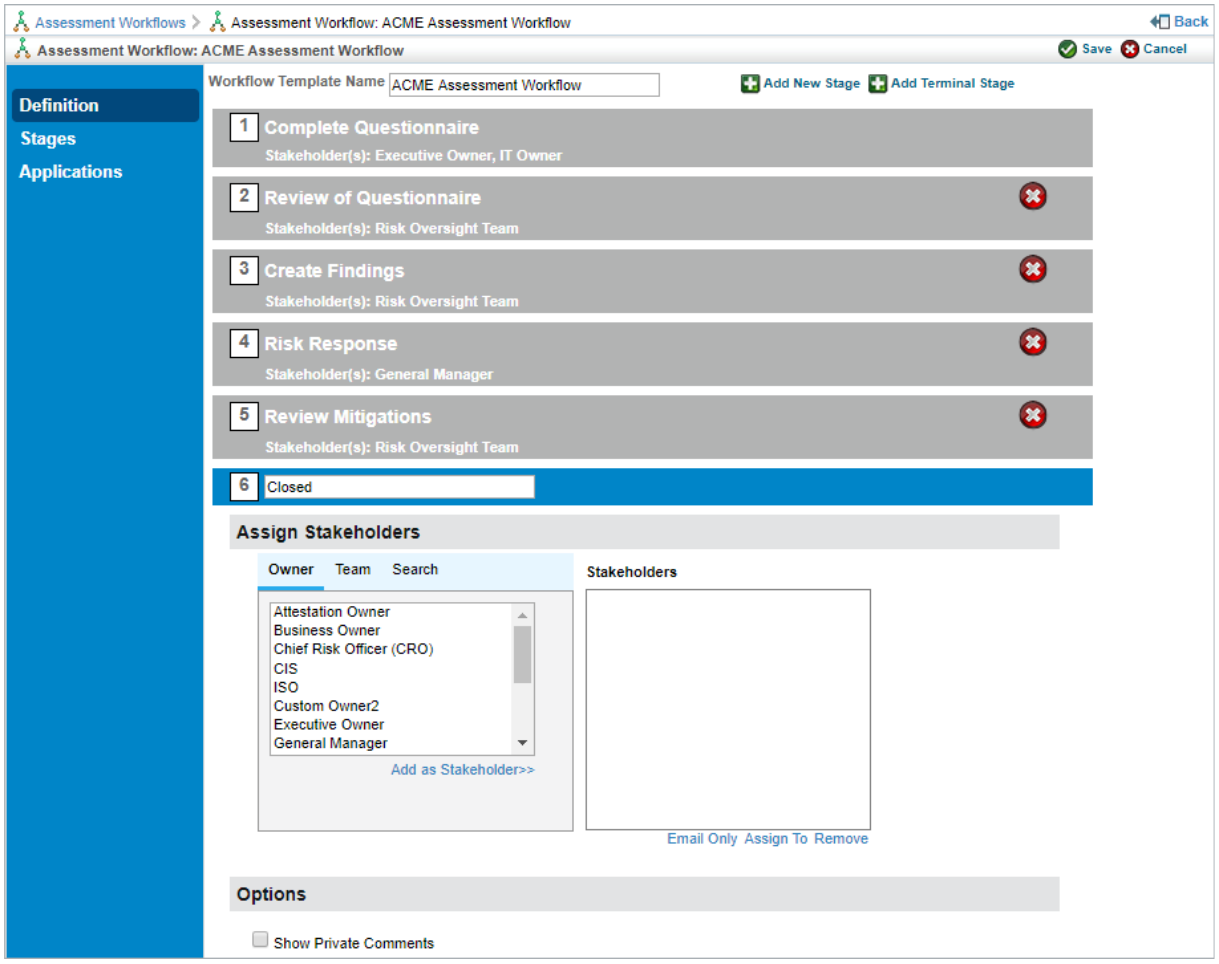
2. Click a workflow on the grid to open the workflow settings. If needed, use the tree to the left or the filter dropdown menu on the far right to filter the results on the grid.

3. Click **Definition** in the pane to the left if it's not already selected.



The Workflow Details page.

4. Click **Edit** in the top-right of the workflow screen.



The workflow edit screen.

5. Click the icon next to any stage to delete it.

6. Click **Save** to finalize your changes.

Other Stage Options

Assessment, Policy, Ticket, Incident,Finding and Exception workflow stages (except as noted) present the following additional options for advanced settings.

Option	Workflow Type	Description
Notify selected stakeholder	Ticket, Policy, Finding and Exception	Notify the stakeholder selected in this stage.
Notify owner	Ticket Finding, and Exception	Notify object owners regarding the object creation.
Allow submitter/requester to make changes	Ticket and Exception	If checked, the original submitter or requester can change the ticketor exception request. Note: • The workflow option has no bearing on the ticket's owner, who can always make changes to the ticket. • If a user has the object Manage permission or is a stakeholder then user will be able to make changes to the object regardless of whether the option is checked.
Allow additional stakeholders to be added	Ticket and Finding	If checked, allow additional stakeholders to add to the stage.
Allow owner to make changes	Finding	If checked, allow owners to make changes in the findings Note: • If a user has the object Manage permission or is a stakeholder, they will be able to make changes to the object regardless of whether the option is checked. • The workflow option should only be applicable if there are stakeholders mapped.
Add option	All	Click to add reminder and escalation options. For more information, see Sending Reminders and Escalations to Stakeholders
Notify by sending...	All	Notify by sending an e-mail to each stakeholder individually, or by sending a single e-mail to all stakeholders. For example, if a workflow stage has 2 normal stakeholders and 3 email, only stakeholders and the user select the below option: • **Notify by sending email individually to each stakeholder**: 2 emails are sent to normal stakeholders in TO list with no one on the CC list and 1 email is sent to email only stakeholders on the CC list with no one on the TO list. • **Notify by sending single email to all stakeholders**: 1 email is sent which includes 2 normal stakeholders in TO list and 3 email only stakeholders in CC list.
Allow each questionnaire to advance workflow stages...	Assessment only	Allow each questionnaire to advance independently, or require that all questionnaires must advance

		together. Specify "branch" and "join" stages that mark the beginning and ending of independent transition zones in a workflow. For more information, see Allowing Independent Stage Transitions.
Enable preferred user matching	Assessment only	If this option is checked, RiskVision will send questionnaires to preferred users. If a preferred user is not found for a particular entity, a related option specifies whether to send a questionnaire. For information about how to set up the preferred ownership, see Preferred Ownership.
Allow Control test authoring	Assessment only	If checked, respondents can author control tests.
Allow Control test evaluation	Assessment only	If checked, respondents can evaluate control tests.
Read Only Stage	Assessment only	Click and select to prevent modification of the entire questionnaire or answers. For more information, see Locking Answers in a Questionnaire.
Notify primary owner when assessment is accessed	Assessment only	If checked, sends the primary owner of the entity or asset an email when the assessment is accessed. For configuration steps, see Notifying Assessment Owner.
Show Private Comments	Assessment only	If checked, show private comments.
Allow all question scoring		If checked, allow all question scoring.
This is Review Stage		Check to indicate that the status of the current stage is in review.
Auto Advance after n days; Action		Advance the assessment workflow automatically using the specified action if it is still in this stage the specified number of days since the start.
Advance to the next stage when...	Finding, Ticket and Exception	Automatically advance to the next stage when any, all, or a specified percentage of stakeholders have performed the specified action

Sending Escalations and Reminders to Stakeholders

RiskVision Server allows you to send of escalations and/or reminders to stakeholders when a workflow does not move forward within a specified time. These notifications can be sent from any stage of any type of workflow. In each workflow stage, you can add a combination of up to ten reminder and escalation options. Escalations and reminders are sent based on different date fields for different objects. For example, a ticket workflow allows you to remind a ticket stage stakeholder *n* days before a ticket will expire. The available escalation and reminder options and the date types for different workflows are as follows:

WORKFLOW	ESCALATE/REMIND OPTIONS	DATE TYPES
Assessment	Remind Stakeholder, Escalate to program owner, and Escalate to stakeholder's manager	Due date, Recurrence date, Stage start date, and custom dates
Exception	Remind Stakeholder and Escalate to stakeholder's manager	Expiration, Start, Stage start date, and custom dates
Finding	Remind Stakeholder, Escalate to owner, and Escalate to stakeholder's manager	Last modified date, Stage start date, and custom dates
Incident	Remind Stakeholder and Escalate to stakeholder's manager	Due Date, Time Detected, Time Received, Stage start date, and custom dates
Policy	Remind Stakeholder, Escalate to owner, and Escalate to stakeholder's manager	Stage start date and custom dates
Ticket	Remind Stakeholder, Escalate to owner, and Escalate to stakeholder's manager	Created, Exception Expiration Date, End, Start, Planned Start, Planned End, Stage start date, and custom dates

Adding Escalations or Reminders

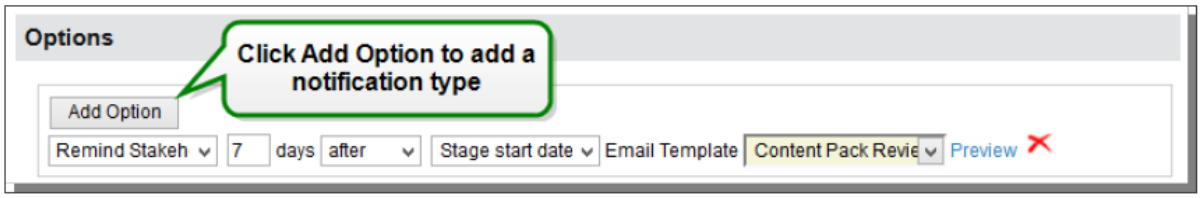
Most of the workflows in RiskVision Compliance Manager have default settings for escalation and reminder notifications within each workflow stage. The default settings are provided based on the real and practical use cases. The default reminder and escalation settings for each stage in different workflows are given in the table below:

Workflow	Stages	Default Option Settings
Assessment	Stage 1, Stage 2, Stage 3	Remind stakeholder 7 days after the workflow stage start date using the Questionnaire Reminder email template
	Stage 4	No reminder and escalation options
Exception	Stage 1	No reminder and escalation options
	Stage 2 and Stage 3	Remind stakeholder 7 days after the workflow stage start date using the Exception Reminder email template
Incident	Stage 1, Stage 2, and Stage 3	Remind stakeholder 7 days after the workflow stage start date using the Incident Reminder email template
Policy	Stage 1, Stage 2, and Stage 3	Remind stakeholder 7 days after the workflow stage start date using the Policy Reminder email template
Ticket	Stage 1, Stage 2, and Stage 3	Remind stakeholders 7 days after the start date with the Ticket Reminder email template

You can add more escalation and/or reminder options if the default settings mentioned above do not fulfill your criteria.

To add an escalation or reminder option:

1. In the RiskVision, go to **Configuration** > **Workflows**. The **Workflows** page is displayed.
2. Select the workflow to open its details page.
3. Click **Edit** at the top-right corner of the details page.
4. Click the workflow stage in which you will want to add an escalation or reminder. The details are displayed.
5. Under Options, click Add Option. A new option is added.



6. In the first drop-down list, select the reminder or escalation option.
7. Enter a number in the days field.
8. In the second drop-down list, select one of the following: **on**, **before**, and **after**.
9. In the third drop-down list, select a date type.
10. In the fourth drop-down list, select an email template to notify users for reminder or escalation purposes.

Editing Escalation and Reminder Settings

You can edit escalation and reminder options one at a time by changing the previously set values.

To edit an escalation or reminder:

1. In the RiskVision application, go to **Configuration** > **Workflows**. The **Workflows** page is displayed.
2. Select the workflow to open its details page.
3. Click **Edit** at the top-right corner of the details page.
4. Click the workflow stage in which you will want to edit escalations and/or reminders. The details are displayed.
5. Change the value or select the value in the row corresponding to the reminder or escalation option.
6. Click **Save** after editing the escalation and/or escalation options.

Deleting Escalations and Reminders

You can choose to delete an escalation or reminder notification in as many stages as you want when you no longer need to notify your stakeholders. Navigate to each stage within a workflow and delete the escalation and reminder options.

To delete escalations and reminders:

1. In the RiskVision Compliance Manager, go to **Configuration > Workflows**. The **Workflows** page is displayed.

2. Select the workflow to open its details page.

3. Click **Edit** at the top-right corner of the details page.

4. Click the workflow stage in which you will want to delete escalations and/or reminders. The details are displayed.

5. In the reminder or escalation option row, click . The option is deleted.

6. Repeat step 4 and step 5 to delete escalation and/or escalation options in other stages.

7. Click **Save** after deleting the escalation and/or escalation options.

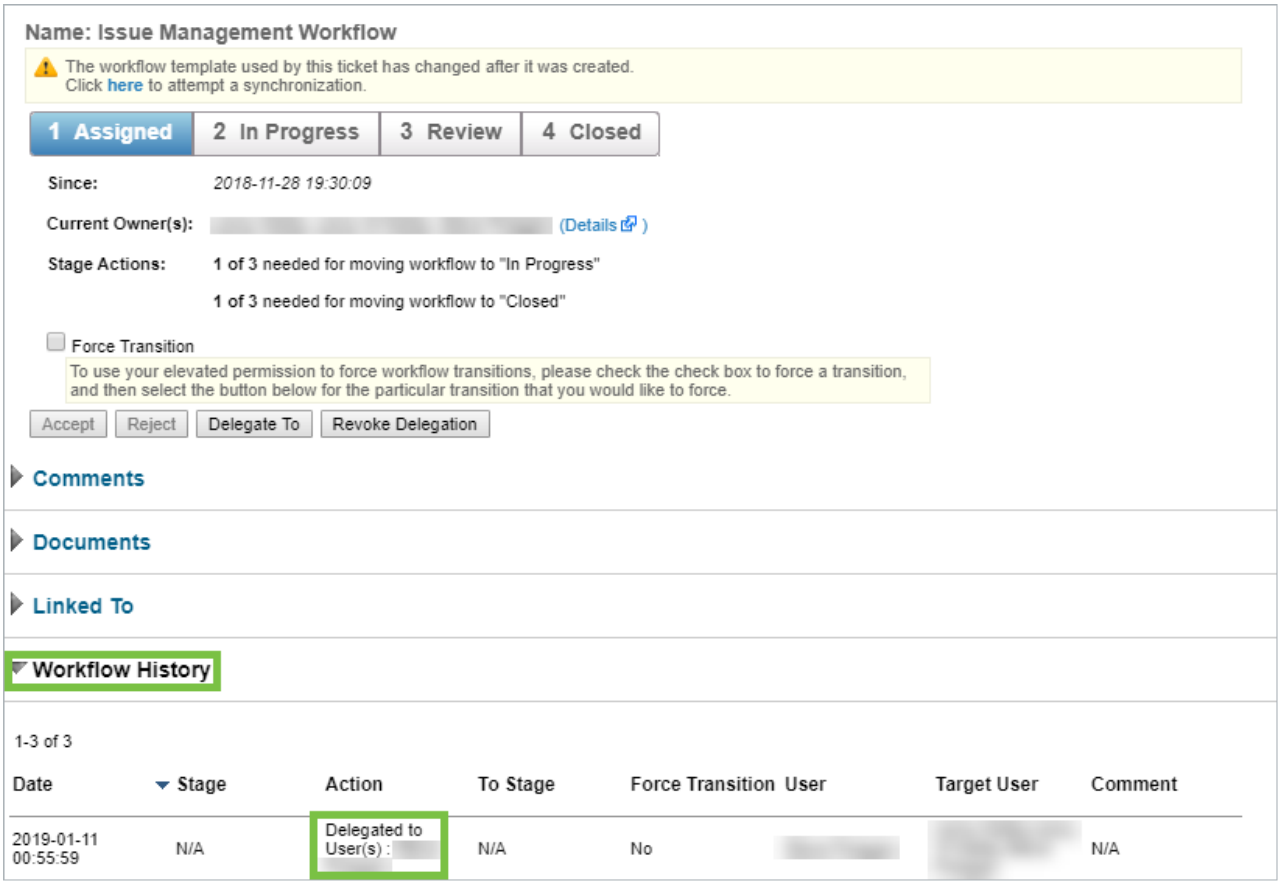
Sending Reminders and Escalations to Task-aware Stakeholders

By default, the configured reminder and escalation options are sent only to the task-performing stakeholders and not the stakeholders who receive emails only and cannot transition workflows. However, if you want to copy task-aware stakeholders on all of the reminder and escalation notifications, then you can add the **com.agiliance.reminderOrEscaltions.notifyEmailOnlyUsers** property to the **agiliance.properties** file and set it to true. When this property is added, the reminder and escalation notifications are sent out to task-aware stakeholders for all stages and workflow types. For information about task-aware and task-performing stakeholders, see Assigning Stakeholders.

Delegation & Delegation Revocation

Users with Manage permissions on an object can read, create, modify, and update instances of that object. These users can also delegate, revoke delegation, and force workflow transitions. Workflow stages can be delegated to any RiskVision user or team. In order to delegate a stage in the workflow, delegation must be enabled. Delegation and delegation revocation is controlled on a per-stage basis by the **Allow Delegation** option.

It's good practice to add a comment/reason for delegation or revoking delegation in the **Comment** section. The comments added are visible to all users who have read access to the Workflow tab of the object and can view the comments in the **Workflow History** section as show below.



The Workflow History section of a delegated workflow.

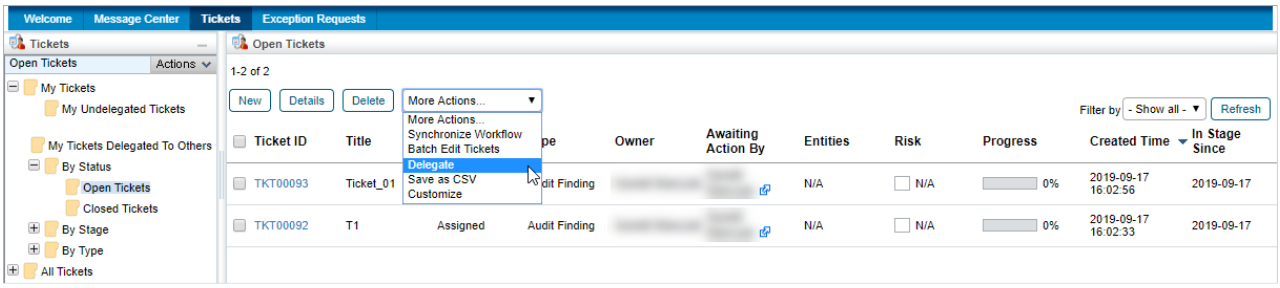
The delegation option that is discussed in this section is available for the below objects:

> Not all of the below objects will be available in each application.

- Tickets
- Findings
- Incidents
- Exception Requests
- Controls
- Policies

For **Tickets**, **Findings**, **Incidents** and **Exception Requests**, workflow stakeholders can view delegated objects in the **My Tickets Delegated To Others**, **My Findings Delegated to Others**, **My Incidents Delegated to Others** and **My Exceptions Delegated to Others** column of their respective grids.

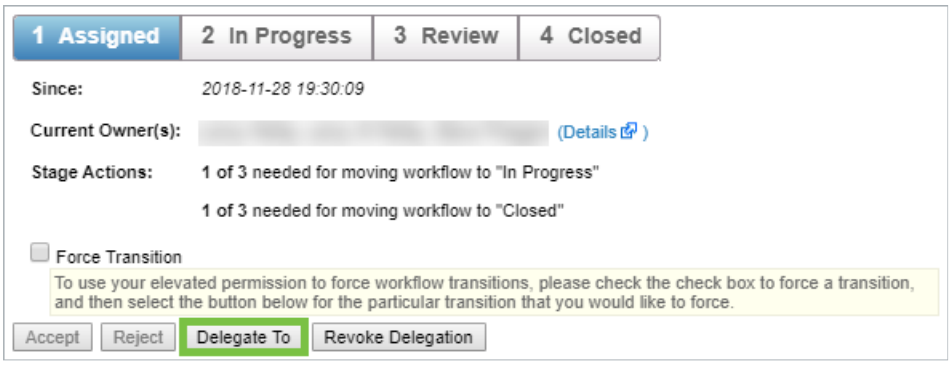
For **Tickets**, **Findings**, **Incidents**, and **Exception Requests,** stakeholders can perform bulk delegation and delegation revocation from the **More Actions** dropdown list.



The Delegate option in the More Actions dropdown.

Delegation

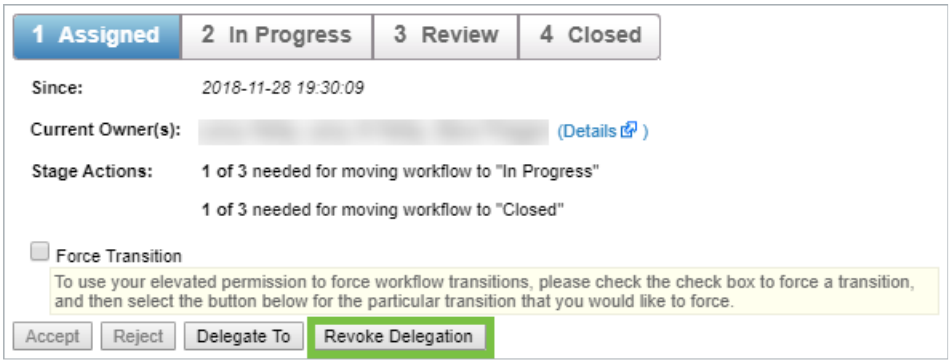
Any stakeholder of a stage that permits delegation can delegate to another user. The workflow designer can allow team Delegation at each stage. For example, the **In Progress** and **Review** stages may allow for delegation, whereas the **Approval** stage might be designed not to allow delegation. The workflow designer can choose another label to describe delegation, such as "Delegated To" or "Transfer Authority" and can select an email template used to notify the delegate.



The Delegate To button.

Delegation Revocation

The original stakeholders can revoke a delegation at any time, regardless of how many times delegation has occurred. This is true regardless of whether the current delegate is the original delegate.



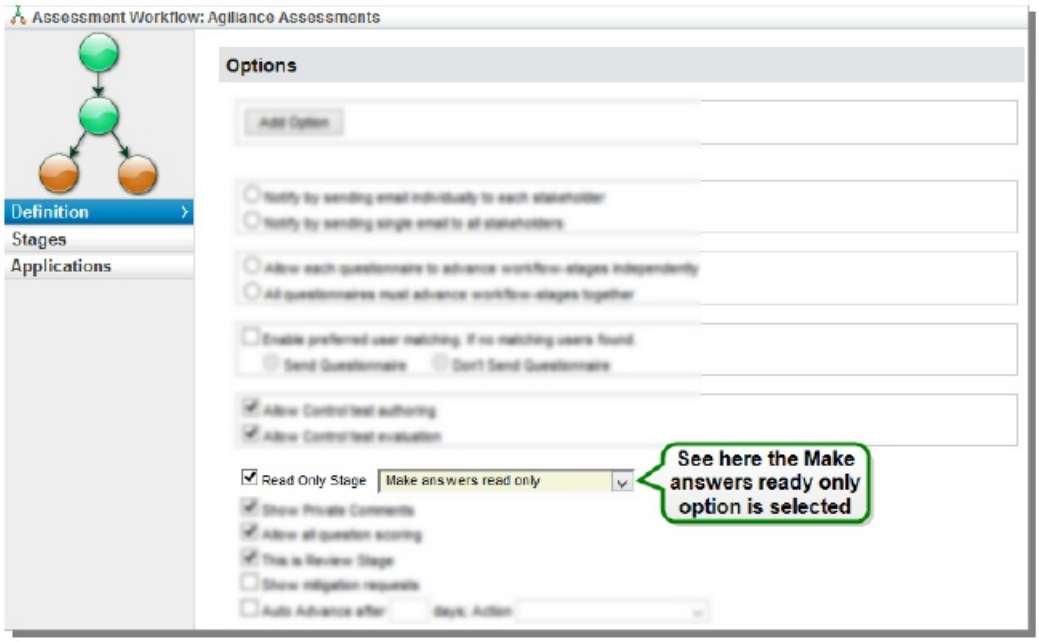
The Revoke Delegation button.

Locking Answers in a Questionnaire

The Assessment workflow type allows you to put a questionnaire in read-only mode while the workflow is in certain stages. Stages after the first stage of the assessment workflow can be designated as a "Read Only Stage." When setting a stage as a Read Only Stage, you have two options: "Make the entire questionnaire read only" and "Make answers read only." Whether you select the Read Only Stage option, and which Read Only Stage option value you choose will depend on how much freedom you want to give workflow stakeholders that are not the users who are responsible for answering the questions to change assessment data. If you want to allow reviewers and approvers to add evidence, comments, and other information, you will choose to make answers read-only. If you don't want to allow this, then you will choose to make the entire questionnaire as read-only.

To lock answers in a questionnaire:

1. In the RiskVision application, go to **Configuration** > **Workflows**. The **Workflows** page appears.
2. Under the **Workflows** tree on the left-hand side, select the **Assessment Workflows** group. The Assessment Workflows appear.
3. Select the workflow to open its details page.
4. Click **Edit** at the upper right-hand corner of the details page.
5. Navigate to the stage of interest, excluding stage one.
6. Under **Options**, check the box next to the Read Only Stageoption, and select **Make answers read only** in the drop-down list.



7. Repeat step 5 and step 6 if you have to put answers in ready-only mode in other stages of the workflow.
8. Click **Save** at the upper right-hand corner of the details page.

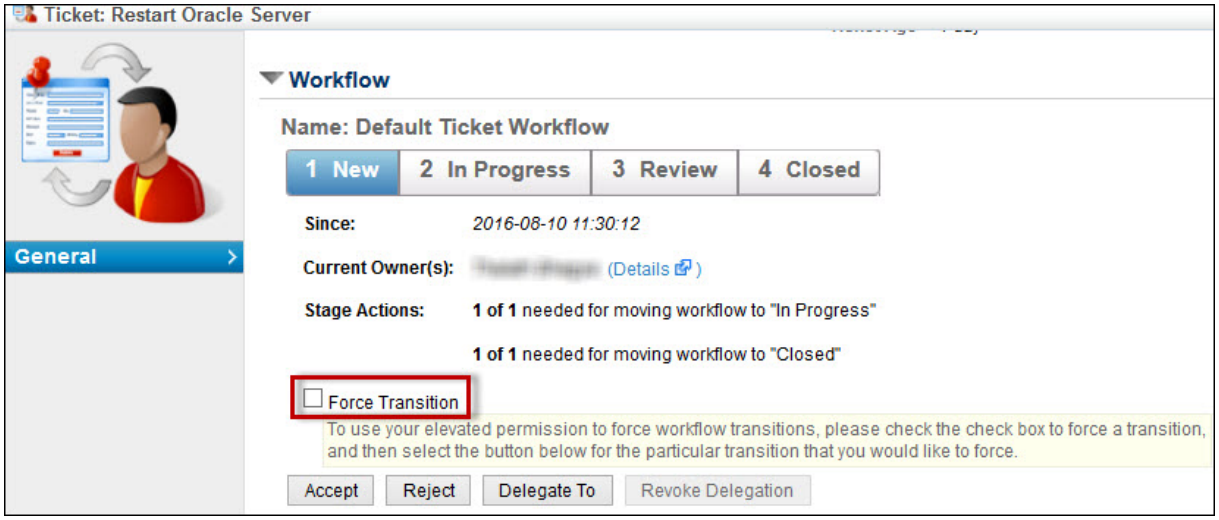
Forcing Stage Transition

Any user with appropriate permissions can force the stage transition of a workflow, for objects such as tickets, exceptions, findings, or incidents, when the stage stakeholder do not transition the workflow to the next stage in time. Forcing the stage transition in a policy workflow requires that the user own the policy. That is, only a primary owner can force the transition. When a workflow stage is set to advance automatically to the next stage at a specified percentage or any or all of the stakeholders have performed a certain action, force transition will facilitate moving the stage even though the specified trigger may not have been achieved. The following table lists the objects and the permission or ownership criteria required to force a stage transition.

Object	Criteria
Ticket	Manage permission
Exception	Approve permission
Incident	Manage permission
Finding	Manage permission
Policy	Primary ownership

To force a stage transition:

1. Select the object to open its details page.
2. In the **Workflow** section, check the box next to Force Transition, and click the desired action to complete the transition.



Determining Stage Transition Mode

Users can transition the workflow stage if they are the stage stakeholder, or if they possess the ownership or appropriate permissions. The **Workflow History** section shows how ticket, exception, incident, and policy workflow stages were transitioned and by whom.

The **Force Transition** column indicates whether the transition was forced and the **User** column displays the stakeholder who completed the transition or action.

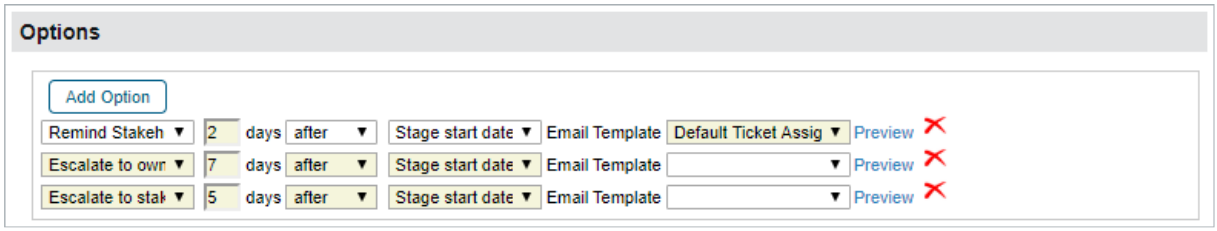
The Workflow History section.

Managing Workflow Escalation

Workflow stages can be configured to send escalations to the program owner, the stakeholder's manager, or both, for further action if the workflow does not advance to the next stage within a specified time. Each workflow stage can be configured separately with a number of days before automatic escalation. For example, you might configure a compliance assessment workflow to notify the program owner seven days after a questionnaire enters the Review stage. The notification email will use the Questionnaire Escalation template, and will only be sent if the questionnaire stays in the Review stage for more than seven days.

To configure escalations in a workflow:

1. Go to **Configuration** > **Workflows**, select a workflow, and then click **Details**.
2. Click a workflow stage, then click **Edit**.



The Options section.

3. Check the **Escalate to owner** or **Escalate to stakeholder's manager** to send notifications.
4. Enter the number of days, the date, and whether it should be sent before, after, or on the date.
5. Select the email template from the dropdown list to use for the notification. You have the option to send notifications to both the program owner and the stakeholder's manager.
6. Click **Save**.

If the ticket does not have an owner, configuring a ticket workflow for the escalate to owner option will not send notifications to a recipient. In a Policy workflow, selecting the **Escalate to Owner** option sends a notification to the policy's primary owner. If a stakeholder does not have a a manager, **Escalate to stakeholder's manager** will not send a notification.

To assign a manager to a stakeholder:

1. Open the RiskVision Administration application.
2. Click the **Users** tab.
3. Click the stakeholder's username to open their account.
4. Click **Edit**.
5. Click the **Manager** dropdown and select the appropriate user.
6. Click **Save**.

Notifying Assessment Owner

To notify the assessment owner, the stakeholders must access the assessment at the first stage of the workflow. If you are a program owner and want your assessment owners to receive notifications, you must perform the following steps before you create a program:

1. Go to the `%AGILIANCE_HOME%\config` directory, open the `agiliance.properties` file by using a text editor, and add the following properties:
    - `notify.assessment.owner.enabled=true` - set this property as 'true' to enable the effect of **Notify primary owner when assessment is accessed** option.
    - `com.agiliance.assessment.surveystart.notifyowner.emailTemplate=` - specify the email template's name with which you will want to notify stakeholders when a questionnaire is accessed first.
2. Restart the Tomcat application server to update to the latest changes.
3. Once the Tomcat application has restarted, open the assessment workflow details. Click **Edit** to bring the workflow into edit mode, scroll down to the details of the first stage, and select the box next to the **Notify primary owner when assessment is accessed** option.

When assessments are accessed for the first time, a notification is automatically sent to the primary owners of the respective assessments.

Specify Multiple Workflows

RiskVision allows you to switch between workflows. Different workflows can be selected based on the actual value of the runtime property. This is particularly useful for tickets, exceptions, and incident workflows. Multiple workflows allow you to create a fast track ticket workflow. For example, with a single workflow, a ticket would always use the default ticket workflow.

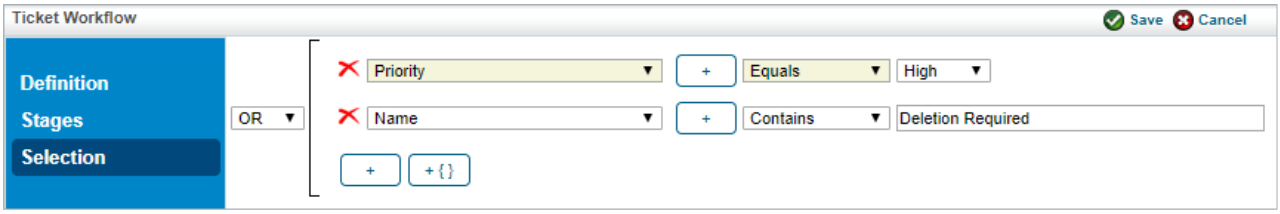
You can specify conditions under which the new workflow will be used in the **Selection** tab.

To define a selection condition:

1. Open a workflow that will be selected under certain conditions. Workflows without selection criteria will be selected by default, as before.

2. Click the **Selection** tab, then click **Edit**.

3. Select an attribute, operation, and value. For example, Priority Equals High.



The Selection tab in Edit mode.

4. Click **Save**.

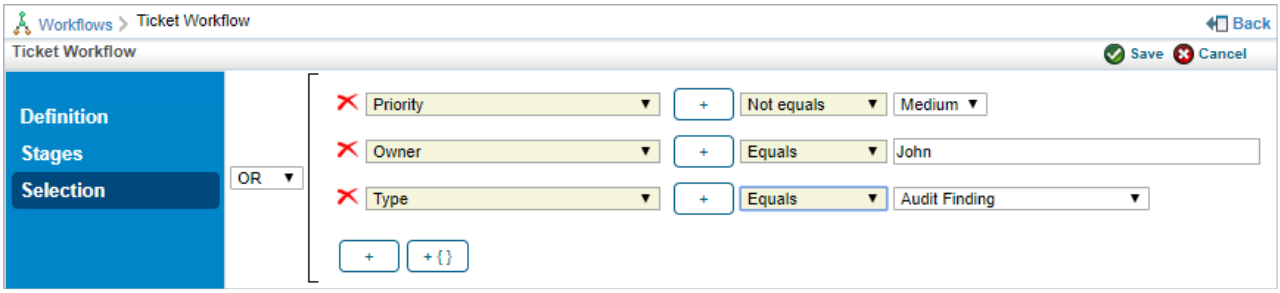
You can import the selection criteria of workflow templates created in RiskVision version 6.0 SP2 or higher.

Defining More Complex Selection Conditions

The Selection Criterion editor can be used to specify complex AND and OR conditions. In addition, parentheses can be used to specify sub-conditions.

For example, if you create three conditions, such as **Priority** =/= **Medium**, **Owner** = **John**, and **Type** = **Audit Finding**, you can choose:

CONJUNCTION	DESCRIPTION
AND	All conditions must be true to select this workflow.
OR	This workflow will be selected if any of the conditions are true.
XOR	Exclusive OR. Select the workflow if one of the conditions is true, but not if more than one is true.

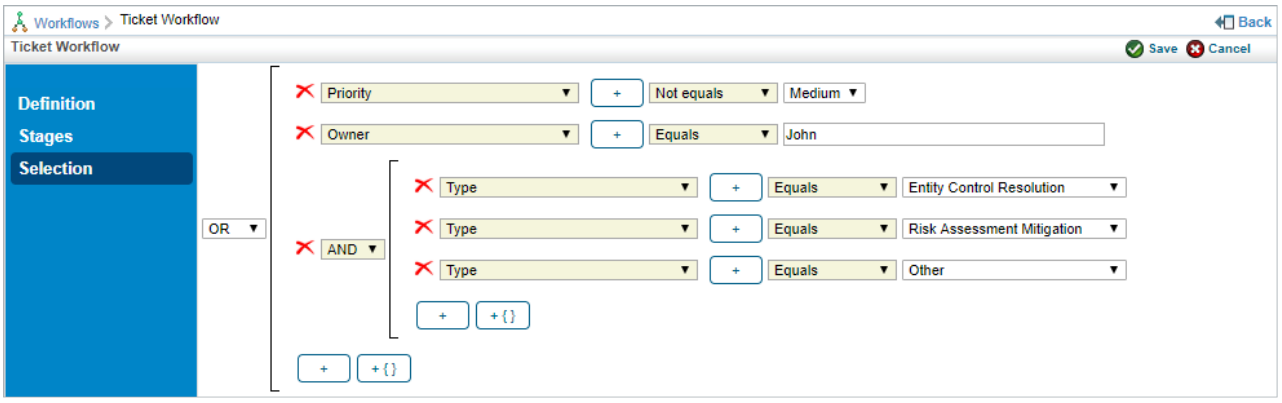


The Selection Criterion editor.

Specifying Sub-Conditions

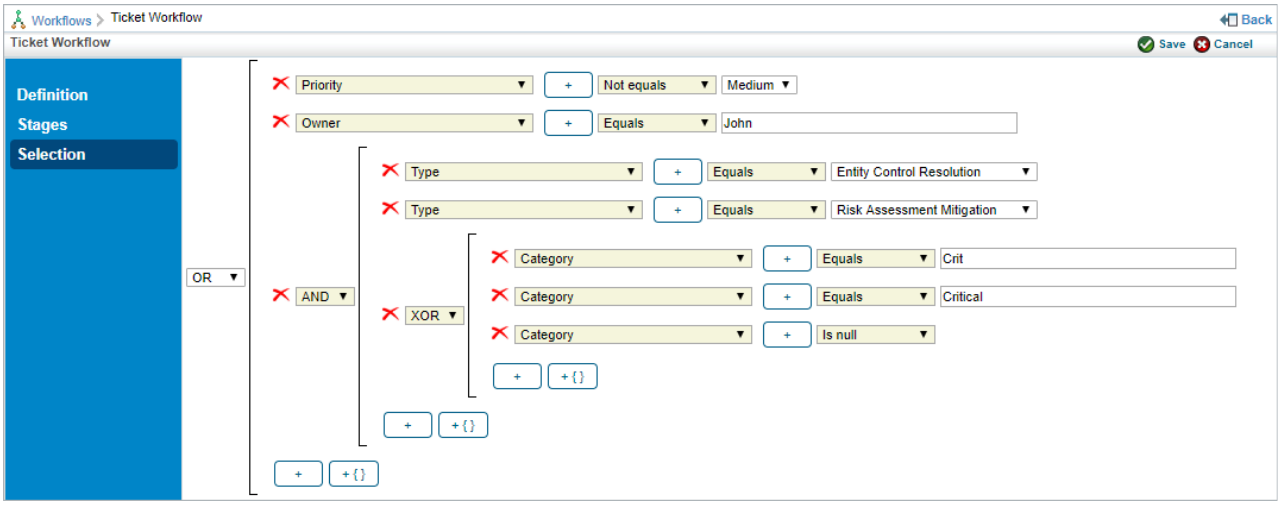
EXAMPLE

You want to select this workflow when **Priority** > **Medium**, when **Owner** is **John**, or when **Type** is **Entity Control Resolution**, **Risk Assessment Mitigation**, or **Other**. To specify the last three sub-conditions, you use the **+ { }** button.



The Selection Criterion editor with sub-conditions.

Sub-conditions can be nested as deeply as necessary. The **OR** and **AND** of the first example might be inverted. You might want to select the workflow when **Priority > Medium** AND when one of a set of sub-conditions is true.



The Selection Criterion editor with two layers of sub-conditions.

In the previous example, the workflow will be selected only when **Priority** does not equal **Medium**, the **Owner** is **John**, and one of the following conditions is true. Either the **Category** is **Null**, it starts with **Crit**, or it ends with **Critical**. If the **Category** starts with **Crit** and ends with **Critical**, the workflow will not be selected because you used the Exclusive OR (**XOR**) operator.

Allowing Independent Stage Transitions

Questionnaires associated with an assessment can advance through workflow stages independently (although entities under assessment can be in different workflow stages, questionnaires had to transition workflow stages in unison in RiskVision solution before 4.1.version.)

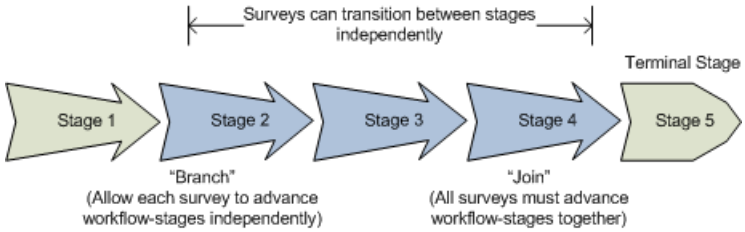
By default, questionnaires advance through workflow stages together. Questionnaires all start in the first stage of a workflow ("Information Gathering," for example) and must reach the Terminal stage together.

Relationships with a set of standard workflow templates, including " Assessments with Branching," which supports independent stage transitions. In addition, you can create custom templates that allow independent stage transitions, also known as branching.

Creating Workflows With Branching

Workflow stages have actions that transition questionnaires to different workflow stages. Typically, questionnaires advance through stages 1, 2, 3, and so on, but returning to previous stages is common. Review or Approval stages, for example, might include a 'Reject' action that reverts to an earlier workflow stage.

When you create a custom workflow template, specify the number of stages you would like and end with a Terminal stage. Each stage includes notification and other options. While planning your workflow template, decide which stages will allow questionnaires to advance independently and which will not. In a five-stage workflow, for example, you might allow independent movement in stages 2 through 4. To specify this, set stage 2 to "branch" and stage "4' to "join" by selecting the "Allow each questionnaire to advance workflow-stages independently" option in stage 2 and selecting the "All questionnaires must advance workflow-stages together" option in stage 4.



There are a few rules:

1. Every "branch" stage ("Allow each questionnaire to advance workflow-stages independently") must have a matching "join" stage ("All questionnaires must advance workflow stages together") later in the workflow.

2. A workflow can have more than one branch-join pair, but they cannot overlap.

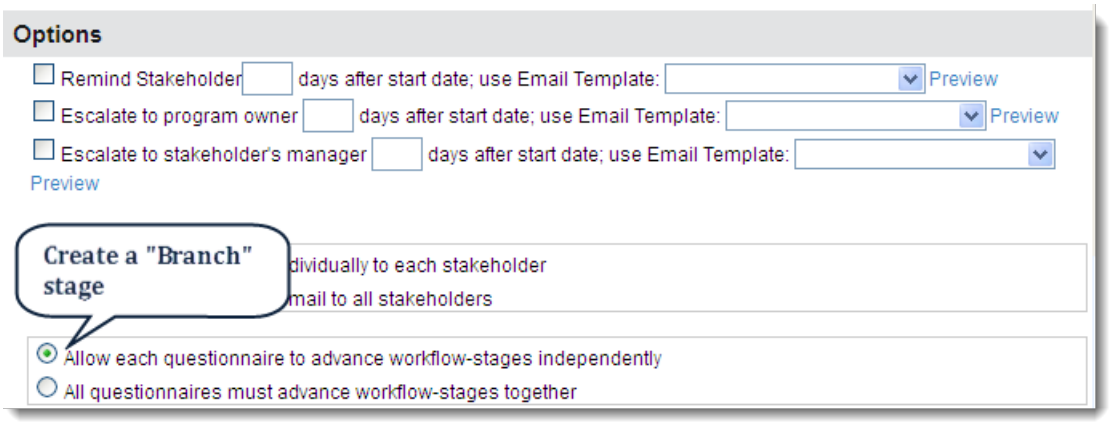
1 - 2 (branch) - 3 - 4 (join) - 5 - 6 (branch) - 7 - 8 (join) - 9 (terminal) <ΘK

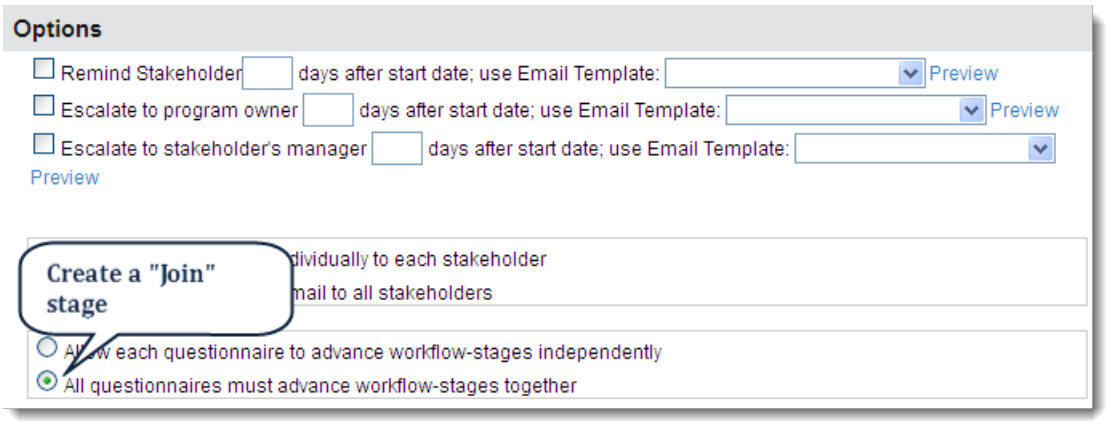
1 - 2 (branch) - 3 - 4 (branch) <<No, need to join the first branch before starting second branch

1 - 2 (branch) - 3 - 4 (terminal) <<No, need to join the branch before the terminal stage

3. A "branch" stage ("Allow each questionnaire to advance workflow-stages independently") can have actions that transition to stages before the branch stage, but no questionnaire will be able to advance past the "join" stage until all questionnaires have reached the "join" stage.

4. Stages after a "join" stage ("All questionnaires must advance workflow-stages together") cannot have actions that transition to stages before the "join" stage.



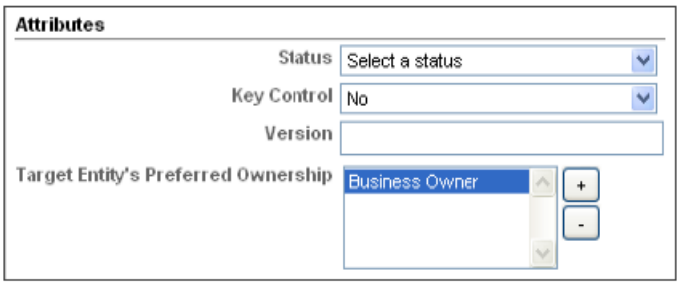

Options
Remind Stakeholder days after start date; use Email Template: Preview
Escalate to program owner days after start date; use Email Template: Preview
Escalate to stakeholder's manager days after start date; use Email Template:
Preview
dividually to each stakeholder
mail to all stakeholders
Create a "Join" stage
Allow each questionnaire to advance workflow-stages independently
All questionnaires must advance workflow-stages together

Preferred Ownership

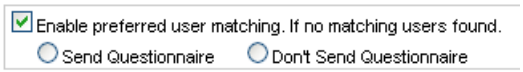
Objects such as entities and controls have at least one owner. Object owners can be nominated as the primary stakeholders of any workflow stage so that the stakeholders can manage the objects in an assessment. Alternatively, you may also assess entities based on the controls, groups or control objectives with preferred ownerships that match the workflow stage owners and entity owners. Preferred ownership allows stakeholders to answer a questionnaire that is different from other stakeholder's questionnaires of the same program assessment. That is,\ preferred ownership allows the first stage of an assessment workflow to send a unique questionnaire to each stakeholder.

To implement preferred ownership efficiently, configure the following:

1. The control, control objective, content pack, or group must list the ownership type in the Target Entity's Preferred Ownership field.



2. In the assessment workflow options, select **Enable preferred user matching** and indicate whether a questionnaire must be sent if the preferred user is not found for a particular entity.



If **Enable preferred user matching** is selected and no matching users are found, the default behavior is that the questionnaire will not be sent.

About Preferred Ownership Options

If your assessment is only valid when key object owners participate, you may want to skip sending a questionnaire when no preferred owners match. If any owner can answer when a preferred owner does not exist, send questionnaires even if no preferred owners match. Below are the preferred ownership options that explain whether to send a questionnaire if no matching users are found:

- Assess entities when control preferred owners and workflow stakeholders do not match.
    - Do not send questionnaires if no matching users are found. When you launch an assessment workflow, the RiskVision application will compare the preferred ownership of a control (group or control objective) with the stakeholders of a workflow stage, and if no match is found, controls are not created;meaning the controls are not listed in the assessment details tab of a program.
    - Send questionnaires if no matching users are found. When you launch an assessment workflow, the RiskVision application will compare the preferred ownership of a control (group or control objective) with the stakeholders of a workflow stage and if no match is found, it compares the workflow stage stakeholders with the entity owners. If a match is found, questionnaire is sent to the matched stakeholders to log the answer choice. Otherwise stakeholders can only view the questionnaire.
- Assess entities when control preferred owners and workflow stakeholders match.
    - When you launch assessment workflow, the RiskVision application will compare the ownership of an entity with the matched owners of a workflow stage and control (group or control objective), and if a match is found, a questionnaire is sent to the matched stakeholders to log the answer choice. Otherwise stakeholders can only view the questionnaire.

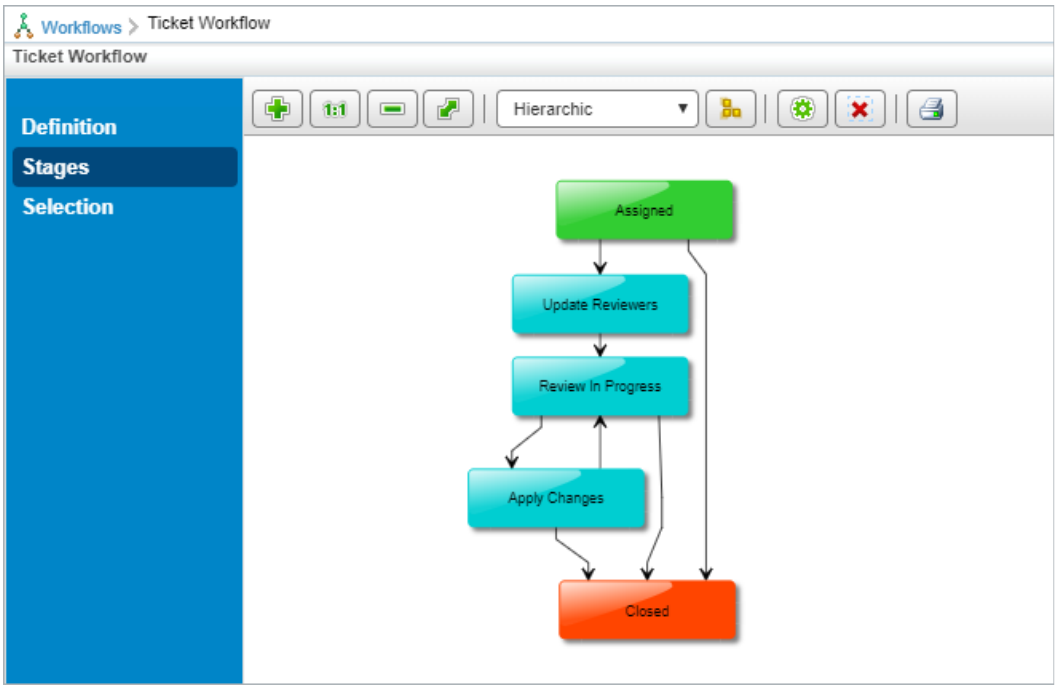
The preferred ownership feature works only in the first stage of assessment workflow that allows each questionnaire to advance the workflow-stages independently**.**

Assign the preferred ownership at the same level as the content added in a program. For example, if the preferred ownership is assigned to the content at the group level, assign the content to the program at the group level. If the preferred ownership is assigned to the content at the control level, assign the content to the program at the control level**.**

Visualizing Workflows

Workflows can be simple or complex, ranging from a few stages with sequential transitions to 20 or more stages with transitions that skip stages and go back to previous stages. For simple workflows, the **Definition** tab allows you to add and configure stages and helps you quickly grasp the stage transitions and the overall behavior.

For workflows with multiple stages, you must be precise in setting up each stage and test the workflow to ensure the behavior is as expected. The **Stages** tab can be used to gain a quick understanding of complex workflows. It shows all stage transitions, both forward and backward, and not just the sequential transitions, and allows workflows to be visualized in graphical layout.

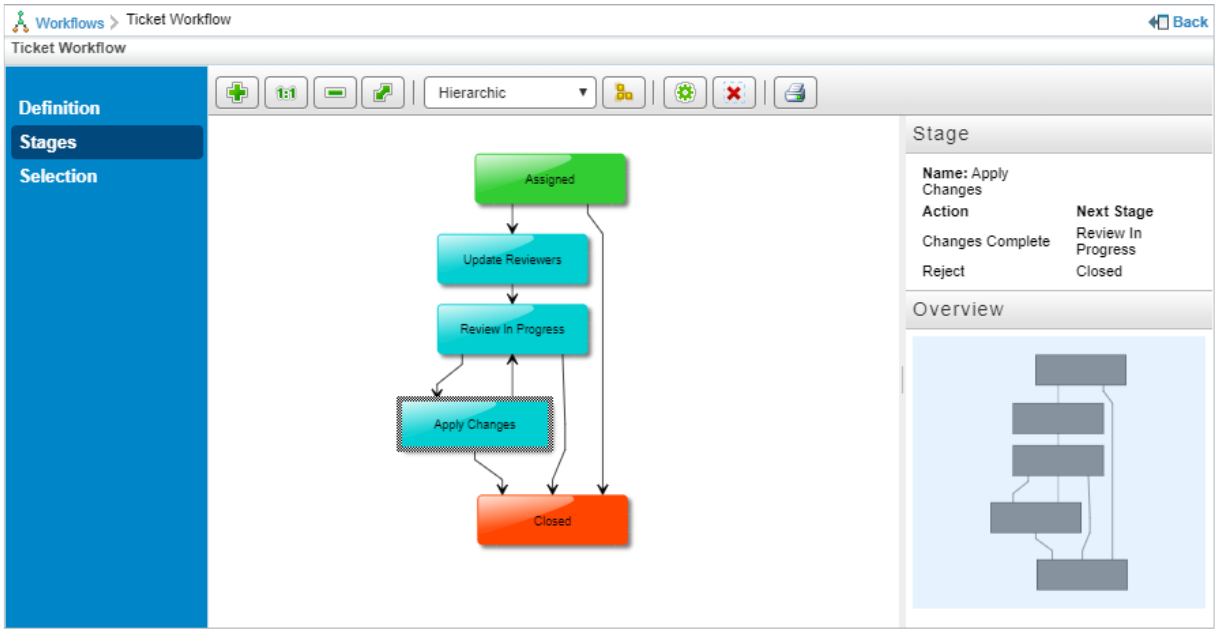


The Stages tab.

For information about the tool options, see Visualizing Objects.

The following is an explanation of the various elements of the **Stages** tab:

- The rounded rectangle in the graph represents the stages in a workflow.
- The incoming and outgoing arrows represent the transitions and indicate that transitions happen only between those stages. The direction of the arrow shows whether the transition is forward or backward.
- The **Stage** pane displays the stage information. Click a stage to view the action and the stage that a workflow will enter when that action is performed by the stakeholder.



The Stage pane when the Apply Changes stage has been selected.

- The **Overview** pane allows you to move the workflow layout in different directions. For more information, seeMoving the Layout.

Escalation

Escalation configurations allow you to control e-mail messages sent when a due date has passed. Three levels of escalation are supported, each with distinct evaluation criteria, recipients, and e-mail templates.

By default, RiskVision provides a single level escalation that sends an e-mail to the ticket's Owner Manager one day after the ticket is due. This escalation uses the Default Escalation E-mail Template by default. You can define additional levels, additional escalations, and individual and team recipients.

For more information about the e-mail template associated with each level of an escalation, seeAbout E-mail Templates.

To manage escalation configurations, go to **Configuration> Escalation.**

Creating an Escalation Configuration

Escalation configurations define what happens when a ticket is overdue. Selected recipients are notified using an e-mail template.

If your escalation requires a custom e-mail template, create the e-mail template.

You can create, update, or delete an escalation if your user role has Email Template View and Email Template Manage permissions.

To create a new escalation configuration:

1. Go to **Configuration** > **Escalation**.
2. Click **New**.
3. Enter the **General** settings as follows:
    - **Name**: Enter the display name that users will use to identify this escalation configuration.
    - **Description**: Enter a summary that will be visible only on the escalation page.
4. Create an escalation for Level 1 by clicking **New** in the **Escalations** section. You can repeat these steps to create escalations for Level 2 and 3 later, if desired.
5. Enter the **Escalation** settings as follows:
    - **Escalation Level**: Choose 1 for the first response to an overdue ticket. To create a different response if the ticket remains overdue, create a second Escalation with Level 2.
    - **Email Template**: Select from the list of available e-mail templates. Click Preview to see how the e-mail will look.
    - **Escalation Date**: The number of days after the ticket is due that triggers this message. Level 1 might be triggered 1 day after a ticket's due date while Level 2 is triggered a few days later. Level 3, if required, would be triggered later.
    - **Recipients**: Check Requester, Owner Manager, or select individuals or teams to receive this message.
6. Click **OK**.
7. Click **Save** to save the new escalation configuration.

About Email Templates

Use customized e-mail templates to include organization-specific details in messages sent to stakeholders during assessments, ticket resolution, and other processes.

Resolver uses the Velocity template engine to generate workflow and system messages. You can use some basic Velocity syntax and parameters to insert context data, such as the user's name, program name, program owner name, entity name, and dates and deadlines. For example, "Hi $Username" inserts the actual stakeholder's first and last name into the message.

Default Email Templates

The default template types are available for your use depending on the RiskVision solution. Resolver provides the following default templates:

NAME	TYPE	DESCRIPTION
Alert Notification (HTML)	Alert	Used to notify users that a compliance, control or risk score has crossed a specified threshold.
Alert Notification	Alert	Used to notify users that a compliance, control or risk score has crossed a specified threshold.
Assessment Launch	Assessment	Notifies users that a new assessment has been launched.
Assessment Launch Status	Assessment	Notifies program owners of assessment launch success or failure.
Assessment Recurrence	Assessment	Notifies program owners that an assessment that is configured for recurrence is about to be restarted.
Assessment Review	Assessment	Sends email when an assessment is sent out for review.
Assessment Review Rejection	Assessment	This template is used when an assessment you sent out for review was rejected.
Assessment Signoff	Assessment	Sends email when an assessment is sent for sign-off.
Assessment Signoff Rejection	Assessment	This template is used when an assessment that you sent out for sign-off was rejected.
Classification Assessment Launch	Assessment	This template is used when a new risk classification assessment has been launched.
Content Pack Delegation	Control	This template is used when a Content Pack is delegated from one user to another user.
Content Pack Deployed	Control	This template is used when a Content Pack is deployed.
Content Pack Escalation	Control	This template is used to alert users that a Control's due date is passed.
Content Pack Reminder	Control	This template is used to remind the user about upcoming due dates.
Content Pack Review	Control	This template is used when a Control is ready for review.
Content Pack Review Rejection	Control	This template is used when a Control is rejected during the review.

Default Escalation	Escalation	This template is used for sending an escalation notification.
Default Ticket Escalation Template	Ticket	The default template used when tickets themselves are escalated.
Default Ticket Assignment	Ticket	This template is used when a new ticket has been launched.
ERM Assessment Launch	Assessment	This template is used when a new ERM assessment has been launched.
ERM Risk Opinion Review Request	Risk	This template is used to notify users to request an ERM risk opinion.
Exception Delegation	Exception	This template is used when an exception is delegated from one user to another user.
Exception Escalation	Exception	This template is used to remind the user that the exception assigned to them is past the due date.
Exception Expire	Exception	This template informs a user that an exception has expired.
Exception Reminder	Exception	This template is used to remind the user about upcoming exception due dates.
Exception Review	Exception	This template is used when an exception is ready for review.
Exception Review Rejection	Exception	This template is used when an exception is rejected during the review.
Exception Signoff	Exception	This template is used when an exception is ready for sign-off.
Exception Signoff Rejection	Exception	This template is used when an exception sign-off was rejected.
Finding Closed	Finding	This template is used when a finding is closed.
Finding Delegation	Finding	This template is used when a finding is delegated from one user to another.
Finding Escalation	Finding	This template is used by the system to notify an assignor that a finding that they have assigned has not been worked on and is nearly past the due date.
Finding Reminder	Finding	This template is used to remind users about upcoming due dates on findings.
Finding Review	Finding	This template is used when a finding is ready for review.
Finding Review Rejection	Finding	This template is used when a finding is rejected during the review.
Finding Update Notification	Finding	This template is used to notify the finding owner when the finding is updated.

New Finding	Finding	This template is used to notify stakeholders when a finding is created.
New Vendor Contact Notification	Vendor	This template is used for notifying a new vendor contact that his/her login account has been created.
Incident Closed	Incident	Notifies users that an incident is closed.
Incident Delegation	Incident	This template is used when an incident is delegated from one user to another.
Incident Detected	Incident	Notifies that an incident is detected.
Incident Escalation	Incident	This template is used to remind users that the incident assigned to them is past the due date.
Incident Reminder	Incident	This template is used to remind the user about upcoming due dates on incidents.
Incident Review	Incident	This template is used when an incident is ready for review.
Incident Review Rejection	Incident	This template is used when an incident is rejected during the review.
Incident Signoff	Incident	This template is used when an incident is ready for sign-off.
Incident Signoff Rejection	Incident	This template is used when an incident sign-off is rejected.
Out of Office Delegation	Access Delegation	This template is used to notify users of assigned access delegations.
Questionnaire Assignment	Assessment	Used for data gathering to notify users that a questionnaire has been assigned to them.
Questionnaire Change Notification	Assessment	Used to notify assessment stakeholders that the questionnaire has been changed.
Questionnaire Delegation	Assessment	Used to notify a user that another user delegated a questionnaire to them.
Questionnaire Escalation	Assessment	Used to alert users that the questionnaire assigned to them is past the due date.
Questionnaire Reminder	Assessment	Used for reminderinf users of questionnaire due dates.
Report or Dashboard Delivery	Analytics	This template is used when a report or dashboard is sent to the user.
Response Notification Error	System	An HTML template used to send notification that a user request was not successfully processed.
Response Notification		An HTML template used to send notification that a user request was successfully

Success	System	processed.
Response to Password Reset Request	System	Sent when a user requests their password to be reset.
Risk Assessment Launch	Assessment	This template is used to notify stakeholders that a new risk assessment has been launched.
Risk Identified	Risk	This template is used to notify owners that a new risk is identified.
Scheduled Job Completed Successfully	System	Sends a job success notification.
Scheduled Job Failed	System	Sends a job failure notification.
Threats Advisory Alerts	Alert	Used to notify users when new threats or vulnerabilities are reported by security research organizations.
Ticket Assignment Notification	Ticket	Notifies a user they have been assigned a ticket.
Ticket Update Notification	Ticket	Notifies the ticket owner when the ticket is updated.
Ticket Closed	Ticket	Sends a notification that a ticket was closed.
Ticket Delegation	Ticket	Sends a notification that a ticket was delegated from one user to another user.
Ticket Escalation	Ticket	Used to alert users that the tickets are assigned to them after the due date is passed.
Ticket Reminder	Ticket	Reminds a user about upcoming due dates on tickets.
Ticket Review	Ticket	Sends a notification that a ticket is ready for review.
Ticket Review Rejection	Ticket	Sends a notification that a ticket was rejected during the review.
Vulnerability Assignment Notification	Alert	Used to notify a user that they have become the owner of a vulnerability.

Configuring E-mail Templates

This section explains how to create, delete, and modify an e-mail template. On the Configuration menu, click Email Templates to view default and custom created template types. To view email templates, you must have the Email Template View permission, and in order to create, delete, or modify them, you must have the Email Template View and Email Template Manage permissions.

The following describes the available email template types:

- **Access Delegation**. Used when notifying users of assigned access delegations.
- **Assessment**. Available for selection in assessment workflows.
- **Analytics.** Available for selection in the Administration application when a report or dashboard is sent to the user.
- **Control.** Available for selection in the policy workflow.
- **Ticket.** Available for selection in the ticket workflow.
- **Incident.** Available for selection in the incident workflow.
- **Exceptions.** Available for selection in the exception workflow.
- **Finding**. Available for selection in the finding workflow.
- **Alerts.** Sent for events, such as an entity scoring higher for risk or compliance than the threshold.
- **Escalation.** Used when ticket deadlines are reached.
- **Reports.** Sent for report notifications.
- **Vendor.** Used to notify primary vendor contact of changes.

Updating Email Template

Modifications to email templates take effect immediately.

To update an email template:

1. Go to **Configuration**> **Email Templates**.
2. Select a template and then click **Details**. The template opens in a pane below the grid.
3. Click **Edit**.
4. In the **General** section, edit the following settings:
    - **Display Name**: Enter the short name for the template.
    - **Template Type**: Select the workflow type.
    - **Content Type**: Select either HTML or Plain text content type of a template.
    - **Description**: Enter information that will help others understand the use of template.
    - **Send Immediately**: Send notifications without sequencing.
    - **High Priority**: Send notifications with high importance.
    - **Sender Email Account**: Select the email account that will send the notifications. The RiskVision administrator's email account is used by default.
    - **Template text**: Author information that suits the template type. Text can be formatted using HTML.
5. When you finish modifying the template, click **Save**.

Adding a New Customized Email Template

Users with sufficient privileges can create new e-mail templates for later use.

To create an e-mail template:

1. In the RiskVision application, go to Configuration > Email Templates. In the Administration application, go to Administration > Email Templates.
2. Click New.
3. In the General section, enter the following fields:
    - Name. Enter the display name that users select when setting up a workflow.
    - Template Type. Select the workflow type.
    - Content Type. Select either HTML or Plain text content type of a template.
    - Description. Enter information that will help others understand the use of the template.
    - **Send Immediately**. Select to send the notifications without sequencing and/or merging. See also Sequencing and Merging of Email Notifications.
    - **High Priority**. Select to send the notifications with high importance. By default, all of the escalation email templates are sent with high priority.
    - **Sender Email Account**. Select the email account of the sender to send the notifications. By default, the administrator email account is used for sending email notifications.
4. Enter the message content.

    Resolver recommends basing new templates on one of the defaults.
5. Click Save.

The email template is now available for selection in workflow templates.

To understand how an email template can be used to notify the stakeholders, see Setting up Email Notifications.

Email Template Variables

The system automatically replaces the variables in the following sections with the corresponding value when the notification or email is sent.

In designing your own email template or modifying those provided, use the default templates as a guide to what variables are available for different types of email template and for how they are used.

- Alert Email Templates
- Assessment Email Templates
- Analytics Email Templates
- Exception Email Templates
- Finding Email Templates
- Incident Email Templates
- Risk Email Templates
- Ticket Email Templates
- Vendor Email Templates
- More Variables

Alert Email Templates

The following variables are available to designers of this type of email template:

VARIABLE	DESCRIPTION
details	Includes properties and methods that describe the details of the alert of which the user is being notified. For example, `details.alertRule` is one property. Alert rule is itself an object, comprised of the properties name and description. So, to cause an Alert email template to display the name of the alert rule that triggered the notification, the designer would specify $details.alertRule.name.
details.alertRule.description	The description of the alert rule that triggered an email notification.
details.alertRule.name	The name of the alert rule that triggered an email notification.

Assessment Email Templates

The following variables are available to designers of this type of email template:

Variable	Description
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
projectName	The name of the Program associated with this assessment.
surveyName	The name of the Questionnaire.
projectDescription	The description of the Program associated with this assessment.
userName	The recipient of the email, usually a stakeholder in the current assessment
launchStatusDetalis	A descriptive string (Assessment Launch Status template only).
assessmentName	The name of the assessment.
commentOwnerName	The name of the user rejecting the assessment (Review Rejection or Signoff Rejection only).
comment	The text of the comment associated with the rejection (Review Rejection or Signoff Rejection only).

You can add the $NT.getValue("RAProject.version") variable in any assessment email template type to display the assessment's version number.

Analytics Email Templates

The following variables are available for this email template:

VARIABLE	DESCRIPTION
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
userName	The recipient of the email, usually a stakeholder in the current workflow.
objectValue	The name of dashboard or chart.
passwordProtectedStatement	The password to open the report.
appurl	The URL of the RiskVision application.

Control Email Templates

The following variables are available to designers of this type of email template:

Variable	Description
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
userName	The recipient of the email, usually a stakeholder in the current workflow.
workItemName	The name of the workItem, either a Control, a Subcontrol, or another kind of item.
stageName	The name of the current workflow stage.
appurl	The URL of the RiskVision application.

Exception Email Templates

The following variables for this email template:

VARIABLE	DESCRIPTION
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
userName	The recipient of the email, usually a stakeholder in the current workflow.
workItemName	The name of the workItem, either a Control, a Subcontrol, or another kind of item.
stageName	The name of the current workflow stage.
xceptionName	The name of the exception (Exception expire template only).
exceptionEndDate	The expiration date of the exception (Exception expire template only). SeeModifying a Variable Displaying Date.
ownerName	The owner of the exception (Exception expire template only).
commentOwnerName	The name of the user transitioning the workflow stage.

You can add the $exceptionId variable in any exception email template type to display the exception ID.

Finding Email Templates

The following variables are available to designers of this type of email template:

Variable	Description
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
userName	The recipient of the email, usually a stakeholder in the current workflow.
workItemName	The name of the workItem.
findingName	The name of the finding.
findingDescription	The description of the finding.
findingStage	The name of the current workflow stage.
currentDate	The date on which a finding is assigned to the stakeholder.
appurl	The URL of the RiskVision application.
commentOwnerName	The name of the user transitioning the workflow stage.

Incident Email Templates

The following variables are available to designers of this type of email template:

Variable	Description
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
userName	The recipient of the email, usually a stakeholder in the current workflow.
workItemName	The name of the workItem, either an incident or another kind of item.
stageName	The name of the current workflow stage.
incidentName	The name of the incident (Incident closed template only).
incidentTypeName	The name of incident type.
incidentSubTypeName	The name of incident subtype.
incidentId	The identifier of the incident (Incident closed template only).
incidentDetected	The string of the date and time that the incident was detected (Incident closed template only).
incidentStatus	The current status of the incident (Incident closed template only).
commentOwnerName	The name of the user transitioning the workflow stage.

Risk Email Templates

The following variables are available for this email template:

VARIABLE	DESCRIPTION
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
projectName	The name of the Program associated with this notification.
projectDescription	The description of the Program associated with this notification.
riskNames	The name of the risk associated with the program for which you are sending the notification.
entityName	The name of the entity associated with the risk.
appurl	The URL of the RiskVision application.

Ticket Email Templates

The following variables are available for this email template:

VARIABLE	DESCRIPTION
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
userName	The recipient of the email, usually a stakeholder in the current workflow.
workItemName	The name of the workItem, either a ticket, or another kind of item.
ticketID	The ID of the ticket.
ticketName	The name of the ticket.
ticketPriority	The priority of the ticket (low, medium, high, and so on).
ticketDue	The string of the date that the ticket is due. SeeModifying a Variable Display Date.
ticketStatus	The current status (workflow stage) of the ticket.
ticketDescription	The description of the ticket.
notificationDescription	The description of this ticket notification (Ticket Update Notification templates only).
ticketAttributeChangeDetails	The old and new values of changed attributes (Ticket Update Notification templates only).
commentOwnerName	The name of the user transitioning the workflow stage.

Vendor Email Templates

The following variables are available for these email templates:

VARIABLE	DESCRIPTION
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
vendorName	Name of the vendor to whom the account details are sent.
userName	Recipient of the email, usually a stakeholder in the current workflow.
userId	Username of the vendor account.
password	Password for the vendor account user.
details	Additional details sent for the vendor account.
senderName	Name of the user who will send this notification.
appurl	RiskVision URL.

In addition to the variables above, you can also use the $NT.getValue(".- workflowTransitionComment") variable to notify stakeholders of the workflow stage comments.

More Variables

The following variables are available for email templates to help point stakeholders to the user interface in which the action is required.

VARIABLE	DESCRIPTION
$NT.getObjectUrl("objectName")	Use this variable in an email template to direct users to the default tab of an object. For example, $NT.getObjectUrl("RAProject").
$NT.getObjectUrlWithTab("objectName", "tabName")	Use this variable in an email template to direct users to a tab available on an object details page. For example, $NT.getObjectUrlWithTab("Assessment", "Control Results").
$NT.getQuestionnaireUrl()	Use this variable in an email template to direct users to the Questionnaire window. This variable must be specified in the email templates defined in the first stage of the assessment workflow.

Modifying a Variable Displaying Date

Although, variables, such as $ticketDue and $exceptionEndDate will display the date in the 'MM/dd/yyyy hh:mm:ss' format when the notification is sent to the workflow stage stakeholders, you can also use the $dateTool velocity template variable to display an alternative format to the default date format. To change the date format in the email template, use the following code corresponding to the format and replace the code with the email template variable:

For $ticketDue variable

- Date and time - `$dateTool.format('MM/dd/yyyy hh:mm:ss',$ticketDue)`
- Date - `$dateTool.format('MM/dd/yyyy',$ticketDue)`

For $exceptionEndDate variable

- Date and time - `$dateTool.format('MM/dd/yyyy hh:mm:ss',$exceptionEndDate)`
- Date - `$dateTool.format('MM/dd/yyyy',$exceptionEndDate)`

Adding Object Fields in Email Templates

You can add fields from an object's details page as workflow-type variables in stakeholder notifications. You can even include custom attributes that you have added to the objects. The following field types can be added to any email template:

FIELD TYPE	VARIABLE
String	$NT.getValue(".customAttributes.")
Number	$NT.getValue(".customAttributes.")
Boolean	$NT.getValue(".customAttributes.")
Date	$NT.getValue(".customAttributes.")

Add Custom Attributes to Email Templates

Any custom attribute supported by RiskVision can be added as a variable to an email template. The following attribute types can be added:

ATTRIBUTE	VARIABLE	DESCRIPTION
Date	$NT.getValue(".customAttributes.")	The date and time in the YYYY-MM-DD HH:MM:SS format by default.
Encrypted string	$NT.getValue(".customAttributes.")	A string value in encrypted format.
Flag	$NT.getValue(".customAttributes.")	Boolean values.
Image	$NT.getValue(".customAttributes.")	An image that can be displayed in the email.
Number	$NT.getValue(".customAttributes.")	Positive and negative numbers, including zero.
Rational number	$NT.getValue(".customAttributes.")	Positive and negative integers displayed as fractions.
String	$NT.getValue(".customAttributes.")	Multiple characters.
Text	$NT.getValue(".customAttributes.")	Character strings and HTML formatting.

Getting Familiar with Email Notifications

RiskVision notifies system users by email under a variety of circumstances. The user who receives the email notification is almost always determined by the entity or other object ownership.

NOTIFICATION	EMAIL TEMPLATE	RECIPIENTS
Assessment Workflow Started	Assessment Launch, Classification Assessment Launch, ERM Assessment Launch, and Risk Assessment Launch	Stakeholders are always notified. Stakeholders includes 'Primary Owner' by default.
Assessment Restart An assessment is automatically restarted based on recurrence rules	Assessment Recurrence	All stakeholders in the initial stage that are tagged with the notify icon.
Exception Workflow Started	Optional **Do Not Send Email** is the default.	Exception requester is the only stakeholder if **Notify selected stakeholder** is checked.
Ticket Workflow Started	Optional No pre-defined templates.	If **Notify selected stakeholder** is checked.
Workflow Action An action changes a workflow to a new stage.	User-selected. Note: Pull down list for Policy workflow is 'Content Pack' choice. Assessment Review, Assessment Review Rejection, Assessment Signoff, Assessment Signoff Rejection, Ticket Review, and Ticket Review Rejection.	All stakeholders of the stage before the change.
Escalate (optional) The escalations for different objects can be sent based on the available different date types.	User-Selected Email Template	Escalates to the stakeholders in the current workflow stage. See the note at the end of this section.
Reminder The reminders for different objects can be sent based on available different date types.	User-Selected Email Template	Reminds all stakeholders in the current workflow stage. See the note at the end of this section.
Ticket Created	Default Ticket Assignment	The user assigned to the ticket.

Exception or Ticket Delegated	Exception Delegation and Ticket Delegation	The new assignee.
Ticket Exception Expiration Date in a ticket's 'Exception Expiration' field has passed.	Specified in the `ticket.exception.expired.notification.template` Property	All stakeholders of the current stage.
Vendor Account Created	New Vendor Contact Notification	New vendor user.
Assessment is Accessed (Optional in all except terminal stages) Assessment is accessed when questionnaire is opened.	N/A	Primary owner. If the primary owner is removed from list of stakeholders, no email is sent.
Score Crosses a Threshold A control, compliance, or risk score crosses a specified threshold.	Alert Notification	Selected in the alert rule.
A Scheduled Job Completes Successfully	Scheduled Job Completed Successfully	Specified email user.
A Scheduled Job Fails	Scheduled Job Failed	Specified email address.
A Dashboard or Report is Sent to the User	Report or Dashboard Delivery	The original requestor.
Risk Created	Risk Identified	Owner.
New Threats or Vulnerabilities are Reported New threats or vulnerabilities are reported from a security research organization.	Threats Advisory Alerts	Control/entity owner.
User Account Delegation Notify users of assigned	Out of Office Delegation	The user who has been designated as a delegate.

access delegations.		
Content has Been Changed	Questionnaire Changed Notification	Stakeholders in the current workflow stage.

Workflow escalation and reminders can be sent as one email to all (single email to all stakeholders) or one email to each (email individually to each stakeholder).

About Filter Data Types

The properties of a field describe the characteristics and behavior of data added to that field. A field's data type is the most important property because it determines what kind of data the field can store. This article describes the data types and other field properties.

Fields contain the following types of data:

Data types	Description
string	Field contains characters, symbols, or numbers.
float, integer, short, long	Field contains a numeric value.
timestamp	Field contains a date. Select the day and time using the calendar widget.
boolean	Field contains true or false.

About Comparison Operators

Comparison operators, as their name implies, allow you to compare two values. Comparison operators are used in logical statements to determine equality or difference between variables or values.

To use a comparison operator, you need to specify the values that you want to compare together with an operator that separates these values. When the input is a collection of values, the comparison operators return any matching values. If there are no matches in a collection, comparison operators do not return anything.

The following table describes the comparison operators:

Operators	Data type	Description
Equals	all	Exactly matches the value. For Tags and Organizational Nodes, use Contains, not ==.
Not equals	all	Any that do not exactly match.
Greater than	float, integer, short, long, timestamp	Definition is higher than the number that you entered.
Greater than or equal	float, integer, short, long, timestamp	Definition is similar or higher than the number that you entered.
Less than	float, integer, short, long, timestamp	Definition is lower than the number that you entered.
Less than or equal	float, integer, short, long, timestamp	Definition is similar or lower than the number that you entered.
Between	string	Value is between two values. (Selecting this Comparison op displays a second value field).
Contains	string	Definition contains the exact phrase that you entered. For example: 'al' matches alright and minimal but not.
Starts with	string	Definition begins with the exact phrase that you entered. For example: 'al' matches alright, but not minimal and.
Ends with	string	Definition ends with the exact phrase that you entered. For example: 'al' matches minimal, but not alright.
Matches filter	string	Allows one filter condition to reference another filter.
Is Null/Is Not Null	all, except boolean	The field, is defined or not defined.

About Conjunctions

Join operands to create a truth table as follows. A single filter can mix AND and OR conjunctions, but the results may not match the author's intent, due to precedence rules. The expression X AND Y OR Z can be interpreted as true only when X and either Y or Z are true, or it can be interpreted as true when either Z or both X and Y are true. Avoid mixing both conjunctions in the same filter. Instead, create two filters and use the 'Matches filter' operator to combine them.

Conjunction	Description
AND	Returns true if all conditions are true and false if any condition is false.
OR	Returns true if any condition is true and false if all conditions are false.

For users, other than the RiskVision administrator, filters can be viewed on the Configuration > Filters menu with the Filter View permission. Creating, modifying, or deleting a filter requires you to have the Filter View and Filter Update permissions.

Adding a Filter

This article explains how to add a filter without conditions. Typically, a filter without any conditions matches all records.

To create a new filter:

1. In the RiskVision application, go to **Configuration** > **Filters**. In the Administration application, go to **Users** > **Filters**.
2. Expand the **Filter** groups to select a specific group to which you want to add the filter.
3. Click **New**. The **New Filter** dialog appears.
4. Enter the general information:
    1. Enter **Name** and Description.
    2. Select the filter type and then click **OK**.

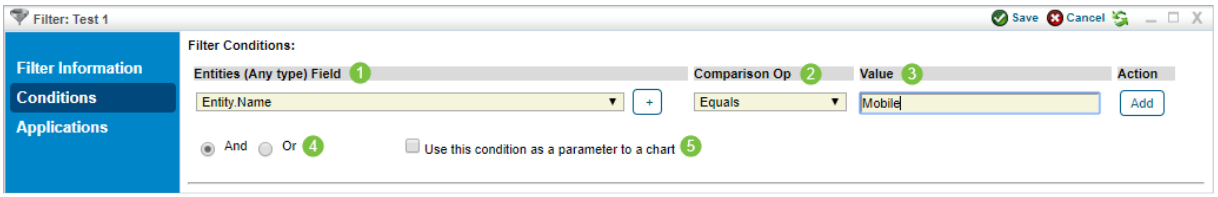
The filter is available for assignment.

Modifying Filter Conditions

This article explains how to add or remove a condition. Changes are applied the next time a report is run or a dashboard is updated. The new settings are used and user access filters are applied the next time the user logs in.

To add a condition:

1. Go to **Configuration** > **Filters**.
2. Expand the **Filters** tree.
3. Select a filter to open.
4. Click the **Conditions** tab.
5. Click **Edit**, then click **Add.**
6. Enter the Filter conditions as follows:



The Filter Conditions section.

1. **Attribute**: Select the field where you want to filter the records.
2. **Operator**: Select the type of operation you want to use to compare the attribute definition and value.
3. **Value**: Enter a string or number, or select from the dropdown list.
4. **Conjunctions**: Joins conditions to build an expression that is matched when returned true. Select the same type for all conditions in a filter. Matches filter to combine AND and OR expressions.
5. **Use this condition as a parameter to a chart** Allow all users to create reports that can drill down to the record level of this field.

7. Click **Save**.

The Matches Filter operator will not produce correct results if the filter it references is not found. If you must use the Matches Filter operator in the condition of a filter, create the filter to be set in the Matches Filter value first**.**

To remove a condition:

1. Go to **Configuration**> **Filters**. In the **Administration** application, go to **Users** > **Filters**
2. Expand the **Filters** tree.
3. Select a filter to open.
4. Click the **Conditions** tab.
5. Click **Edit**, then click the **Delete X** icon next to the condition.
6. Click **Save**.

Removing a Filter

You can only remove unassigned filters. If you try to remove a filter that is in use, an error lists the location where it is used.

To delete a filter:

1. In the RiskVision application, go to **Configuration** > **Filters**. In the **Administration** application, go to **Users** > **Filters**.
2. Expand the **Filters** tree and locate to select the filter.
3. Click **Delete**.

The filter is no longer available.

Grouping Filters

To make it easier to get an overview of the filters in the filters panel, you can create filter groups within a data table and place certain filters in these. You can only group filters that belong to the same data table. You can then expand or collapse various groups to only work with the filters you want for the moment.

The navigation pane contains the following predefined groups:

GROUP NAME	DESCRIPTION
Filters	Root folder contains RiskVision Content and Organization Content; displays a recursive list of all filters.
My Filters	Contains filters visible to the current user only.
Shared Filters/System	Contains default system filters.
Shared Filters/Public	Contains filters configured by your organization.

Creating a New Group

You can only add groups in Organization Filters group.

To add a group:

1. In the RiskVision application, go to **Configuration > Filters**. In the Administration application, go to **Users > Filters**.
2. Select the organization group.
3. Select **New Group** in the **More Actions** drop-down list.
4. Enter a name and description.
5. Click **OK**.

The group displays in the list.

Deleting a Group

Deleting a group removes all filters in the group. You can only remove groups that contain unassigned filters.

To remove a group:

1. In the RiskVision application, go to **Configuration > Filters**. In the Administration application, go to **Users** > **Filters**.
2. Select the group that contains the one you want to delete. For example, if the group you are removing is in an organization, then select an organization.

   The group displays in the Filter list.
3. Select the group and click **Delete**.

The group and any subgroups and filters are removed.

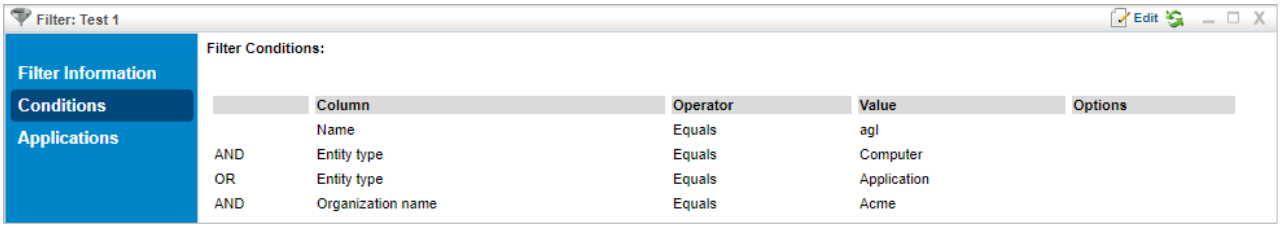
Understanding Complex Filters

A filter can be as simple as **Setting Equals 1**, but more complex filters can be used in reports or for access control.

The built-in filter editor can be used to add conditions one at a time to a filter. These filter conditions are added using the **AND** or **OR** logical operators. By default, the **AND** operator has higher precedence than the **OR** operator. The filter editor does not allow the user to override the precedence (typically done by adding parenthesis).

Example

You have the following filter set up:



The Conditions tab of a filter.

The filter in this example translates to:

```
Entity Name starts with agl AND Entity Type = Computer OR Entity Type = Application AND Organization name = Acme
```

Since the **AND** operator has higher precedence than the **OR** operator, the above filter means:

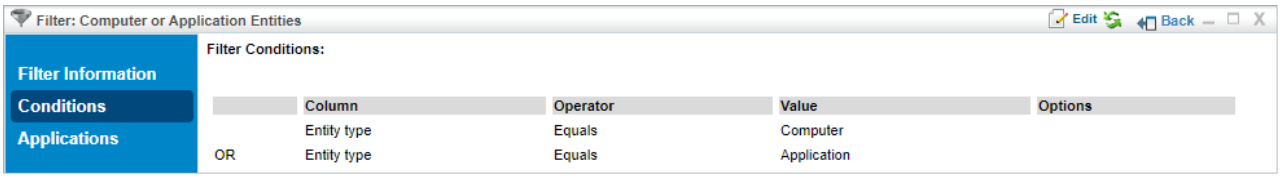
```
(Entity Name starts with agl AND Entity Type = Computer) OR (Entity Type = Application AND Organization name = Acme)
```

That is, the **AND** operations are performed first.

If you want this filter to evaluate as:

```
(Entity Name starts with agl) AND (Entity Type = Computer OR Entity Type = Application) AND (Organization name = Acme)
```

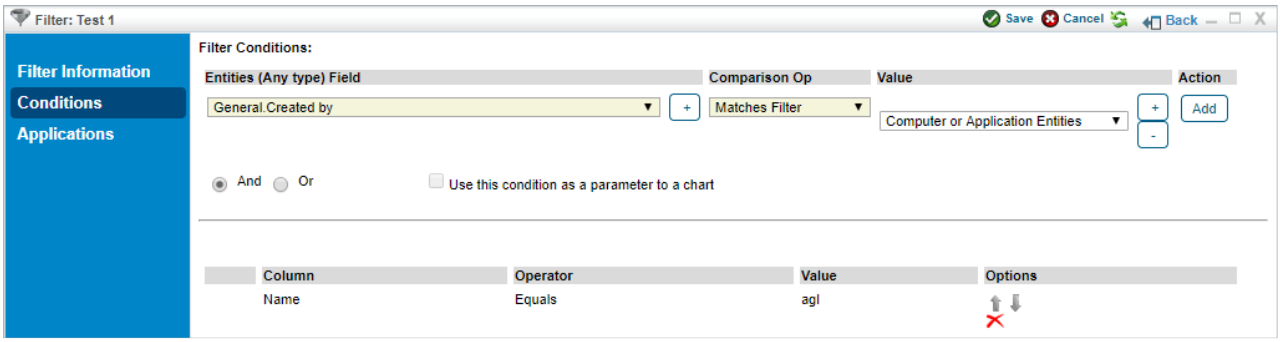
There is no way to do this directly by using the filter editor. You must do this using the **Matches Filter** operator. To implement the above filter, you must build a Computer or Application Entities filter for the condition `(Entity Type = Computer OR Entity Type = Application).`



A Computer or Application Entities filter.

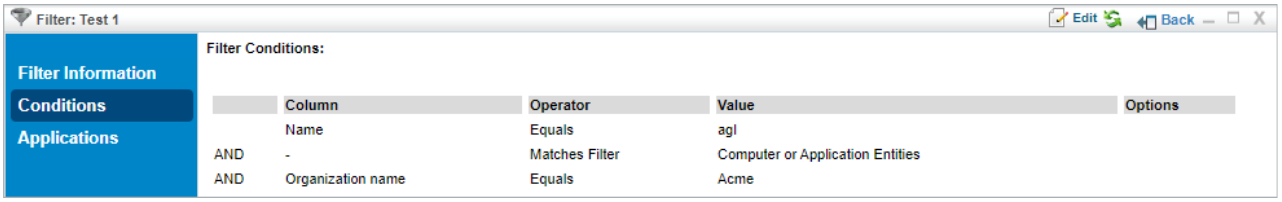
The original filter will use the Computer or Application Entities filter using the **Matches Filter** operator.

First, add the **Name Equals agl** condition. Use the **Matches Filter** operator to add the Computer or Application Entities filter. Note that a dummy entry must be selected in the first dropdown of the filter editor. In this case, **Created By** is selected, which is ignored by the server.



Adding the Matches Filter operator.

Add **Organization name Equals Acme**. The filter will now look like this:



The filter with the Matches Filter operator added.

Internally, the server surrounds the filter condition of the **Matches Filter** operator with parenthesis. So, this will translate to:

```
(Entity Name starts with agl)AND(Computer or Application Entities) AND (Organization name = Acme)
```

Which is effectively similar to the filter that you set out to construct:

```
(Entity Name starts with agl) AND (Entity Type = Computer OR Entity Type = Application) AND (Organization name = Acme)
```

This can be taken further by using **Matches Filter** operator within the filters used by another **Matches Filter** operator.

User Variables

Users can refer to the following variables when creating filters or custom SQL queries for reports.

USER VARIABLE	DESCRIPTION
%USER_ID%	Login user ID of the current user.
%SYSTEM_USER_ID%	Internal ID of the current user.
%USER_FIRSTNAME%	First name of the current user.
%USER_LASTNAME%	Last name of the current user.
%USER_NAME%	Concatenation of the first name, a single space, and last name of the current user.

About Alert Rules

Alert Rules trigger notifications when compliance and risk scores fall outside specified thresholds.

An Alert Rule consists of:

- Compliance and risk score thresholds
- Assessments of interest
- Entities of interest (or specific dynamic groups)
- Controls of interest
- Recipient list
- Options

When an assessment, entity, or control triggers an alert rule, recipients will receive e-mail notifications. Recipients can be specified by name, by team, or by role (such as Primary Owner).

You can view alert rules on the **Assessments** > **Notifications and Alerts** menu only if you have the Assessments View and Tenant Configure permissions. Creating, modifying, or deleting an alert rule requires you to have the Assessments View, Tenant Configure, and Alert Rule Manage permissions. When you have these permissions, you can manage any alert rule irrespective of the ownership.

Creating an Alert Rule

To create a new alert rule

1. **Click Assessments> Notifications and Alerts. A list of alert rules appear.**
2. Click **New.**
3. Enter the following fields:
    1. **Name.** Enter a name and description for the new Alert Rule and click **Next**.
    2. **Thresholds.** Enter thresholds for compliance and risk score. A notification will be sent if the compliance score falls below the threshold, or if the risk score rises above the threshold. To ignore the compliance score, set it to 0. To ignore any of the risk scores, set them to 100. Click **Next.**
    3. **Programs**. Select the programs of interest, all programs or selected to this alert rule. When you have specified programs, click **Next**.
    4. **Entities**. Select specific entities of interest to this alert rule. Find entities by dynamic group, or search for the entities. When you have specified entities, click **Next**.
    5. **Controls**. Select controls from the controls tree. Check the box to select approved versions only, if desired. When you have specified controls, click **Next**.
    6. **Recipients**. Select recipients by name, team, or role. You may select recipients using a combination of methods. To move on, click **Next**.
        - To select by name, check Select Individual Users. Search for the user, select the user and click >>.
        - To select by team, check Select Teams. Select the team from the list and click >>.
        - To select by role, such as Primary Owner, check the box associated with the desired role.
    7. **Options**. Select an email template for the notification, or click Create a new template to display an editor to design a new email template. Click P**review Template** to see an example notification. Un-check Enable this alert to postpone making this alert active. Specify how much of the assessment must be complete before testing scores against the thresholds.
4. Click **Finish**.

E-mail Templates

Email templates are provided for HTML and plain text alert notification. New templates can be created for special purposes. Email templates include variable references and commands such as #foreach in order to embed system data in custom content.

This example illustrates part of a plain text alert notification email.

#if ($macs && 0 != $macs)

##

#set($totalAlerts = $details.getTotalAlerts('ASSESSMENT_COMPLIANCE_SCORE'))

#set($newAlerts = $details.getNewAlerts('ASSESSMENT_COMPLIANCE_SCORE'))

##

Alerts on assessment compliance score:

There are $totalAlerts.size() assessments that fell below the minimum compliance score $details.threshold.get('ASSESSMENT_COMPLIANCE_SCORE'). $newAlerts.size() of them are new violations since the last alert. They are listed below

#foreach($project in $details.alertsByProject)

##

#set($totalAlerts = $project.getTotalAlerts('ASSESSMENT_COMPLIANCE_SCORE'))

#set($newAlerts = $project.getNewAlerts('ASSESSMENT_COMPLIANCE_SCORE'))

##

#if ($newAlerts && 0 != $newAlerts.size())

project: $project.projectName, total: $totalAlerts.size(), new: $newAlerts.size()

project details: $project.projectDetailsUrl

#foreach($alert in $newAlerts)

$alert.entityName: $alert.score ($alert.entityDetailsUrl)

#end

#end

#end

#end

For more information about template variables, see About Email Templates.

Modifying An Alert Rule

To modify an alert rule:

1. Click **Assessments** > **Notifications and Alerts**. The alert rules appear.
2. Check the box next to the alert rule and click **Details**.
3. Change the threshold, programs, entities, controls, recipients, or options as desired.
4. Click **Finish** to save the revised alert rule.

Deleting an Alert Rule

Users with sufficient privileges can delete alert rules.

To delete an alert rule:

1. Click **Assessments**> **Notifications and Alerts**. The alert rules appear
2. Check the box next to the alert rule and click **Details**.
3. Click Delete.

Configuring a Threshold Range for Calculating Vulnerability Scores

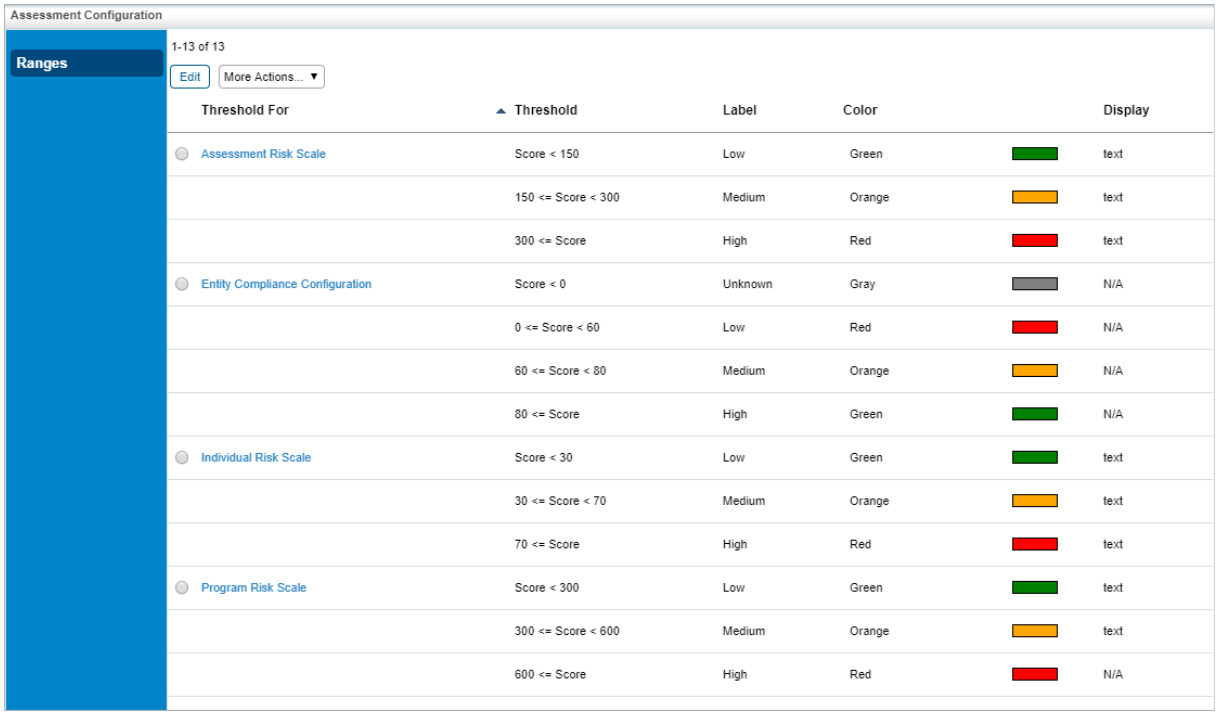
A common threshold range criteria must be established for assessment, finding, and risk objects. When assessments are run, the vulnerability scores are derived according to the scale that has been defined for a range. Before running an assessment, ensure that the threshold range is configured to meet the auditing guidelines and policies of the assessment objectives.

Each configuration range allows the user to adjust the threshold range by specifying the numeric value, unique name, color, and the option to display text or a score.

In order to adjust the configurations, you must have the Tenant Configure permission.

To set up Assessment Configuration:

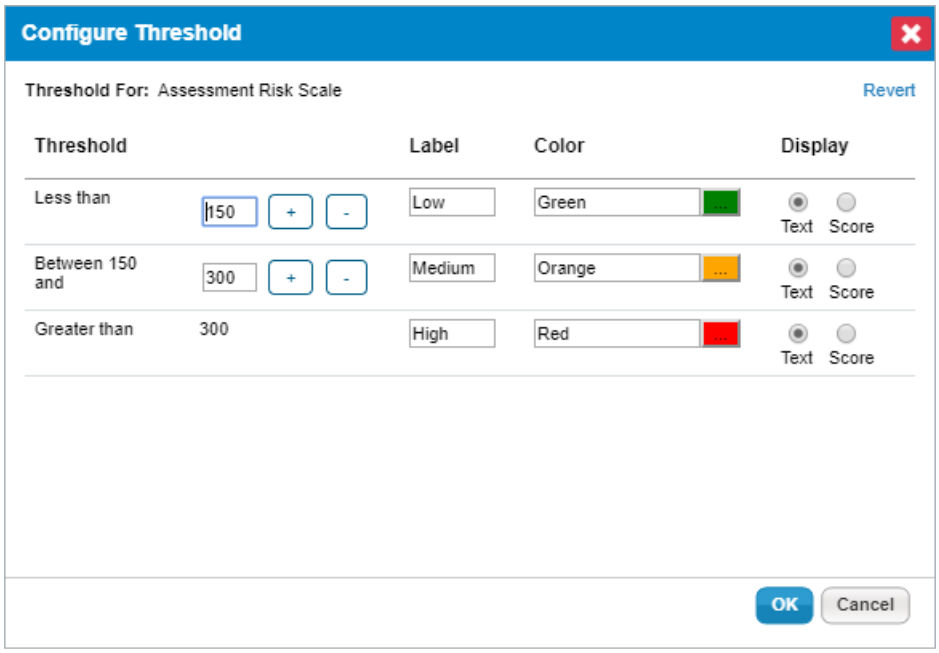
1. Open the Compliance Manager.
2. Go to **Configuration > Assessment Configuration**.



Threshold For	Threshold	Label	Color	Display
Assessment Risk Scale	Score < 150	Low	Green	text
	150 <= Score < 300	Medium	Orange	text
	300 <= Score	High	Red	text
Entity Compliance Configuration	Score < 0	Unknown	Gray	N/A
	0 <= Score < 60	Low	Red	N/A
	60 <= Score < 80	Medium	Orange	N/A
	80 <= Score	High	Green	N/A
Individual Risk Scale	Score < 30	Low	Green	text
	30 <= Score < 70	Medium	Orange	text
	70 <= Score	High	Red	text
Program Risk Scale	Score < 300	Low	Green	text
	300 <= Score < 600	Medium	Orange	text
	600 <= Score	High	Red	N/A

The Assessment Configuration tab.

3. Select **Assessment Risk Scale**, then click **Edit**.



The Configure Threshold dialog.

4. Click + or – to add or remove a threshold range. For any assessment configuration, you can add a maximum of five threshold ranges. At a minimum, any configuration range contains two threshold ranges.
5. **Optional:**
    - To modify a range, enter a numerical value in the threshold range field.
    - To change the threshold display name, enter a name in the **Label** field.
    - To assign a color for a threshold, click the **Color** icon, choose the desired color, and click **Close**.
    - Choose the **Text** or **Score** option to display the threshold label or the value for the risk after the assessment is run.
6. Click **Revert** to ignore all the changes or click **OK** to save the configuration.

Similarly, set up **Entity Compliance Configuration**, **Individual Risk Scale**, and **Program Risk Scale**.

Understanding Questionnaire Presentation Options

A Questionnaire Presentation Option is a set of options associated with a program. When assessments within a program are launched, only options visible to stakeholders enable the questionnaire presentation option feature. Using the Questionnaire Presentation Option, the user can set options such as "Allow user to skip questionnaires," "Allow user to skip resolved questionnaires," or "Allow forwarding of questions" to make it easy for stakeholders' to answer questionnaires, or enforce stakeholders to enter comments when answering a radio button or checking box type questions. Before creating a questionnaire presentation option, the user must be thorough with the entire assessment strategy and objective. All assessments created within a program are carried out using the same questionnaire presentation option. Any changes to preferences will affect assessments and questionnaires that are in progress.

The Questionnaire Presentation Option can view the Configuration menu only if the user has the Questionnaire Preferences View permission. To modify the default questionnaire presentation option or create a new questionnaire presentation option, the user must have the Questionnaire Preferences View and Manage permission.

The user can only delete unassigned presentation option sets.

Setting up Questionnaire Presentation Options

The following articles are settings in the questionnaire presentation option. Each section contains a table describing the fields and its purpose. Change the settings using a radio button, check box, drop-down list, or entering the test.

- Questionnaire Responder
- Questions
- Control Testing
- Supporting Information
- Actions
- Evidence
- Questionnaire Reviewer

Questionnaire Responder

Field	Description
Display the main logo in the questionnaire header	Select Yes to display the main logo in the questionnaires header.
Display the co-branding logo in the questionnaire header	Select Yes to display the co-branding logo in the questionnaires header.
Display the image of the subject in the questionnaire header	Select Yes to display the image in the subject questionnaires header.
FAQ URL for the questionnaire responders	Enter a web address where Frequently Asked Questions are posted.
Show more information link	Displays a 'more information' link where appropriate.
Show policy documents	Displays a link that allows the user taking the questionnaire to download the policy document attached to the control.
Distribute attachments	Attach all questionnaires in Excel format in the launch e-mail.
Maximum number of table rows shown in summary	The default is 5 rows.
Maximum number of table columns shown in summary	The default is 5 columns.

Questions

Field	Description
Use a rich text editor for text questions	A rich text editor allows questionnaire takers to highlight words and phrases with styles, such as bold and italic, and to control formatting of the text.
Allow scoring of text questions (in Review Stages)	Set to Yes to enable scoring of the answers to text-based questions.
Choice Template	The name of the program-level choice template.
Always use the Choice Template from the Program	Set to No to allow overriding the program-level choice template.
Display cell choices horizontally	For table questions. Set to No to display cell choices vertically.
Show multiple time series entry fields	Automatically provides multiple fields.
Group questions using each	Choose Control Objective or Control.

Control Testing

Field	Description
Show Design Test	Show the associated design test in the UI.
Show Effectiveness Tests	Show the associated effectiveness tests in the UI.
Show Documents	Show attached documents.
Show Evidence	Show attached evidence.
Show Findings	Show Findings.
Show Applicable Entities	Show entities that are applicable to the questionnaire.
Show Change History	Show the change history.
Design Test	Select a Choice Template to use with the design test.
Effectiveness Test	Select a Choice Template to use with effectiveness tests.
Effectiveness Tests cannot be rated until Design Test has passed	Select Yes or No
Overall control cannot be rated until all Effectiveness Tests have been rated.	Select Yes or No.

Supporting Information

Field	Description
Show comments	Displays a text field where the user can enter more information. When the questionnaire is exported to a spreadsheet, the user enters text in the My New Comments field. This text is merged with the Comments field when the spreadsheet is subsequently imported.
Comments section label	The title of the Comments section.
Require comments	Set to Yes to require that questionnaire takers provide comments when answering radio or checkbox type questions, or text questions when Allow text question scoring' is Yes.
Allow deletion of comments	Allow questionnaire takers to delete comments.
Show implementation	Displays the implementation information to the users.
Implementation section label	The Enter the title of the implementation section.
Show remediation	Displays a text field where the user can enter more information.
Remediation section label	The title of the Remediation section.

Actions

Field	Description
Allow flagging questions for followup	Displays the Follow up button that allows users to flag the question.
Allow exception requests	Displays the Request Exception button that allows users to create a new exception request while taking a questionnaire.
Allow forwarding of questions	Displays the Delegate button that allows users to delegate a question to other users while taking the questionnaire.
Allow splitting and merging of Questionnaires	Provides the option of delegating each group of questions to a different user, or merging split questionnaires back into one.
Allow primary owners to advance questionnaires	Allow questionnaire to be advanced by the primary owner, even if it not all questions are answered or resolved.

Evidence

Field	Description
Document upload required for evidence	Forces the user to upload a document as evidence.
Required evidence label	The label that displays next to the link for uploading evidence when required by the questionnaire choice settings.
Show evidence links for all choices	Provides a mechanism for optional evidence for choices. Note: Allows evidence to be uploaded for choices that do not require evidence.
Show evidence link when the user clicks on a choice	Select Yes or No.
Hide evidence links for these choices	Specify the choices that must not have evidence links.
Optional evidence label	The label that displays as the link text for "Show evidence links for all choices."
Provide evidence descriptions automatically	Inserts the question title into the description field.
Allow data feeds to be used as evidence	Questionnaire takers can display and attach data feeds associated with the Entity that is the target of the assessment
Evidence must come from the same program	Only allow evidence that is associated with the current program.
Evidence must be owned by questionnaire responder	Only allow evidence that is owned by the questionnaire responder.
Allow adding evidence to the Evidence Repository	Allows you to hide or display the option to select evidence from evidence repository.
Allow selecting evidence from document repository	Allows you to hide or display the option to select evidence from document repository.
Allow selecting evidence from the Evidence Repository	Allows you to hide or display the selecting an evidence from evidence repository.
Allow selecting evidence from the Document Repository	Allows you to hide or display the selecting an evidence from document repository.

Questionnaire Reviewer

Field	Description
Show the discrepancy report	Displays conflicting answers if the questionnaire taker's answers differ.
Show mitigation requests	Displays the icon which indicates that a mitigation for the subcontrol has been requested.
Show if a question changed	Select Yes or No.
Review resolutions	Displays the resolutions associated with the questionnaire. The resolution list is displayed in the questionnaire if the stage is marked as a Review stage.
Show risk score in header	Displays the normalized risk score (10 - compliance score) of the questionnaire taker's answer to the question. **Note**: Risk scores apply to compliance assessments only.
Show risk report	Enables the Risk Report button that allows questionnaire responders to display a list of risks while taking the questionnaire.

About Ticket Management Preferences

The **Ticket Management Preferences** page manages the list of ticket dispositions. A ticket disposition is a text string such as "Pending customer confirmation" or "Under investigation." You can use a ticket disposition to label a ticket's status. You can access the **Ticket Management Preferences** page only if you have the Ticket Manage permission.

When a ticket reaches it's due date, it follows the escalation configuration by automatically escalating to additional stakeholders who are notified about the ticket's overdue status.

Ticket Management Preferences allow the user to disable escalations for tickets with a specified disposition. For example, the user may not want to escalate overdue tickets if the disposition is "Pending customer confirmation."

To add to the list of ticket dispositions:

1. Go to **Configuration** > **Ticket Management Preferences** and then click **Edit**.
2. Click **Add**, enter a new disposition in the **Ticket Dispositions** text box, and then click **OK**.
3. Click **Refresh** to update the **Do not escalate when disposition is set to** drop-down list.
4. Click **Save** after you finish modifying a ticket disposition .

To change a ticket disposition:

1. Go to **Configuration** > **Ticket Management Preferences** and then click **Edit**.
2. Click the disposition name to change, update the name, and click **OK**.
3. Click **Refresh** to update the **Do not escalate when disposition is set to** drop-down list.
4. Click **Save** after you finish modifying a ticket disposition.

To delete a ticket disposition:

1. Go to **Configuration** > **Ticket Management Preferences** and then click **Edit**.
2. Select the disposition, click **Delete**, and confirm the action.
3. Click **Refresh** to update the Do not escalate when disposition is set to drop-down list.
4. Click **Save** after you finish modifying a ticket disposition .

To disable escalation for a specific disposition:

1. Go to **Configuration** > **Ticket Management Preferences** and then click **Edit**.
2. Select a disposition from the **Do not escalate when disposition is set to** drop-down list and click **Save.**

Entities

For customers using the RiskVision solution to build and deploy a risk and compliance management solution, there are two main components to be concerned with:

- The first component is determining the controls and subcontrols that you want to enforce or monitor across your organization, for example to measure security risk across the various computers and other IT assets/entities across your organization.
- Using the RiskVision solution , you can choose from standards-based risks and controls already provided in the Resolver content library. You can then add and combine controls to create a customized “Organization Content” collection of controls that are used in creating programs, performing entity assessments and risk evaluation across your organization.
- The second component very closely tied to controls is the collection of your organization’s combined entities or resources. Accessing groups of entities from the RiskVision solution, you can apply or evaluate controls for selected entities included in an assessment, measure or monitor their compliance, and calculate associated risk. Resolver provides the capability to capture information and inventory nearly any item of value within your organization (referred to as entities), from IT resources such as computers, systems, and applications to non-IT resources such as property, business equipment, business operations, people, vendors, and processes. In addition, using methods such as ERM, you can model the processes, sub processes, and business objectives that you want to evaluate for risk.

Entity Types

For customers using the RiskVision solution to build and deploy a risk and compliance management solution, there are two main components to be concerned with:

Entity Types

The following list describes the predefined entity types:

Icon	Entity	Description
	Account	Account or login information pertaining to privileged access of financial accounts, computer applications, etc.
	Application	Software applications that are critical to a company's operation, for example, financial reporting, CRM, procurement, change management, incident management, and database applications.
	Computer	Computers, servers of different types (file, database, authentication), notebooks, laptops, etc. Predefined subtypes such as Desktop and Notebook.
	Data	Specific data that may be critical to operations and are important enough to be classified and tracked on their own, for example, account numbers, customer lists, documents containing product formulas, market-sensitive information, intellectual property, etc.
	Device	Other network devices such as routers, switches, printers, VPN, etc.
	Domain	An Active Directory domain.
	Financial	Entities related to financial resources such as stocks, bonds, cash, etc.
	Group	An Active Directory security group.
	Intangible	Entities such as intellectual property, product secrets and proprietary information, etc.
	Location	Physical or geographical locations, real estate, offices, etc.
	Mobile Device	Mobile devices are entities, such as mobile phone, personal digital assistant (PDA), and much more that are allowed by organizations under the Bring your own device (BYOD) policy. Employees bring their mobile devices to access email, file servers, and critical applications. Track and assess all employee-owned devices by creating or importing a Mobile Device entity type.
	Network	Computer network infrastructure like subnets and wireless networks.

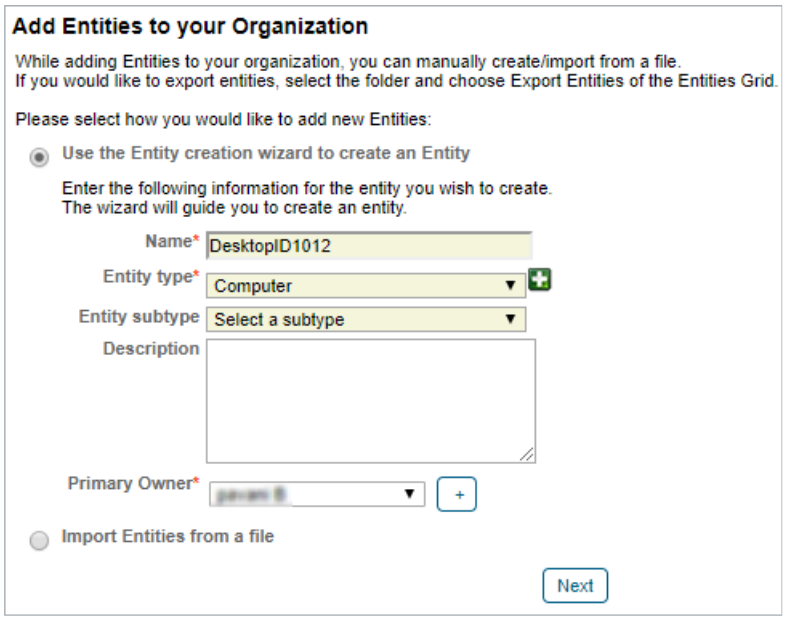
Icon	Entity	Description
	Network Device	Network devices such as firewall, routers, modems, etc.
	Organizational Unit	An Active Directory organizational unit.
	Person	Individuals within an organization where compliance and risk are managed by the RiskVision system. Also linked as users of applications, processes, documents, and storage.
	Physical	Non-computer entities such as mechanical, manufacturing, and production equipment, vehicles and capital goods.
	Process	Business operations such as order entry, payment transaction, accounts payable and receivable, shipping and receiving, RMA, etc.
	Project	Shows individual entity assessments defined as part of a larger program.
	Vendor	Organizations or entities outside your own enterprise for which you want to apply and monitor control compliance and calculate risk.

Create a New Entity

To create a new entity, you must have the Entity View and Entity Create permissions. The entity wizard takes you through the configuration of basic entity settings. For computer type entities, see Creating a New Computer Type Entity.

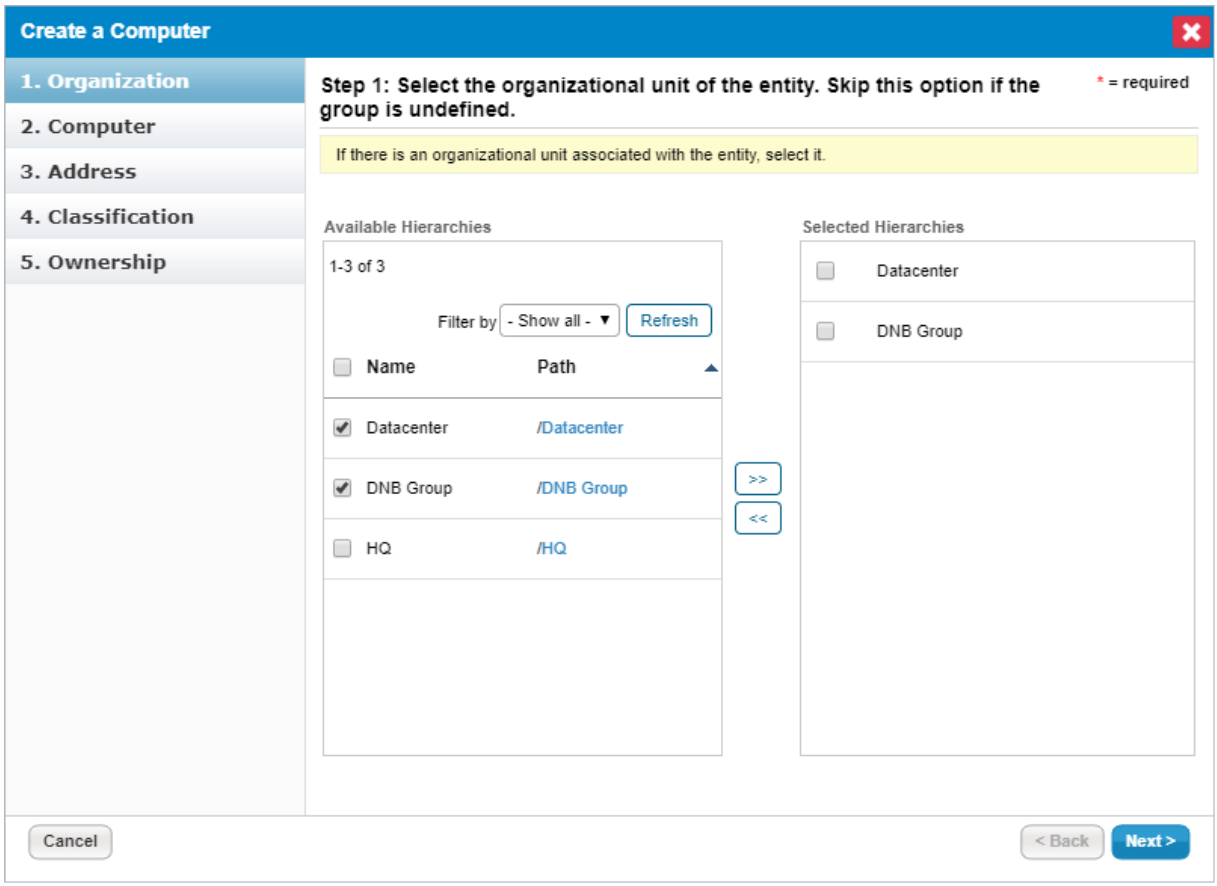
To create a new entity:

1. Go to **Entities** > **Entities** and select an entity group.
2. Click **New**. The **Add Entities to your Organization** page is displayed.



The Add Entities to your Organization page.

3. Set the name, type, and owner and then click **Next**. The **Create a Computer** wizard appears, showing the **Organization** wizard page.

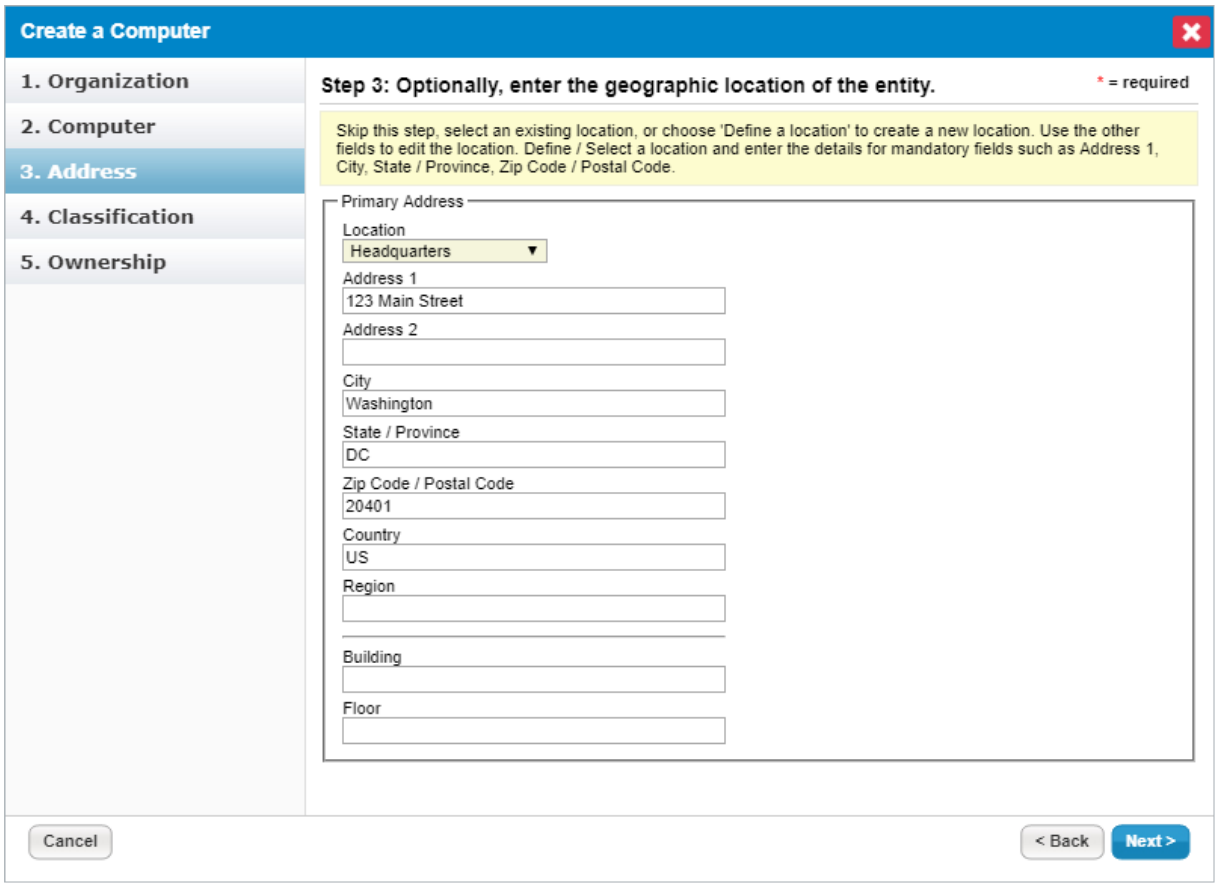


The Organization wizard page.

4. Select the organizational group to automatically set the organization fields. Skip this step if the organization has not been configured.

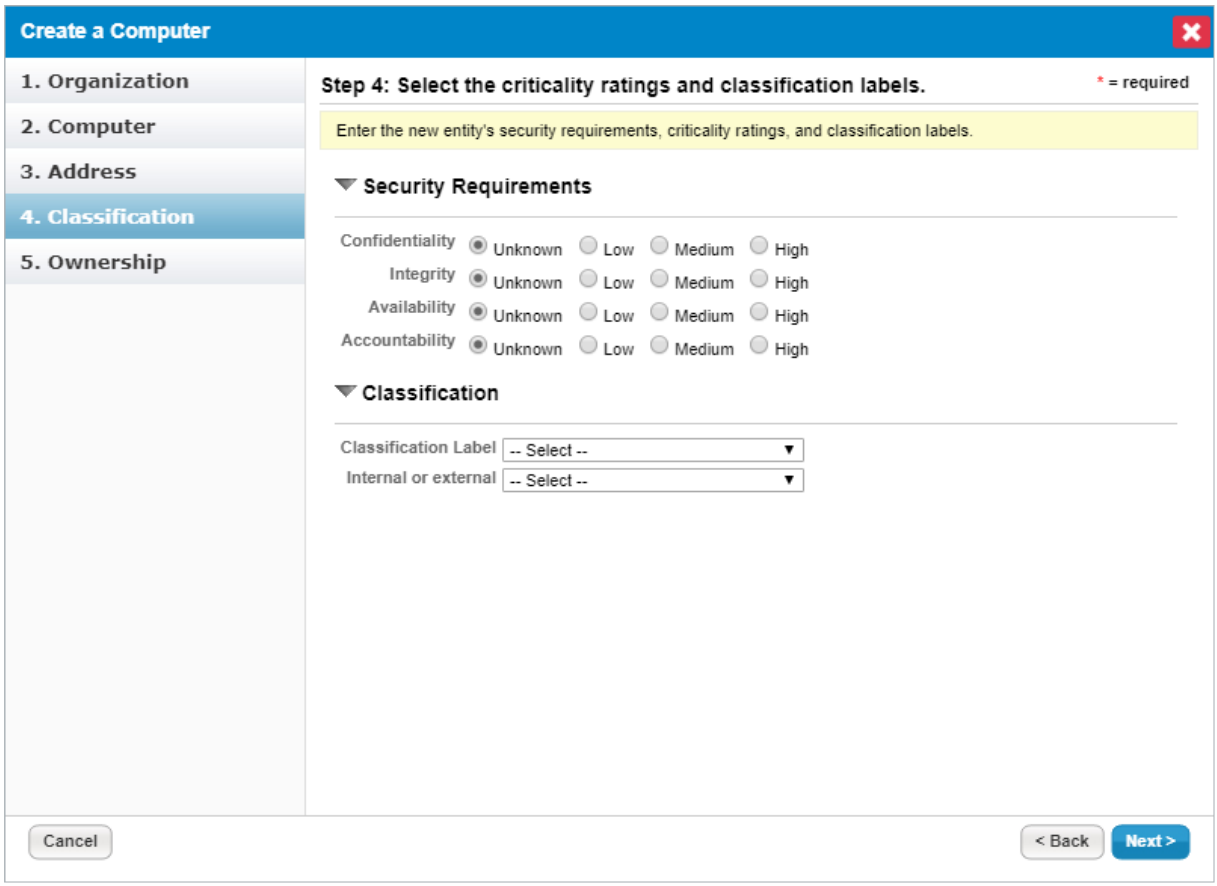
   For more information on organizational groups, see Defining a New Organization.

5. Click **Next**. Click **Next** again. The **Address** wizard page appears.



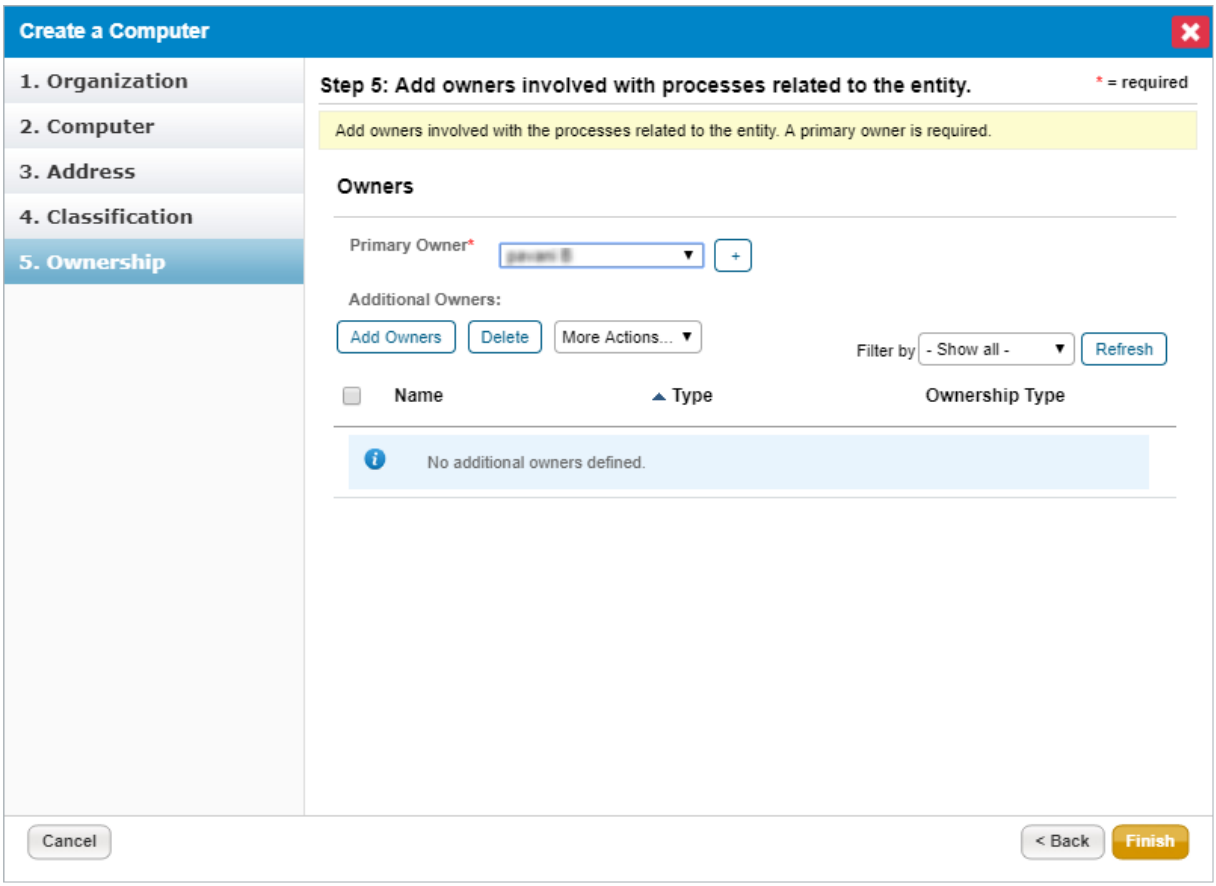
The Address wizard page.

6. Enter the address and click **Next**. The **Classification** page is displayed.



The Classification wizard page.

7. Select the criticality setting. The **Ownership** page is displayed.



The Ownership wizard page.

8. Change the primary owner and assign other users as owners. See Configuring Owners. While it is possible to import an entity without a primary owner, or to delete an entity's primary owner, many operations require that each entity has a primary owner. Creating a program that references an entity without a primary owner, for example, will cause an error.

9. Click **Finish**.

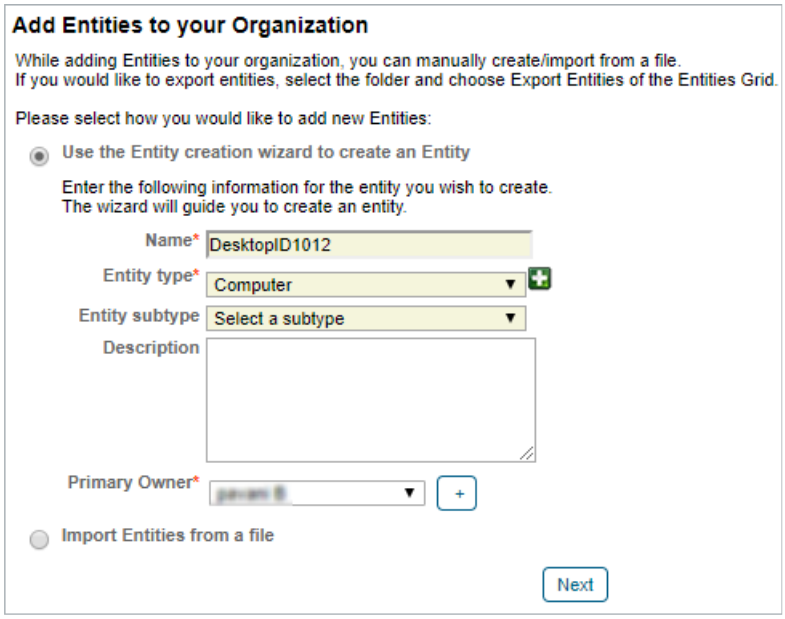
The entity is added to the system. If the entity is part of a dynamic group, an assessment automatically launches the entity depending on the program settings.

Creating a New Computer Type Entity

The entity wizard takes you through the configuration of basic entity settings.

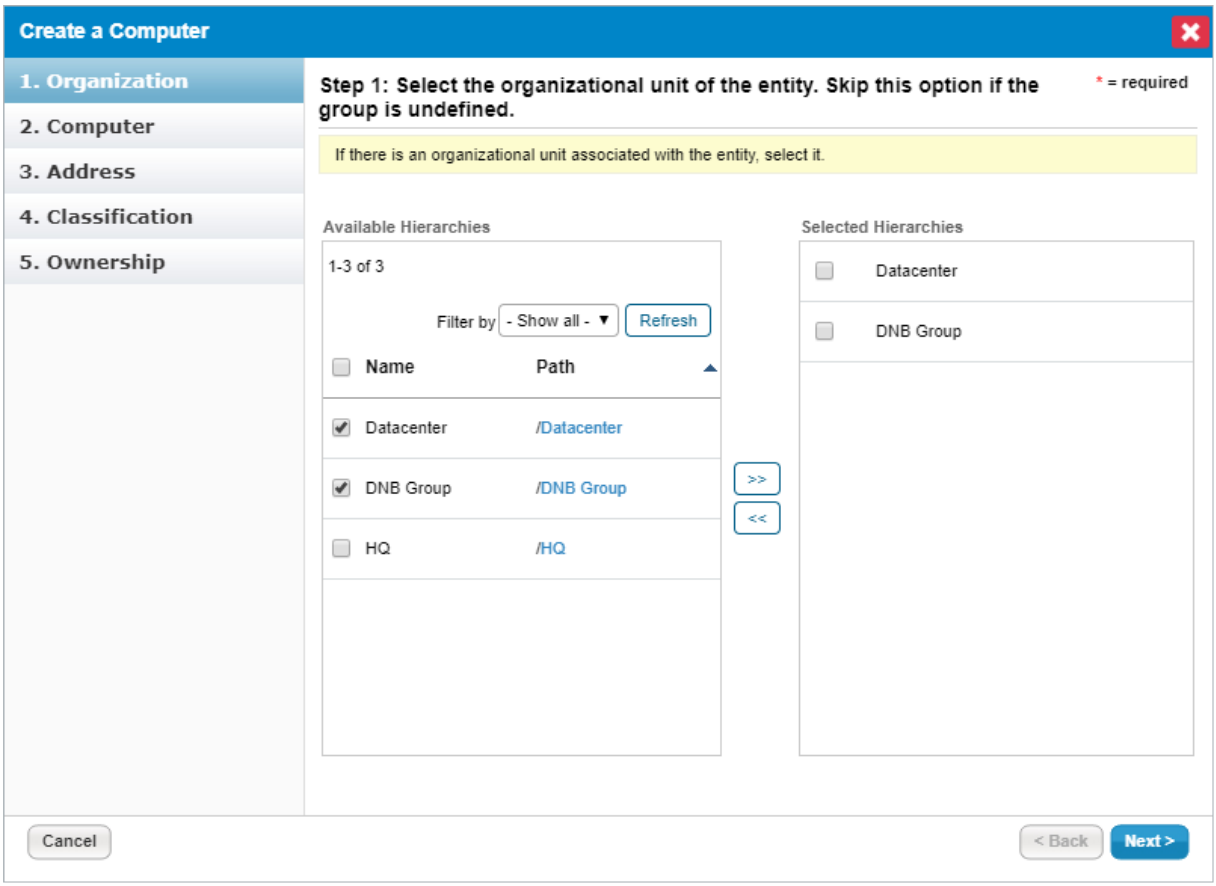
To create a new entity:

1. Go to **Entities**> **Entities** and select an entity group. The Entities page is displayed.
2. Click **New**.



The Add Entities to your Organization page.

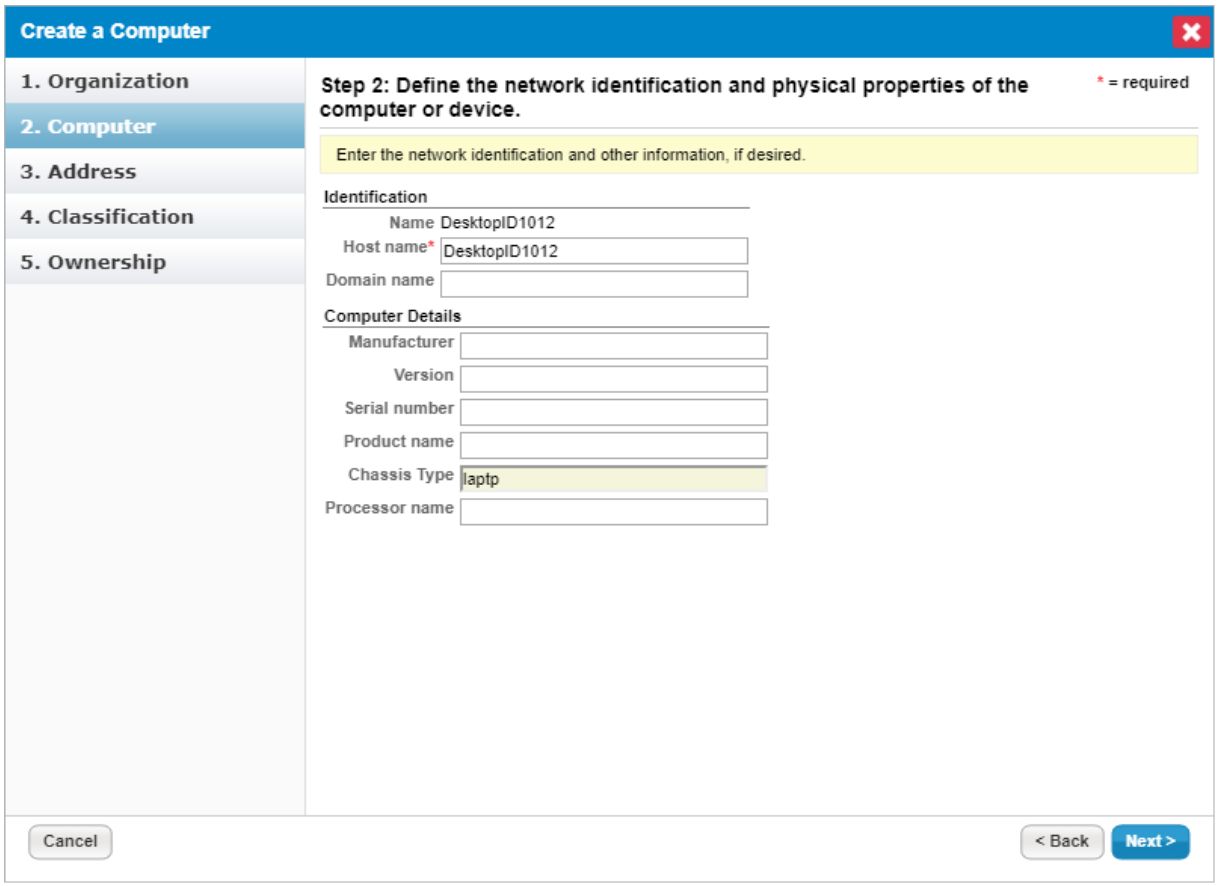
3. Select the **Entity type**. Enter the name, select the owner, and then click **Next**.



The Organization wizard page.

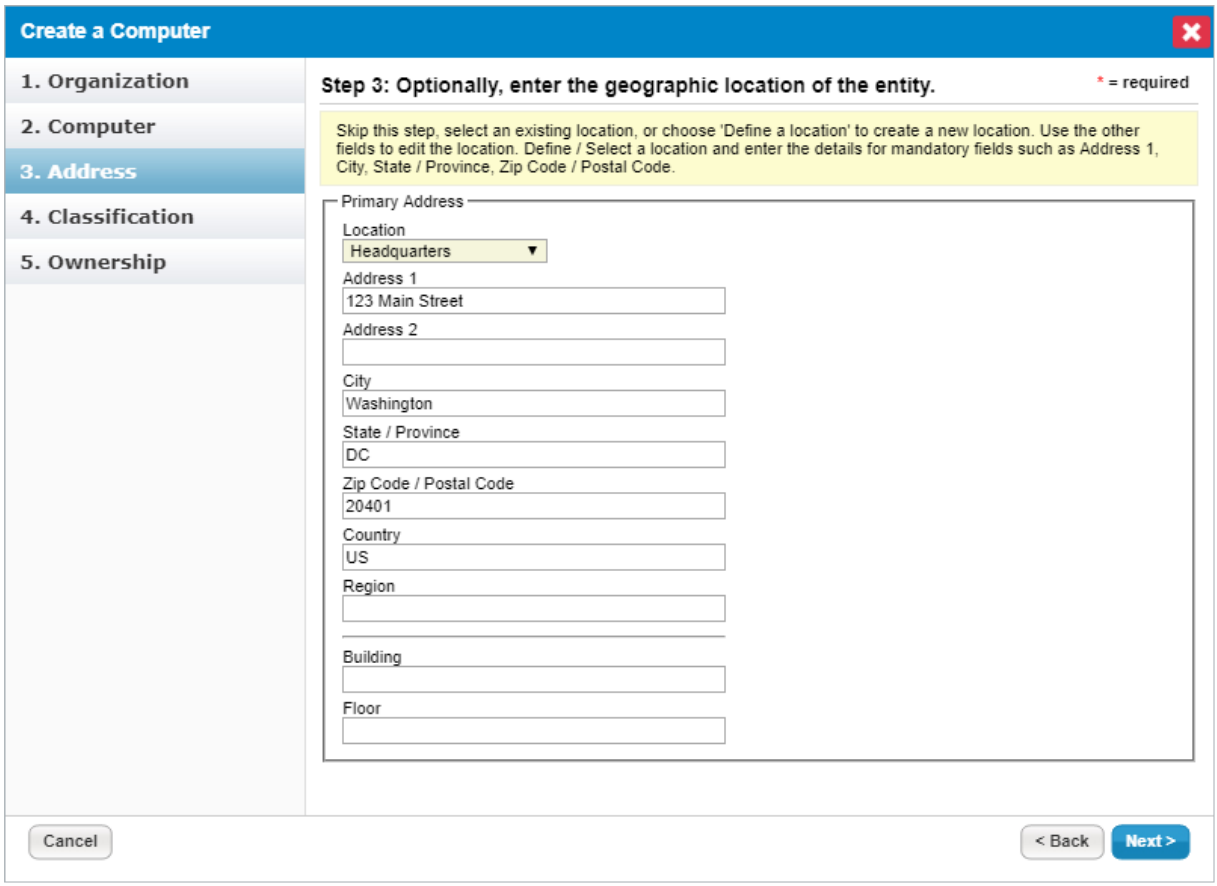
4. Select the Organizational group to automatically set the organization fields. Skip this step if the organization has not been configured. For more information on organizational groups see Defining a New Organization.

5. Click **Next**. The **Computer** wizard page appears.



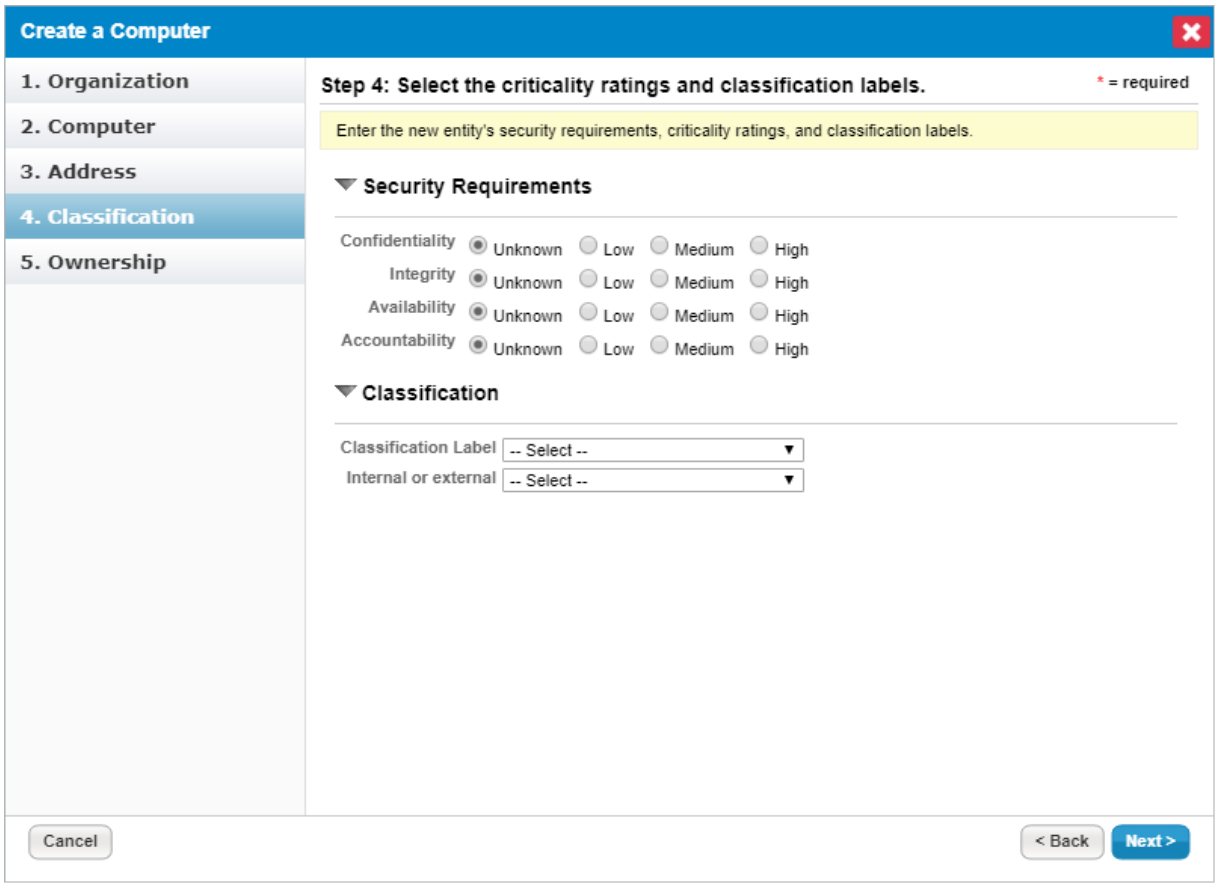
The Computer wizard page.

6. Enter the **Identification** and **Computer Details**, then click **Next**.



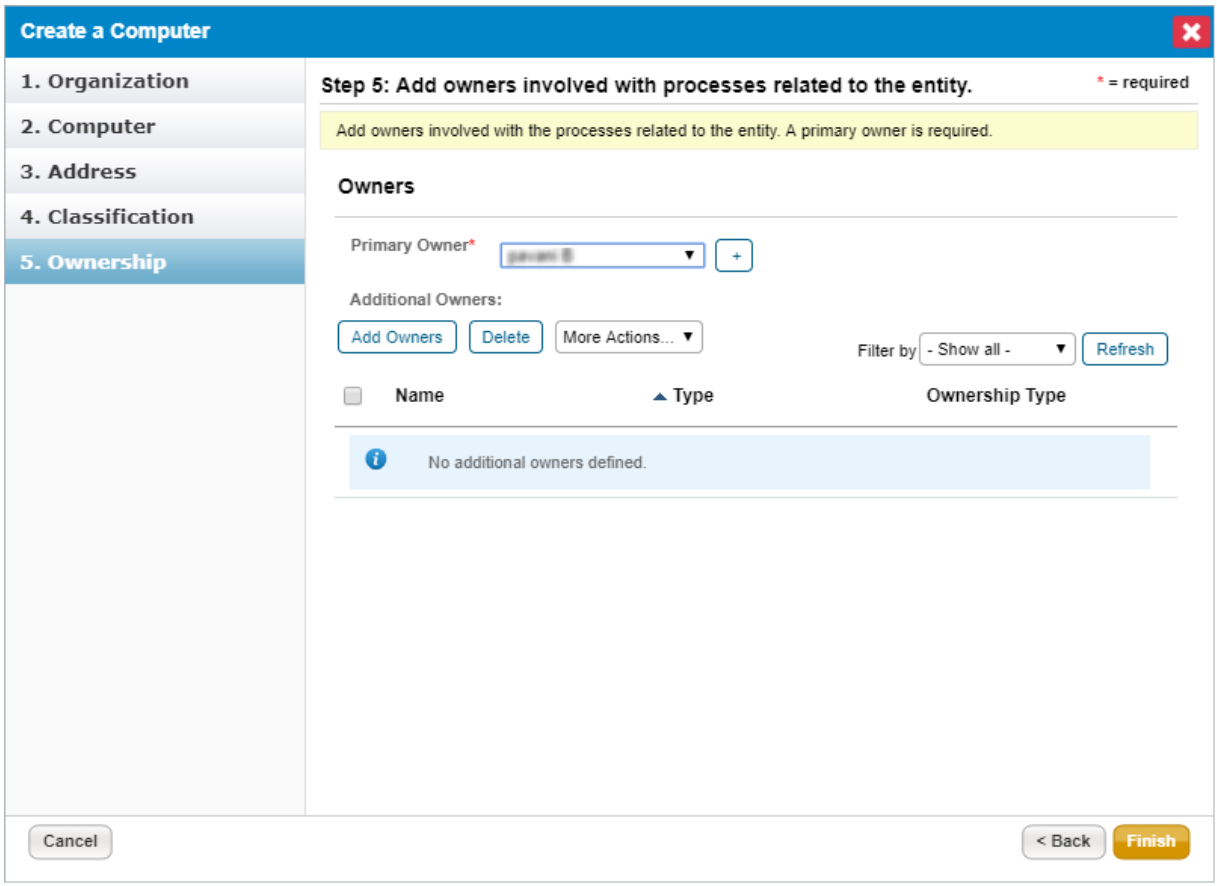
The Address wizard page.

7. Enter the address, then click **Next**.



The Classification wizard page.

8. Select the criticality setting. The **Ownership** wizard page appears.



The Ownership wizard page.

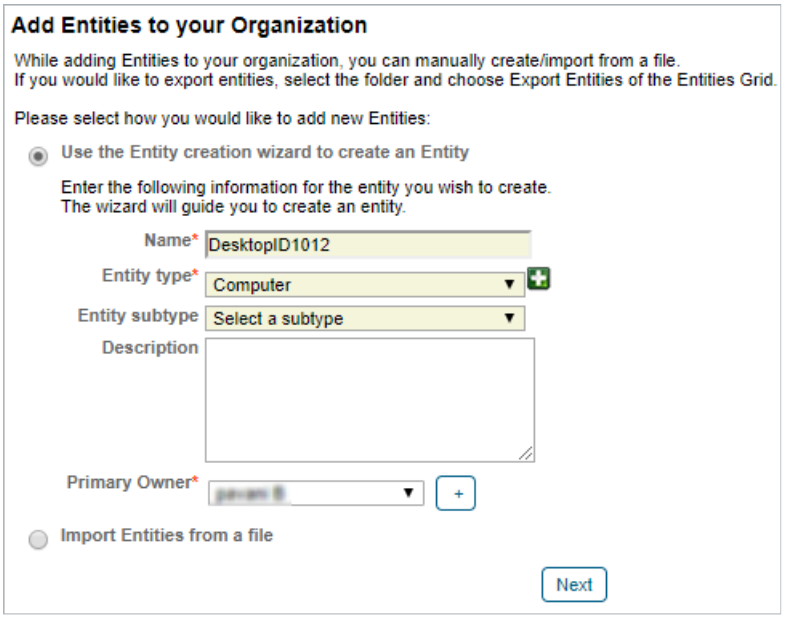
9. Change the primary owner and assign other users as owners. See Configuring owners for more information.

10. Click **Finish**.

The computer type entity is added to your system. If the entity is in a dynamic group that is included in a program, an assessment may automatically launch for the entity, depending on the program settings.

Setting the Name, Type, and Owner for an Entity

Set the following information on the **Entity Wizard Name and Owners** page:



The Entity Wizard Name and Owners page.

Setting	Type	Description
Name	string	Enter a name that Identifies the entity in programs, assessments, questionnaires, tickets, exceptions, incidents, and reports.
Entity type	Default entity types	Displays a list of predefined entity types.
	Define new type	Displays a text box where you can enter up to 255 characters. The new type is added to the list of entity types when you save the entity.
Entity subtype	Define new type	(Optional) Displays a text box where you can enter up to 255 characters. The new subtype is added to the selected type and displays as an option the next time you select the type.
Description	string	Enter up to 1024 characters that summarize the entity. Displays in the entity in list and detail pane.
Primary owner	System user	Select a user.

About Discovered Entities

The Discovered, Managed and Unmanaged dynamic groups provide dynamic subgroups that categorize entities by entity type, for example, application, computer, and so on. Entities first show up in the Discovered dynamic group when they are discovered, for example, using a connector, or created from imported entities. Discovered or Unmanaged entities can be moved to the Managed group by selecting the Manage in the Status pull down list in the General detail display for a particular entity. You can also click on the Manage node or any Manage node subgroup and choose the "Start Managing These Entities" option from the right-click context menu. Also, from the list pane display for a selected group, you can choose Manage Entities from the More Actions menu.

Entities require a minimum of a hostname or IP and a domain to be included in displays of Discovered or Managed entities.

Display Entity Details

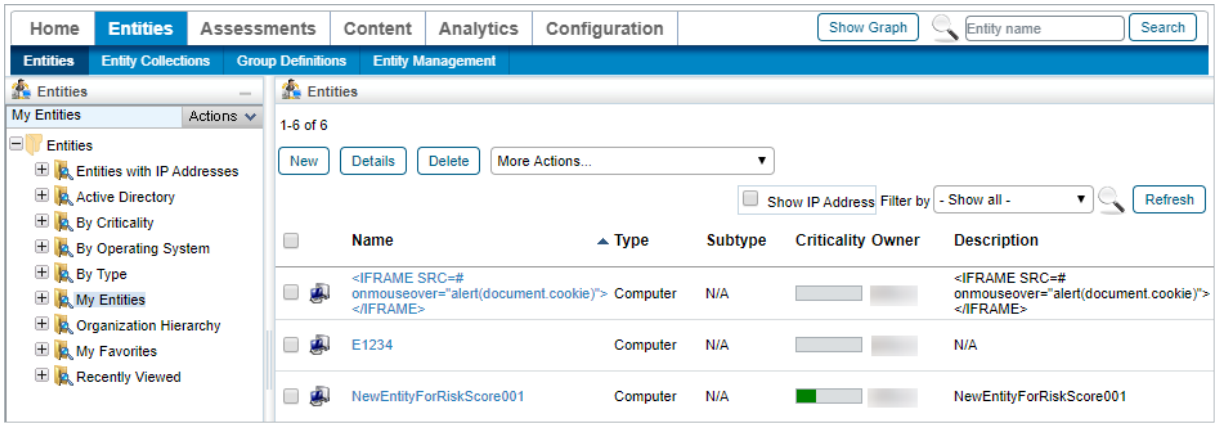
There are a few ways to open the entity details pane from other menus, such as opening the**Assessment Details** page. This section explains how to open the details pane from the **Entities** menu. To view and search an entity, you must have the Entity View permission. In general, entities are visible only to their primary owners. However, if a primary owner nominates another user as a business owner for an entity, then the business owner will be able to view that entity. Find an entity by entering part or all of the name in the search field, then click **Search**.

The search field.

To display the entity details pane:

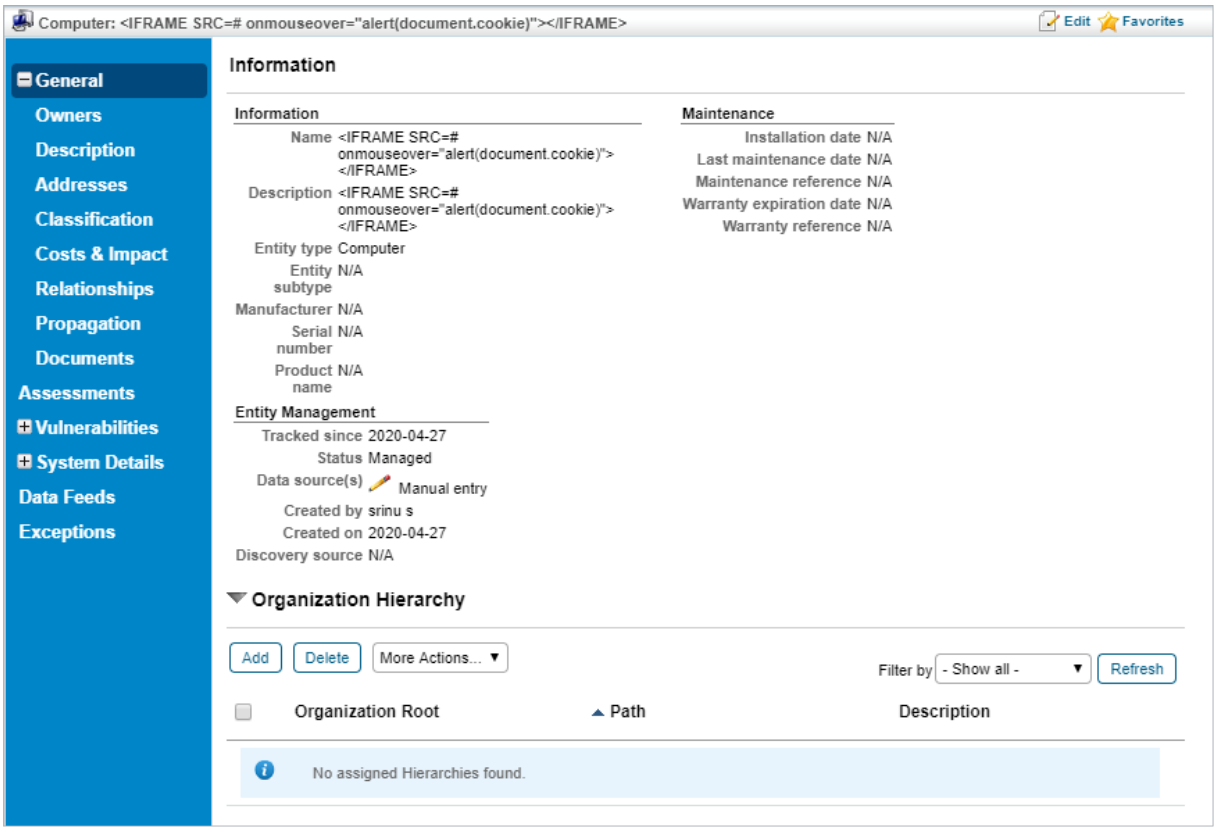
1. Go to **Entities** > **Entities**.

2. Click a group, such as **My Entities**, to display the Entity list.



The My Entities list of entities.

3. Select an entity, then click **Details** to open the **Entities Details** pane.



The Entities Details pane.

Entity Details Tabs

Entity details are categorized into a set of tabs. The available tabs will depend on the entity type. You can edit these tabs if you have the Entity View and Entity Update permissions. To edit entities created by other users for which you have not been named an additional owner, you must have Entity View and Entity Update all permissions. You can update the **Classification** tab if you have Entity View and Entity Manage permissions.

These are the available entity details tabs:

Tab	Attributes
General	All entity types have a General tab. Attributes include name, type and subtype, and other identifying fields. Status can be Managed or Discovered. The entity's Organization Hierarchy is described here.
Owners	Entities have a primary owner and a grid of additional owners. Click Add Owners to associate more users with this entity.
Description	The Description provides additional type-specific fields, such as Publisher and Version, for applications. The profile information is listed on this tab, if a matching profile is found.
Addresses	A grid of physical addresses, if any, associated with this entity. Click New to define a new physical address. Use the following property to delete an entity's address: com.agiliance.asset.deleteAddress=true.
Classification	Entities can be classified in many different ways, such as Business Criticality, CIAA (Confidentiality, Integrity, Availability, and Accountability), or tags. There is a Change History associated with entity classification.
Cost & Impact	This tab associates specific costs and importance metrics with a particular entity. Costs include attributes such as "business value per hour ($)," and "average remediation time (days)." Important attributes include "number of users."
Relationships	A grid listing the other entities with which this entity has a relationship. Click Add relationship to specify how an entity must relate to another entity. Also, see Relationship Explorer. For a Person-type entity, a relationship is listed in the Teams tab.
Propagation	This tab displays the programs in which the entity is inheriting and propagating the controls. Because the entity is related to another entity, the control results are propagated after answering the assessments.
Documents	The Documents tab is a grid listing documents, web links and network path associated with this entity. Click New Document to upload a document related to the entity, such as a contract for a Vendor type entity, or click New Web Link / Network Path to record an external link. Note: By default, users with the Entity view+create+update permission and without any Document Repository-related permissions can attach or delete documents on Entities, but when users are using the new Global Document Repository feature to attach a document from the Document Repository to an entity, then Document Repository-related permissions and ownerships are required.
Assessments	A grid of the assessments associated with this entity. Click New to create a new assessment.
Automation	Entity types, such as Computer or Application, have an automation tab that displays target type parameters based on the entity type, subtype, and product name.
Vulnerabilities	For some entity types, the Vulnerabilities tab provides a summary of vulnerabilities found by scanners or users. Computer and Vendor types, for example, list vulnerabilities on different tabs.
Vulnerabilities List	The Vulnerabilities List tab is a grid of all vulnerabilities found by scanners or entered manually by users. To create a new vulnerability and associate it with the entity, click either New or Import. To assign an existing vulnerability to this entity, click Assign. For more information, see Assigning Vulnerabilities. Some entity types, such as Vendors, do not have associated vulnerabilities.
Inferred	The Inferred tab lists the vulnerabilities that are associated indirectly with an entity type, such as Computer and Network Device.
Comp Controls	The Comp Controls tab lists each of the vulnerability compensation controls attached to the entity. Users can add new compensating controls, delete them, add notes, and view the recent changes made. Note: Only users with the Entity View, Threats and Vulnerabilities View, and Vulnerability

	Compensating Control Update permissions can view, add, update, and remove vulnerability compensating controls from the entity or add comments. All updates and changes to a vulnerability compensating control will be logged in the Change History section.
System Details	Certain types and subtypes of entity, such as Computers, have a number of tabs organized under the heading 'System Details.' These tabs include: • Network • Ports • Services • Applications • Patches • Network Shares • User Accounts • Membership
Data Feeds	A grid listing the data feeds associated with the entity, if any.
Exceptions	The Exception tab is a grid of all exceptions, including the controls, findings, and vulnerabilities related to the entity that the tab is associated with.

About Ownership Types

Ownership types link workflow stage stakeholders to the system users who are assigned to an entity or policy. This allows processes such as programs, tickets, and policy pack approval to run automatically. You can restrict user access based on the role of the user and the type of ownership.

Different workflow stages are assigned automatically to different object owners:

- Ticket, Assessment program, incident, and exceptions are processes for entities. Therefore the workflow stage stakeholder is linked to an entity ownership type.
- Content packs and control objectives contain content objects such as Controls and Questionnaires that also have owners.

You can also assign users and teams as stakeholders in a workflow. For more information, see About workflows. Adding, modifying, or deleting an ownership type requires you to have the Tenant Configure permission

Adding A New Ownership Type

Add ownership types to create a new mapping between workflow stages and system users you want to automatically assign to workflow related actions.

To create a new ownership type

1. Go to **Configuration** > **Ownership Types**.
2. Click **New**.

   The **Configure Ownership Type** dialog appears.
3. Enter the ownership configuration:
   - In the **Name** field, type name that uniquely identifies the ownership type.
   - In the **Display Name** field, enter the name that you want to display in ownership assignment dialog.

     For example, the display of an Entity type appears in the list on the workflow stage stakeholder owner roles tab.
   - Select the type. Entity: Assign to Entities and the Assessment, Ticket, Exception, and Incident workflows. Policy: Assign to policy packs and policy workflows.
   - Select a role to limit which users can be assigned as the ownership type. The user must have at least one of the roles.

     When no roles are selected, any user can be assigned.
4. Click **OK**.

The new ownership type displays in the list.

Deleting an Ownership Type

You can delete unused ownership types only. Change the ownership type entity and policy owners or remove the ownership type from the workflow stage.

To delete an ownership type:

1. Go to **Configuration** > **Ownership Types**.
2. Select the ownership types.
3. Click **Delete**.

The ownership type is removed from the list and is no longer available on corresponding policy, entity, and workflow pages.

Changing the Setting of an Ownership Type

You can change the display name and role restrictions. Modifying role restriction only affects new ownership assignments.

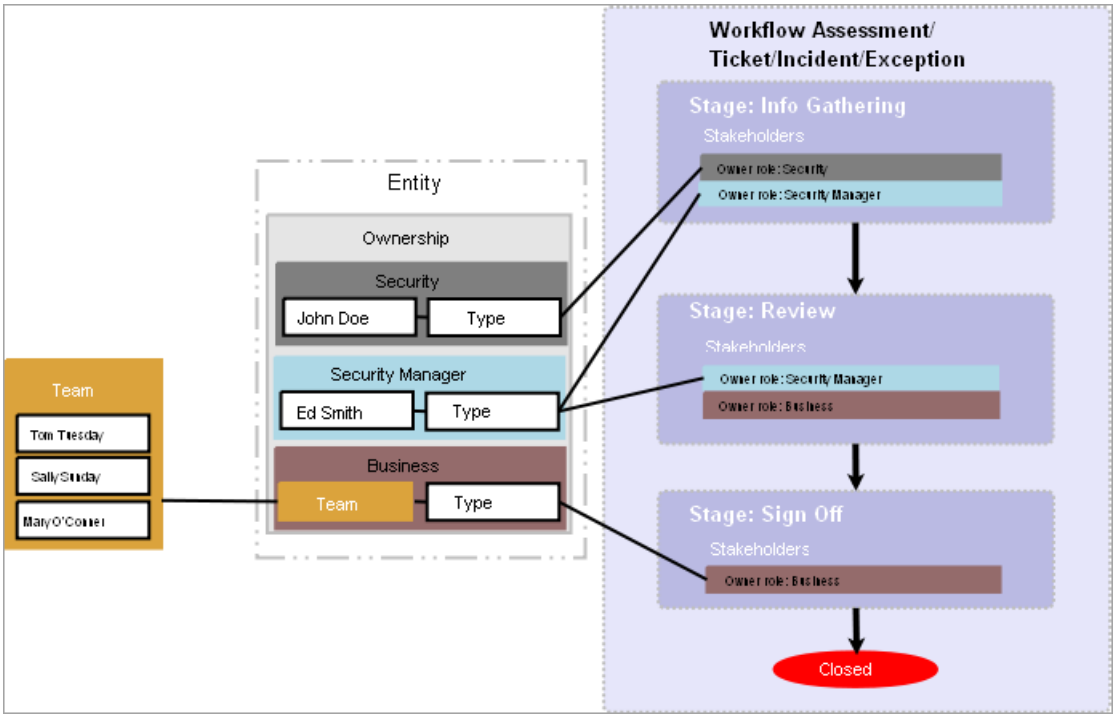
To modify an ownership type settings

1. Go to **Configuration** > **Ownership Types**.
2. Select the ownership type.
3. Click **Edit**. The **Configure Ownership Type** dialog appears.
4. Modify the configuration and click **OK**.

The display name is updated immediately. Role restrictions apply to the next owner assignment.

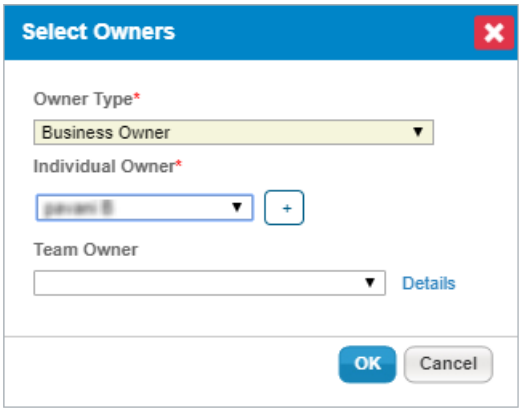
Configuring Owners

Entity ownership allows RiskVision to automatically assign stakeholders for workflow stages, such as assessments, when the entity is selected for the process.



To modify owners:

1. Click an entity to open.
2. Go to **Ownership**, then click **Edit**.
3. Perform one of the following actions:
    - To change the primary owner, select a different user from the primary owner dropdown.
    - To remove an owner, click **X** in the top-right corner of the window.
    - To add another user, click **Add Owners**.



The Add Addinal Owners dialogue.

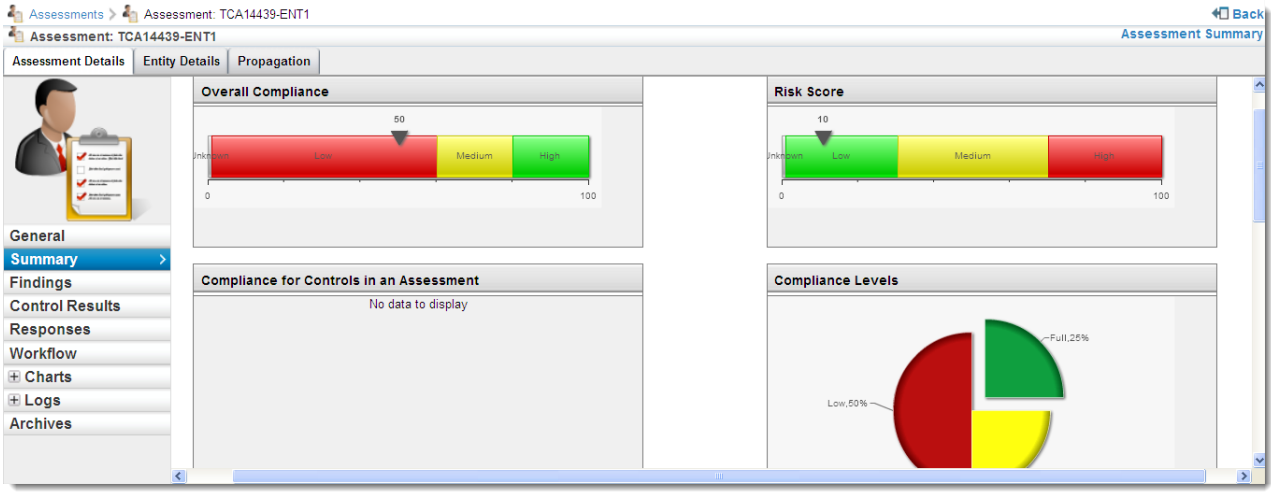
4. Select the ownership type. For more information, see About Ownership Types.
5. Select a user from the individual user dropdown. Skip this option to assign a team only.

6. Select a team from the Team drop-down. Skip this option to assign a user only.
7. Click **OK**.
8. Click **Save**.

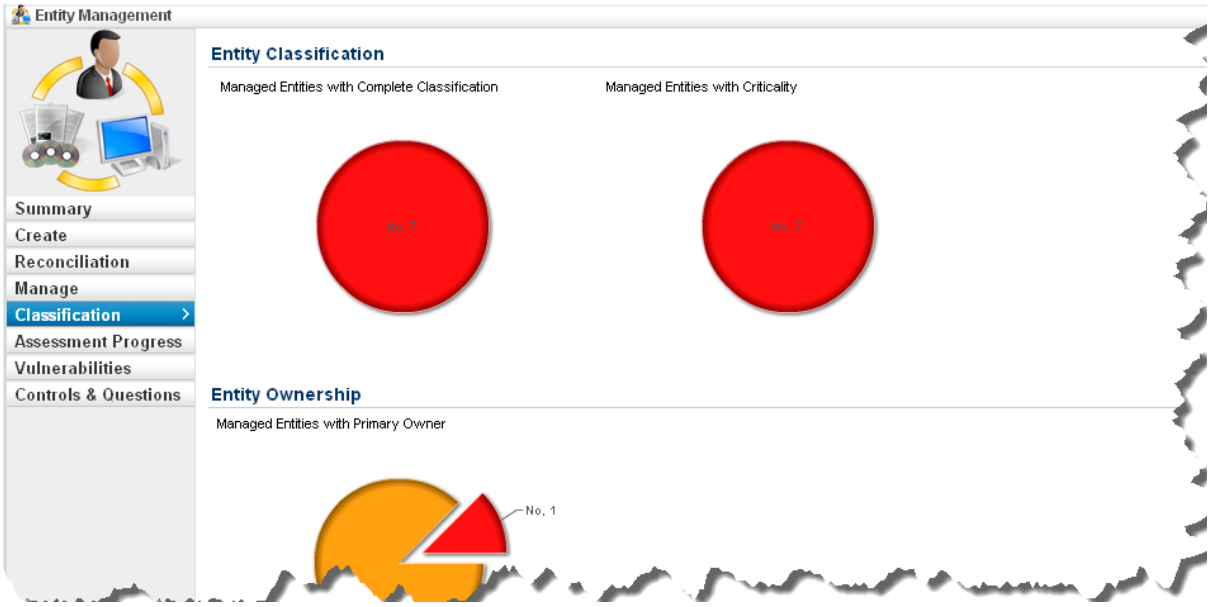
Configuring Entity Compliance and Criticality Ranges

The Range option controls the numeric score for the low, medium, and high or VL (very low), L (low), M (medium), H (high), and VH (very high) selections a user can make on various RiskVision pages as well as the color and ranges that display in graphs and charts on dashboard pages and reports:

- **Compliance range**: Controls the numeric values for displaying overall compliance levels, such as on the Assessment Details > Control Results > Compliance Summary pane.

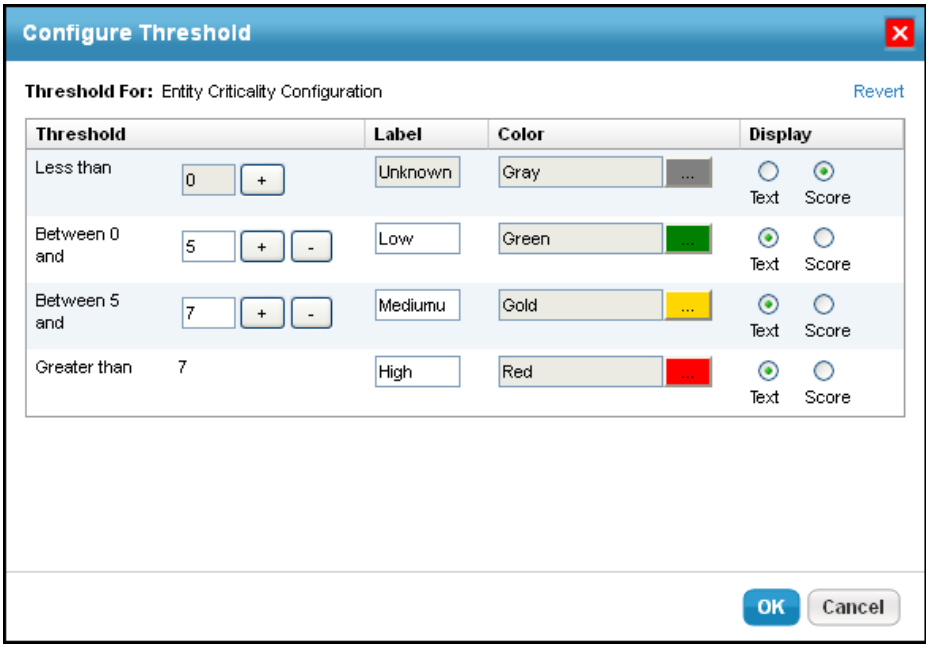


- **Criticality values:** Controls numeric values for the choices on Entity Details > Classification > Security Requirement. The Business criticality is an average of the confidentiality, integrity, and availability security requirement settings.It displays on the Assessment Details page and in reports.



To modify a range:

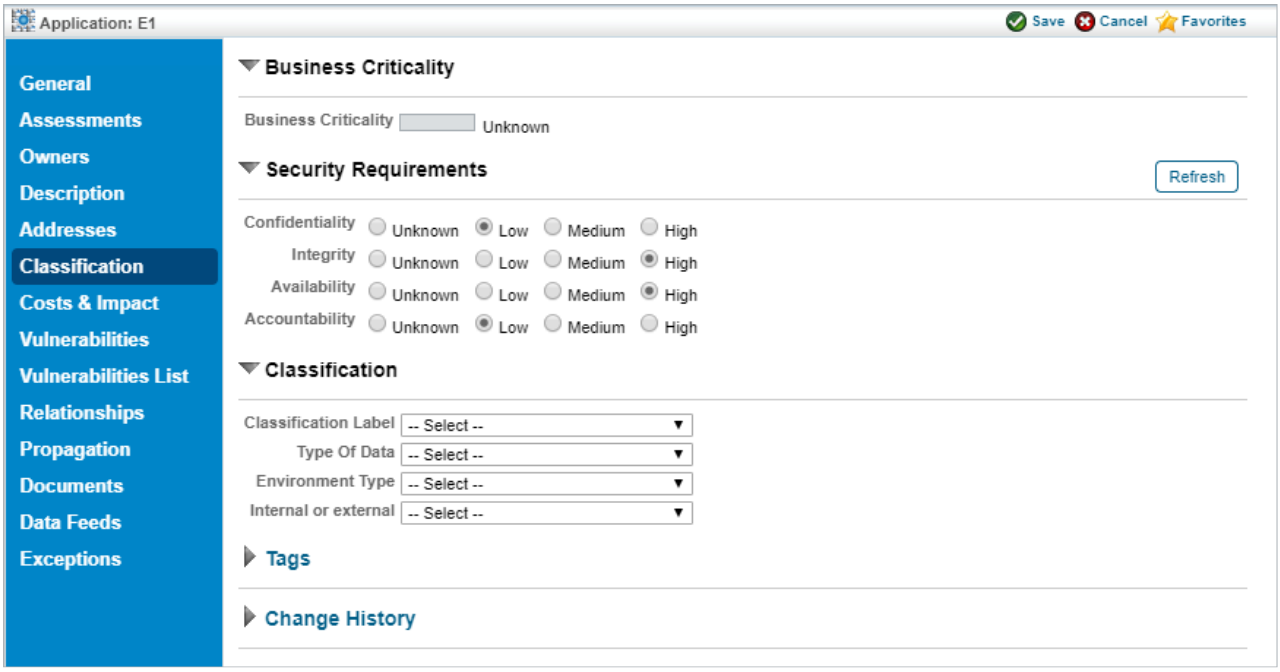
1. Go to **Configuration**> **Entity Configuration**.
2. Click **Ranges**.



3. Choose **Entity Criticality Configuration** and click **Edit**.
4. If you want to increase the Threshold range, click **+** (plus symbol).
5. Click **-**(minus symbol) to decrease the Threshold range. The color will change based on the selected Threshold range.
6. Click **OK**.

Setting the Criticality

The **Security Requirements** section allows you to manually set the entity criticality.



The Security Requirements section of the Classification tab.

For discovered entities, you can configure a Control Target Profile to automatically set this value.

Criticality is not set when importing vulnerabilities from a saved XML file, even if the vulnerabilities were exported with criticality information. Vulnerabilities can be imported into other entities, and the criticality cannot be assumed.

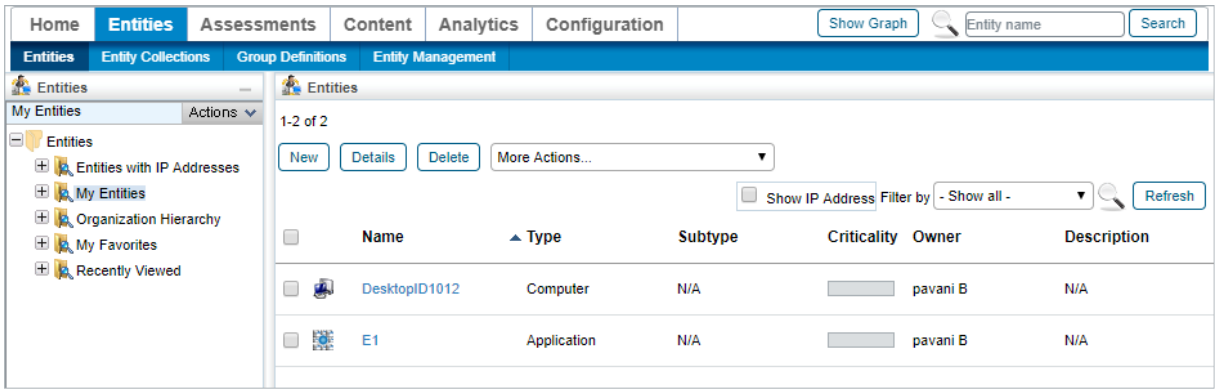
Clicking on the **Refresh** button will manually update the confidentiality, integrity, availability and accountability values of the entity.

These settings are used for:

- Automatically reassessing entities;
- Calculating the simple risk and compliance scores; and
- Calculating the Business Criticality score.

To set the criticality rating:

1. Go to **Entities** > **Entities**.
2. Select a group.



The Entities list.

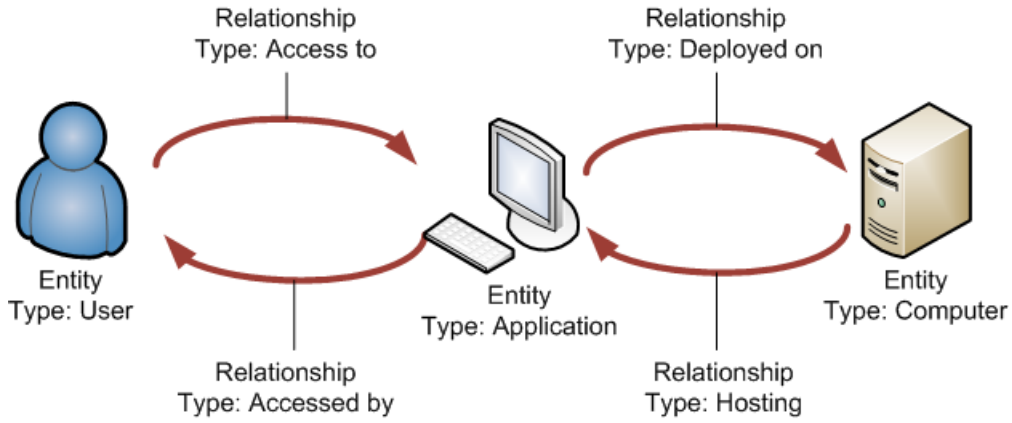
3. Select an entity, then click **Details**.
4. Click the **Classification** tab, then click **Edit**.
5. Select the desired radio button in the **Security Requirements** section,
6. Click **Save**.

Related scores and settings are immediately updated.

About Entity Relationships

Entities are related to one another, usually in understood ways. An application is hosted on a particular computer; a user has access to a certain application, and so on. In RiskVision, entity relationships model these associations. Once the relationships between entities are understood by the system, you can propagate controls, risk scores, and other aspects of entities within a given program, for use in dashboards and reports.

Relationships between entities have types, and each are s bidirectional. If an application is deployed on a computer, the computer hosts the application.



Entity relationships allow risks to propagate from entity to entity. For example, Mark Smeeth (User) has access to a critical business application. He leaves his user name and password on a sticky note on his computer monitor at his desk. Despite the security measures (authorization and authentication controls) in place on the server, Mark's negligence increases the risk that an unauthorized person will access the server and application data.

When a parent entity is deleted, the child entities are not automatically included in assessments in which their parents had participated.

By default, entity relationship propagation settings are disabled.

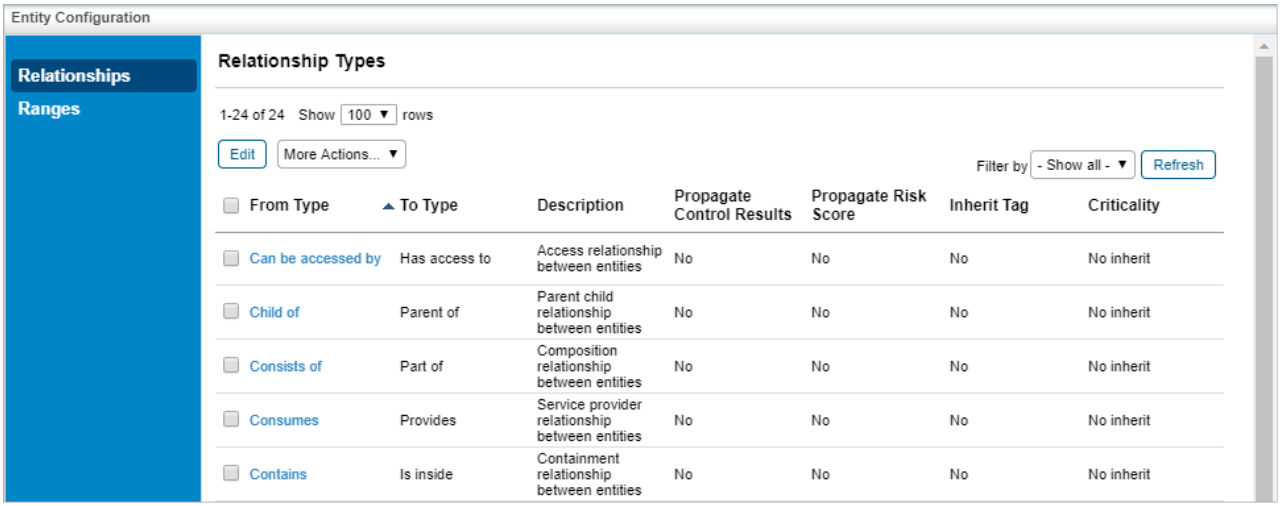
Understanding Relationship Types

RiskVision defines several entity relationship types. Each relationship type includes propagation and inheritance settings that allow the entities to share controls and show aggregate scores. Propagation and inheritance settings can be specified separately for each direction of a bi-directional relationship.

- **Propagate Control Results**: Automatically import questionnaires and check results into assessments of the **To** entity.
- **Propagate Risk Score**. Shows aggregated scores of all **From** entity assessments in assessments of the To entity.

  Use score with propagate controls.

Only set propagation for policies, results, and scores in one direction of a relationship pair. For example, enable propagation on either the **Parent of** or the **Child of** relationship to avoid looping.



The Relationships tab of the Entity Configuration screen.

To configure entity relationships:

1. Go to **Configuration** > **Entity Configuration**.
2. On the **Relationships** tab, select any of the relationship types.
3. Click **Edit**. The **Relationship Type** dialog displays.
4. Modify the settings, click **OK**, and click **Save**.

Programs and scores for entities with the relationship are updated immediately.

Predefined Relationship Type

The following types and their inverse are defined by RiskVision. That is, a relationship pair such as Child of/Parent of is specified in either direction. A source entity can have either the Child of or the Parent of relationship with a target entity. In the following table, the Relationship Type can be swapped with the Inverse Type.

Relationship type	Inverse type	Description
Can be accessed by	Has access to	Access relationship between entities
Child of	Parent of	Parent-child relationship between entities
Consists of	Part of	Composition relationship between entities
Contains	Is inside	Containment relationship between entities
Depends on	Needed by	Dependency relationship between entities
Deployed on	Hosting	Deployment relationship between entities
Entity Collection	Member of Entity Collection	Membership relationship between entities and entity collections
For	Has	Requirement relationship between entities
Group	Member of Group	Membership relationship between entities
Member of Program	Program	Membership relationship between entities and programs
Owned by	Owner of	Owner-ownee relationship between entities
Consumes	Provides	Service provider relationship between entities

Defining Entity Relationships

Relationships can be defined between entities and entity collections.

Because entity relationships are always bi-directional, defining a relationship from one entity to another automatically defines the inverse relationship. When you define a relationship from one entity to another, two relationships are created. You can define a relationship between one source entity and more than one target entity, in which case several relationships are created. If you relate one source to three targets, six relationships are created.

For example, if you set the relationship of a user to 'Access to' an application, the system automatically adds the 'Accessed by' relationship to the application. Removing either 'Access to' or 'Accessed by' removes both definitions.

Relationships immediately affect assessments in progress and are visible in reports and dashboards the next time they run.

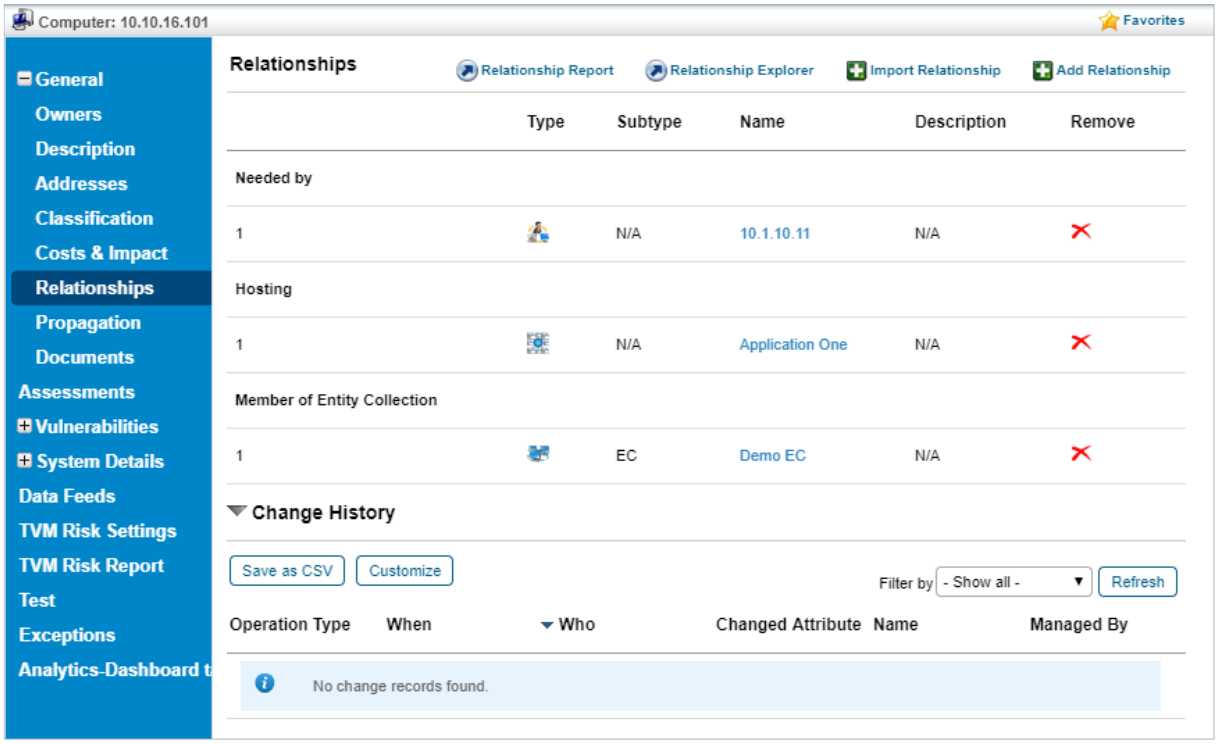
By default, control and score propagation settings are disabled. See Configuring Entity Relationship Attributes for more information.

EXAMPLE

You want to establish a parent-child relationship between entity A and entity B. As an entity owner, you know that an entity A must be the parent of entity B. In this case, you must add a 'Child of' relationship type on the Relationship tab of entity B and select entity A.

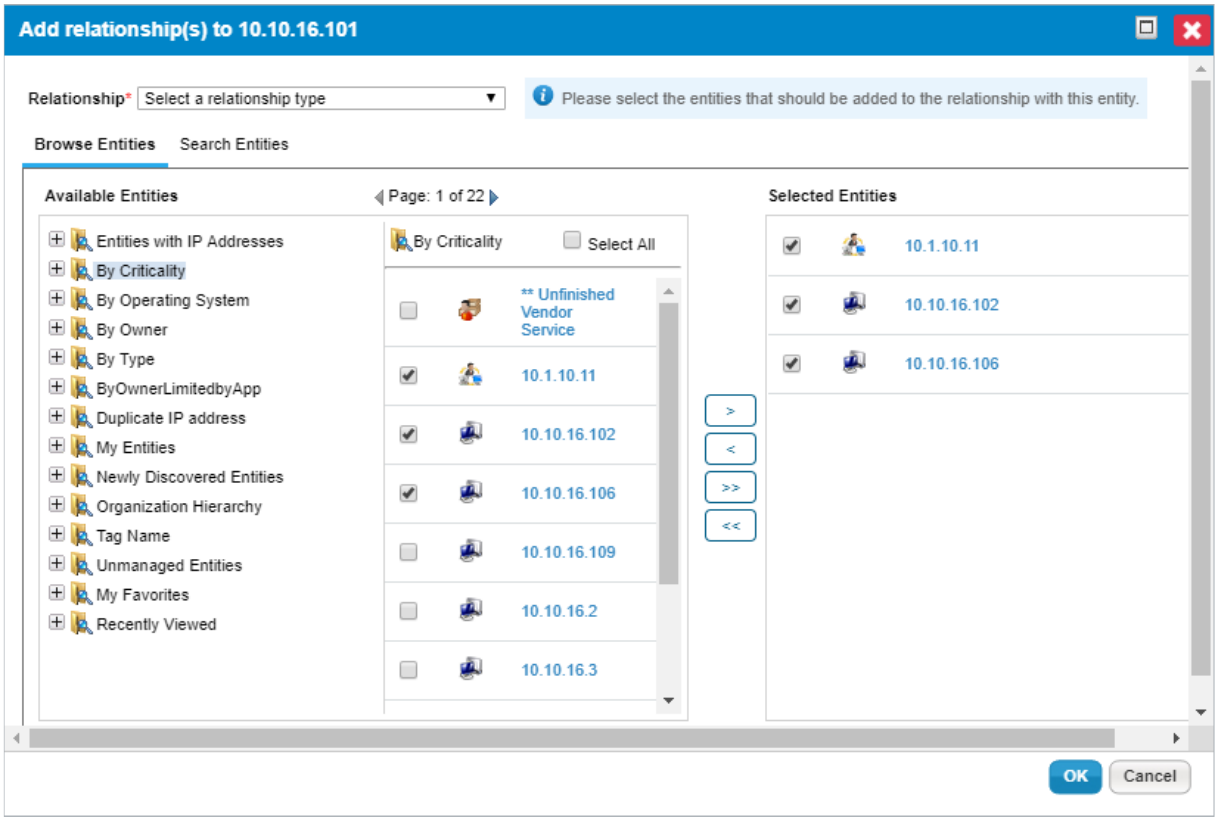
To establish a relationship between entities:

1. Go to **Entities** > **Entities**.
2. Click an entity to open.
3. Click the **Relationships** tab.



The Relationships table on the Relationships tab.

4. Click **Add relationship**.



The Add relationships dialog.

5. Click **Relationship** and choose a relationship type.
6. Select an entity group in the **Available Entities** box, or click **Search** to find a particular entity using the search criteria. To specify search criteria, select a field in the first dropdown box, then select a condition in the second dropdown box, and enter the search value in the box. Click **+** to add a new search condition. Click **Search** to retrieve the results for selecting entity(s). To select specific entities, check the box next to entity(s), or dynamic group, or **Select All**.
7. Click **OK**.

The specified relationship is added, as well as the inverse relationship from the target(s) to the original entity.

When a relationship is established with a dynamic group or its member(s):

- Selecting only specific entities within a dynamic group will create a relationship with only those entities.
- **Select All** will create a relationship with all the selected entities within a dynamic group, but not the dynamic group. Therefore, when members are added or removed from a dynamic group, the relationship of those entities with the entity collection are not affected.
- Selecting **dynamic group** will create a relationship with dynamic group itself. This selection creates a dynamic relation with members of the dynamic group. You must be careful with this selection because when members are added or removed from a dynamic group, their relationship with other entities is affected.
- Even though a member is shown on the **Entities** tab of entity collection, the **Relationship** tab will not show the EC Member or the Member of EC relationship type.

To remove a relationship:

1. Go to **Entities**> **Entities** and select an entity to open.
2. Click the **Relationships** tab.
3. Find a the relationship and click **X** in the **Remove** column.
4. Click **OK** .

The inverse relationship is automatically removed from the related entity.

Creating and Deleting Relationship Types

Beginning with version 7.0, RiskVision provides the ability to create and delete a relationship type when com.agiliance.asset.enableCreateRelationshipTypes=true property is added to the agiliance.properties file. You can only delete the relationship types you have created, if the relationship type is not in use.

To create a new relationship type

1. In the RiskVision application, go to **Configuration** > **Entity Configuration**. The **Relationships** tab details are displayed.
2. Click **New**. The **Create New Relationship** dialog appears.
3. In the dialog, enter the following fields.
    - **Relationship Name**. Name of the relation between entities
    - **Inverse of Relationship**. Name of the reverse relation
    - **Description**. Information that helps demonstrate the purpose of creating the relationship type
4. Click **OK**. The new relationship type is created.

User-defined relationship type allows the establishment of the relation only between the entities.

To delete a relationship:

1. In the RiskVision application, go to **Configuration** > **Entity Configuration**. The **Relationships** tab details are displayed.
2. In the **Relationships** tab, select the custom relationship type that is not in use, and click **Delete**. The relationship is deleted

Importing Relationships

You will need the **EntityRelationshipImportTemplate.xls** file to import relationships between entities and entity collection.

To import relationships:

1. In the RiskVision application, use one of the following navigation:
    - Go to **Entities** > **Entities** and select an entity to open its details page.
    - Go to **Entities** > **Entity Collections** and select an entity collection to open its details page.
2. Click the **Relationships** tab and click **Import Relationship**.
3. The **Import Entity Relationships** dialog appears. Click **Browse**, select the EntityRelationshipImportTemplate.xlsfile, click **Open**, and click **OK**.
4. The relationships are added.

Propagation Overview

IT infrastructures are usually complex, with many interconnected systems and components. Propagation allows you to reflect these inter-dependencies by disseminating control results and risks from one entity and/or entity collection down to multiple other entities or entity collections. Generally, with propagation, you are spreading the results from one to many entities or entity collections, as opposed to doing it from many entities or entity collections to a single entity or entity collection. In order for propagation to occur, there must be a relationship between entities or between the entity and entity collection. Also, propagation must be enabled for the relationship. This allows the entities or entity collection to inherit the results from the related entities or entity collections within a program

RiskVision utilizes a publish - auto-subscribe - revocation model for propagation. Before any control results can be propagated, they first have to be published by a related entity or an entity within the same program for a relationship for which propagation has been enabled. All related entities or entity collections will automatically inherit the results but can then revoke those results if they decide to meet the control(s) on their own.

RiskVision application has the following types of propagation:

- Inter system
- Intra system

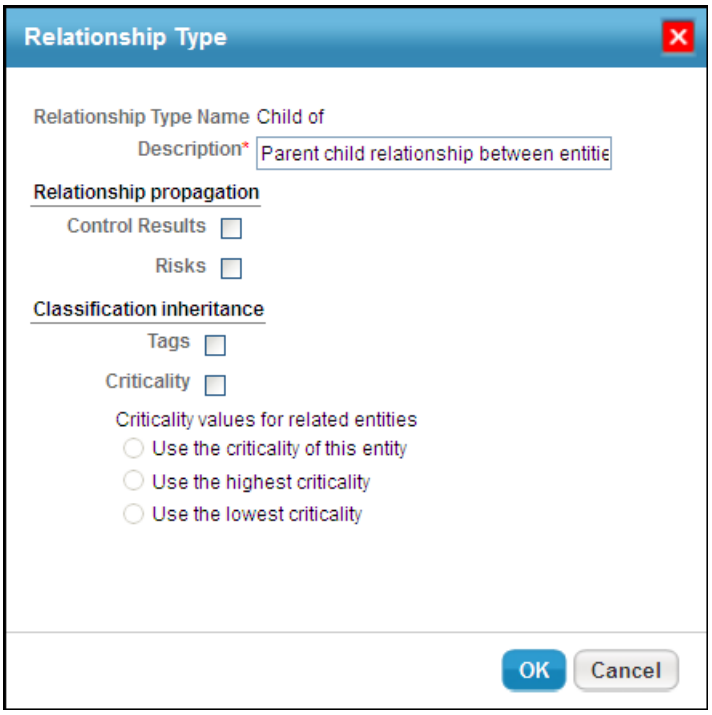
Inter system: This type of propagation happens between entities and other entities, between entity collections and other entity collections, or between entities and entity collections. An example of this type of propagation would be propagating results for authentication and authorization-related controls from Active Directory to the SAP financial system.

Intra system: This type of propagation happens between entity collection and its members and is meant to capture controls that apply only to the specific system in question and not other systems or components. For example, Active Directory may provide authentication and authorization-related services to other systems, but for internal Active Directory components, may need to propagate results for other controls, such as whether there is a system security plan in place or whether risk management processes are being followed for the system.

About Propagation Settings

Entity classification and tags can be inherited from other entities using entity relationships. Any relationship between two entities can be configured to propagate Control Assignments, Control Results, Risk, Tags, or Criticality. The system is designed to make circular references impossible. Entities cannot inherit what they propagate.

To specify the propagation associated with an entity relationship, navigate to **Configuration** > **Entity Configuration** > **Relationships**. Click on a relationship to display the Relationship Type dialog.



Control results and risks are propagated, but only within a particular program. Propagating control results or risks across programs can be performed manually. If a Control Profile is specified, the system uses the control profile and ignores the control assignment.

When propagating criticality, choose the value to use:

- The "from" entity's criticality

- The highest criticality between the "from" and the "to" entity
- The lowest criticality between the "from" and the "to" entity

If your program owner configures each entity with different criticality values and then establishes parent-child relationship type between entities in such a way that the parent entity propagates either criticality or tags, and control results to child entities. It is recommended to first run the Update Objects job before you include entity pairs in an assessment. By doing so, you can ensure that all the child entities inherit the criticality value of the parent entity and that when you run the assessment, the control results will propagate effectively.

Adding entities and then creating a new relationship with an existing entity relationship type requires running the Update Objects job to propagate the scores effectively to the newly added entities.

A child entity inherits the security risk score if you configure the parent entity to propagate the risk score.

Visualizing Relationships

Relationship visualization allows you to view associations between entities and entity collections for multiple levels of relationships. The Relationships Report provides the relationships of entity collections with entities, entity collections with other entity collections, and entities with other entities in graphical form.

To visualize entity relationships:

1. On the **Entities** menu, Click **Entities**. The **Entities** grid is displayed.
2. From within the Entities tree, expand the group containing the entity you want to visualize its relationships, and select the entity to open its details page.
3. On the entity details page, click the **Relationships** tab. The **Relationships** tab details are displayed.
4. Click **Relationship Report**. The web browser opens the **Relationship Report** in a new window.

To visualize entity collection relationships:

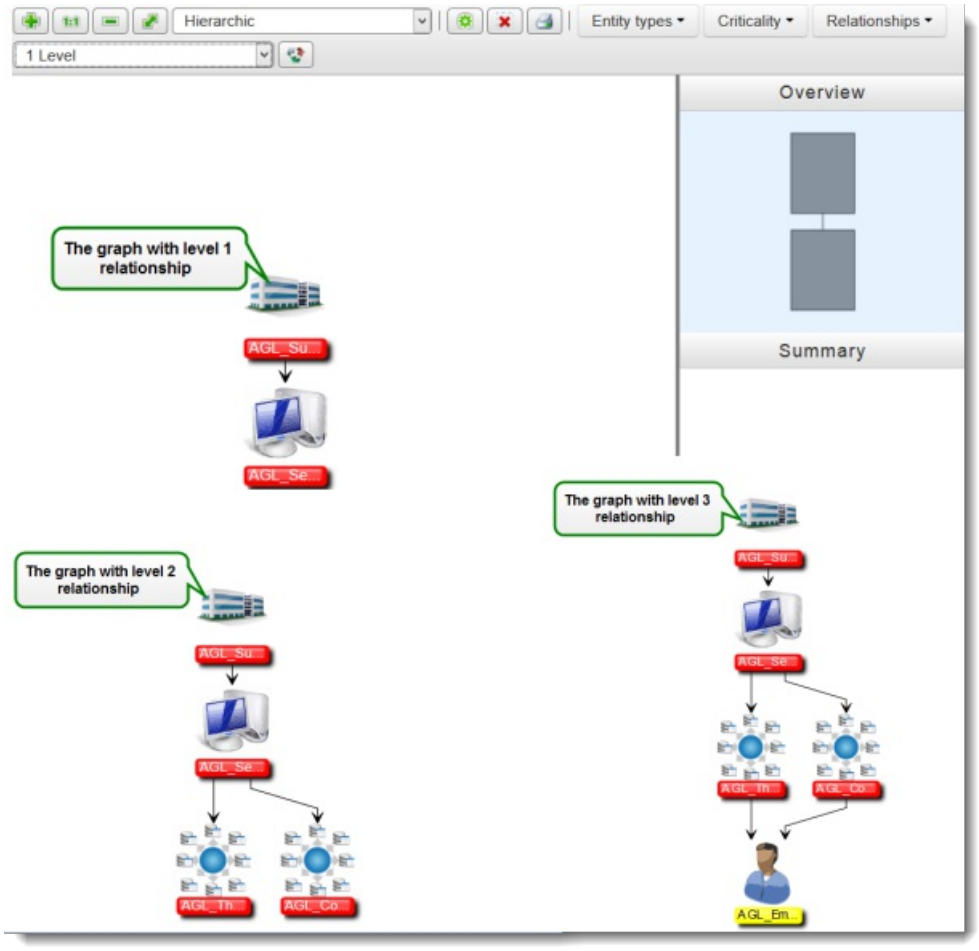
1. On the **Entities** menu, Click **Entity Collections**. The **Entity Collections** grid is displayed.
2. From within the Entity Collections tree, expand the group containing the entity collection you want to visualize its relationships, and select the entity to open its details page.
3. On the entity collection details page, click the **Relationships** tab. The **Relationships** tab details are displayed.
4. Click **Relationship Report**. The web browser opens the **Relationship Report** in a new window.

Relationship Report

The Relationship Report is displayed in a window in which different visualization tools are available to study relationships at varying depths from level 1 through level 6. In the Relationship Report, you can use filters, such as Entity Types, Criticality, and Relationships to exclude the leftover items not selected in the filter types. The default graphical view includes all of the entity types, criticalities, relationship types, and level 1 relationships the entity or entity collection has established with other entities and/or entity collections. The Level 1 relationship is one that is directly related to the source entity or entity collection. The graph also displays the criticality colors for the related entity and entity collections.

For each relationship type, the entities will be grouped based on the entity type when the count exceeds the value set in the com.agiliance.web.visulization.maxentitycountofsametype property.

The image below shows graphical layouts of level 1, level 2, and level 3 relationships.

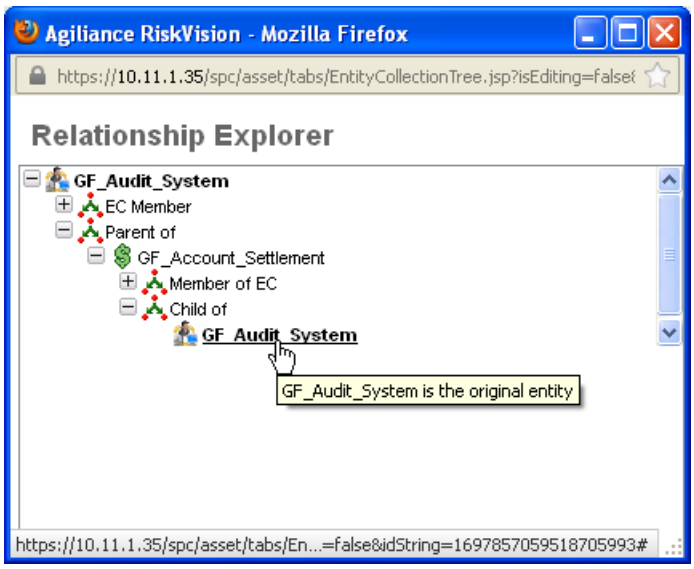


In the graphical layout shown above, the arrows indicate the relationships, the label colors associated with entities or entity collections indicate the criticality ratings, and double-clicking an entity or entity collection displays the details page.

Relationship Explorer

The **Relationships** tab for an entity or entity collection shows only the direct relationships of an entity or entity collection and not the indirect relationships. That is, the relationships of one or more entities or entity collections that are related to other entity or entity collection. The **Relationship Explorer** window allows you to drill down into a context of interdependence with other entities and entity collections and can be used to show all of the dependencies that a particular entity collection or entities, and not just those that are one level removed from that entity collection.

To open the **Relationship Explorer** window, select an entity or entity collection to open its details page, click the **Relationships** tab, and then click **Relationship Explorer** at the top right corner of the view.



At the top of the **Relationship Explorer** window, you will notice the entity (or entity collection) as a root. When you expand the root, any established relationships will appear. Expand each relationship type to see with what entities that the root entity is associated. You can also expand other entities to see if those entities have a relationship with any other entities, and so forth. This will provide an overview of the dependencies of the root entity or entity collection with the other entities or entity collections.

Assigning Vulnerabilities

To assign vulnerabilities to RiskVision objects, such as entities, tickets, controls and subcontrols, select the vulnerabilities by entering the search criteria. The **Select Vulnerabilities** interface has search elements with a text box or a check box that you can choose to narrow search results.

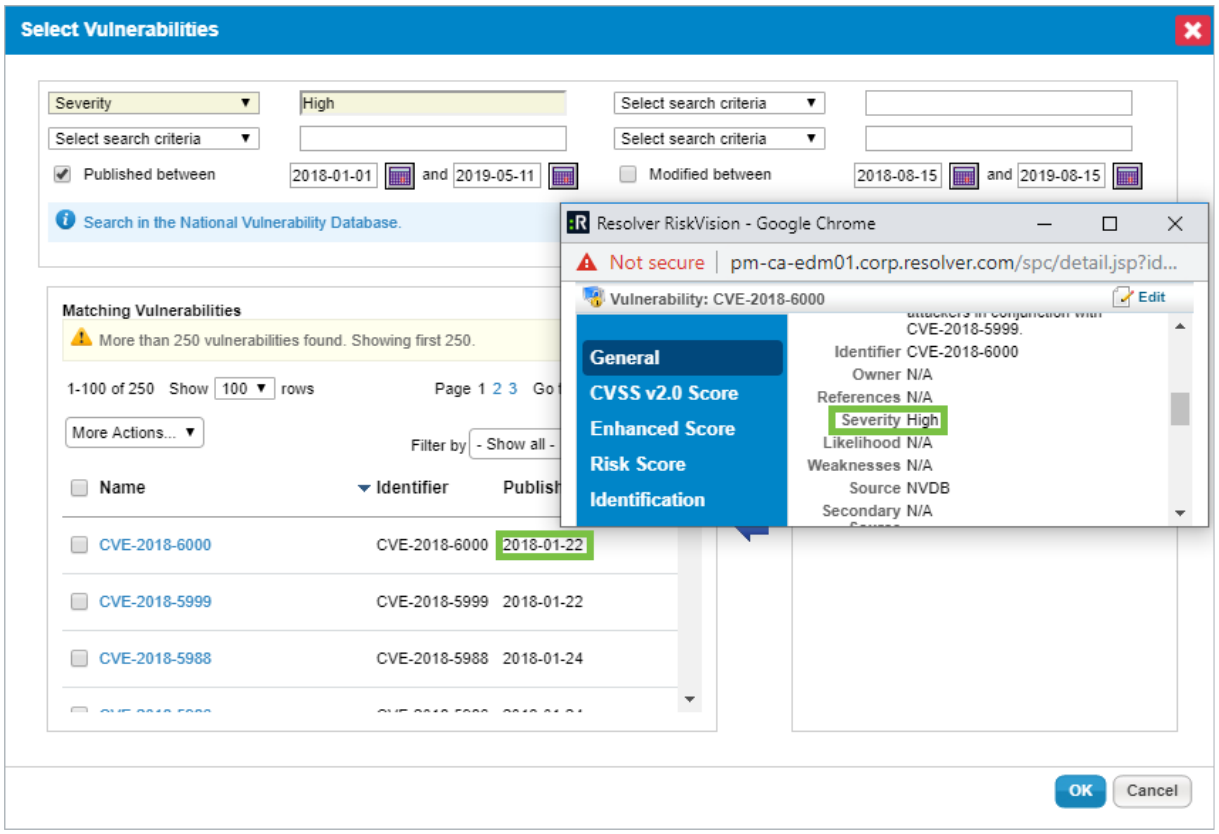
Search Element	Description
Title	Input the title text to search for vulnerabilities.
Identifier	Input the alphanumeric character to search for vulnerabilities.
Description	Input the vulnerability description to search for vulnerabilities.
Severity	Search for vulnerabilities based on their severity, such as low, medium, or high. Specify the complete string to search vulnerabilities based on the severity. For example, "med" will not return any results.
Source	Search for vulnerabilities based on their source, such as NVDB or Nessus.
Secondary Source	Search for vulnerabilities based on a secondary source, such as a scanner.
Technology	Search for vulnerabilities that are associated with a technology, such as Microsoft, Symantec, or Oracle.
Patch Name	Search for resolved vulnerability instances for which a patch has been applied.
CWE	Input the CWE value to search for vulnerabilities.
Other Identifiers	Search for vulnerabilities identified from a vulnerability database other than NVDB, such as MLIST or Security Focus.
CVSS Score less than	Search for vulnerabilities with a CVSS score less than a specified value.
CVSS Score greater than	Search for vulnerabilities with a CVSS score greater than a specified value. Use CVSS Score less than and greater than to find vulnerabilities between a score range.
Published between	Search for NVDB vulnerabilities and user-created vulnerabilities published between a specified period of time.
Modified between	Search for vulnerabilities modified between a specified period of time.

To assign a vulnerability:

1. Follow with the navigation in the following table for the desired object type:

Object	Navigation
Entity	Go to **Entities** > **Entities**, then select an entity to open. Click the **Vulnerabilities List** tab > **Assign**.
Control and Subcontrol	Go to **Content** > **Controls** and Questionnaires, then click a control or subcontrol to open. Click the **References** tab > **More Actions** > **Map to Vulnerability**.
Ticket	Go to **Home** > **Tickets**, then click a ticket to open. Click **Linked To** > **Vulnerabilities** tab > **Assign**.
Technology	Open RiskVision Threat and Vulnerability Manager. Go to **Vulnerabilities** > **All Technologies**, then click a technology to open. Click **Vulnerabilities** > **Link to Existing Vulnerabilities**.
Chart	Go to **Analytics** > **Charts**. Click a chart. Go to the **Filters** tab, then click +.

2. Search for vulnerabilities. Click **Select Search Criteria** and select search elements, or click the **Published between** or **Modified between** checkbox to select a date range. Click **Search**.



Searching for elements in the Select Vulnerabilities dialog.

Search results are returned using:

- The "*AND*" operator - If the search criteria is applied to the different search elements.
- The "*Contains*" operator - If the input text is entered for a single search element.
- The "*Or*" operator - If the search criteria is a comma separated value for the Identifier search element.

- Select the check box next to the vulnerability, then use the right arrow to move the vulnerability into vulnerabilities to assign pane, and then click **OK**. To remove the selection, use the left arrow.

Operating Systems

Operating systems are available on the Computer, Network Device, and Mobile Device entity types. You can add a new operating system or use an existing one.

To add an operating system:

1. In the **Entity Details** page, click the **System Details** tab.
2. Click **New**. The **Operating System** dialog appears.
3. In the Operating System dialog, enter the following fields:
    - **Full Name**. Enter the application name. This must be a relevant name.
    - **Description.** Enter any information that describes the operating system.
    - **Product**. Enter the product name. This is a short name for the operating system.
    - **Version**. Enter the version number of the operating system. This helps you notice the differences between the new version and old version.
    - **Vendor**. Enter the organization's name that is providing the operating system.
    - **Update**. Enter the software revision number, if available. You can derive this field if your operating system includes the most recent fix.
    - **Edition**. Enter the edition, such as standard, professional, or enterprise, if applicable.
    - **Language**. Enter the language if the operating system is procured for non-native English users.
    - **Version name**. Enter the version name, if available.
    - **Serial number**. Enter the unique number that identifies the operating system.
4. Click **OK**. The operating system is added.

To assign a predefined operating system:

1. In the entity details page, click the **System Details** tab.
2. Click **Add**. The **Choose Operating Systems** dialog appears.
3. In the dialog, use the following fields to search the application:
    - Title. Enter the operating system's title.
    - Version. Enter the operating system's version number.
    - Vendor. Enter the vendor's name.
        - The fields above can be used in combination to narrow the search results.
4. Click **Search** after entering the search field(s).
5. The results are returned and displayed in the **Known Operating Systems** box. If the search returns too many operating systems, use the scroll-bar to find the operating system.
6. After you locate the operating system, select the operating system in the **Known Operating Systems** box, and click the arrow pointing towards downward to move the operating system into the **Selected Operating Systems** box.
7. Click **OK**. The predefined operating system is added.

To edit an operating system:

1. In the entity details page, click the **System Details** tab.
2. Select the box in the corresponding operating system row. You can edit only the user-defined and scanner-imported operating systems.
3. Select **Edit** in the More Actions drop-down list. The **Operating System** dialog appears, where changes to the operating system can be made.
4. After the completion of changes, click **OK**.

To delete an operating system

1. In the entity details page, click the **System Details** tab.
2. Select the box in the corresponding operating system row and click **Delete**. The selected operating system is removed from the entity.

Applications

Applications installed can be found on the Computer, Network Device, and Mobile Device entity types. Typically, this data is brought in from scanners, but there may be times when you may want to manually update the data.

To add an application:

1. In the entity details page, click + to expand the **System Details** tab, and click **Applications**.
2. Click **New**. The **Application** dialog appears.
3. In the **Application** dialog, enter the following fields:
    - Full Name. Enter the application name. This must be a relevant name.
    - Description. Enter any information that describes the application.
    - Product. Enter the product name. This is a short name for the application.
    - Version. Enter the version number of the application or product. This helps you notice the differences
    - between the new version and old version.
    - Vendor. Enter the organization's name that offers the application.
    - Update. Enter the software revision number, if available. You can derive this field if your application
    - includes the most recent fix.
    - Edition. Enter the edition, such as standard, professional, or enterprise, if applicable.
    - Language. Enter the language if the application is procured for non-native English users
    - System Component: Select 'Yes' if the application is a system component.
4. Click **OK**. The application is added.

To assign a predefined application:

1. In the entity details page, click + to expand the System Details tab, and click Applications.
2. Click Add. The Choose Applications dialog appears.
3. In the dialog, use the following fields to search the application:

- Title. Enter the application's title.
- Version. Enter the application's version number.
- Vendor. Enter the vendor's name.

The fields above can be used in combination to narrow the search results.

4. Click **Search** after entering the search field(s).

5. The results are returned and displayed in the **Known Applications** box. If the search returns too many applications, use the scroll-bar to find the application.

6. After you locate the application, select the application in the **Known Applications** box, and click the arrow pointing downward to move the application into the **Selected Applications** box.

7. Click **OK**. The predefined application is added.

To edit an application

1. In the entity details page, click + to expand the **System Details** tab, and click **Applications**.
2. Select the box in the corresponding application row. You can edit only the user-defined and scanner-imported applications, since the applications that come from the NVD are not meant to be changed.
3. Select **Edit** in the More Actions drop-down list. The **Application** dialog appears, where changes to the application can be made.
4. After the completion of changes, click **OK**.

To delete an application:

1. In the entity details page, click + to expand the **System Details** tab, and click **Applications**.

2. Select the box in the corresponding application row and click **Delete**. The selected application is removed from the entity.

Ports

Ports are available on the Computer, Network Device, and Mobile Device entity types. Typically, ports are automatically imported into RiskVision by a vulnerability scanner, such as the Tenable Nessus Connector or the Qualys QualysGuard Connector. However, there may be times when you may want to manually modify port data.

To add a port

1. In the entity details page, click + to expand the **System Details** tab, and click **Ports**.
2. Click **New**. The **Port** dialog appears.
3. In the **Port** dialog, enter the following fields:
   - **Name**. Enter the port name.
   - **Protocol**. Enter the type of protocol, such as UDP and TCP.
   - **Protocol Number**. Enter the port number.
   - **Description.** Enter the information that helps understand the purpose of adding the port.
4. Click **OK**. The port is added.

To assign a predefined port:

1. In the entity details page, click **+** to expand the **System Details** tab, and click **Ports**.
2. Click **Add**. The **Choose Ports** dialog appears.
3. In the dialog, use the following fields to search the port:
   - Port Name. Enter the port's name.
   - Port Number. Enter the port's number.
   - Protocol. Enter the protocol, such as TCP or UDP.
4. The fields above can be used in combination to narrow the search results.
5. Click **Search** after entering the search field(s).
6. The results are returned and displayed in the **Known Ports** box. If the search returns too many ports, use the scroll-bar to find the port.
7. After you locate the port, select the port in the **Known Ports** box, and click the arrow pointing downwards to move the port into the **Selected Ports** box.
8. Click **OK**. The predefined port is added.

To edit a port:

1. In the entity details page, click **+** to expand the **System Details** tab, and click **Ports**.
2. Select the box in the corresponding port row. You can edit only the user-defined and scanner-imported ports
3. Select **Edit** in the More Actions drop-down list. The **Port** dialog appears, where changes to the port can be made.
4. Click **OK** after the completion of changes.

To delete a port:

1. In the entity details page, click **+** to expand the **System Details** tab, and click **Ports**.
2. Select the box in the corresponding port row and click **Delete**. The selected port is removed from the entity.

Manually modified port information will be overwritten by scanner data if the scanner data pertains to the same entity.

Performing Entity Actions

Entities can be managed in the **Entities** and **Entity Collection** grids. Entity actions are visible only if you have the Entity View and Entity Manage permissions. The actions provide a convenient way to update all of entities in a dynamic group where multiple entity attributes can be updated simultaneously, newly discovered entities can be allowed to participate in assessments, and entities can be excluded from participating in assessments.

The following table lists different actions and their purpose:

Action	Description
Manage Entities	Entities imported into RiskVision application must be managed before you include them in assessments.
Unmanage Entities	Refrains entities from participating in assessments.
Add Operating System to Entities	Adds operating system information to entities. Use the **Choose Operating System** dialog to search and select the operating system. For information about how to add the operating system to entities, see Operating Systems.
Remove Operating System from Entities	Removes operating system information from entities.
Add Application to Entities	Adds application(s) to entities. Use the **Choose Applications** dialog to search and select the applications. For information about how to add the application to entities, see Applications.
Remove Application from Entities	Removes application(s) from entities.
Copy Entity	Creates a copy of an entity into the selected assessment. While copying choose whether to copy an entity's attributes. Or use this action to copy an entity's data to other entities.
Batch Edit Entities	Select multiple entities to update common attributes simultaneously.
Save as CSV	Export entities out of the RiskVision application in Excel format.
Show Relationship Graph	Display a graph showing the relationship between the selected entities.
Run Contextual Report	View a contextual report of the selected entities.

The **Export Entities** option is configurable. If you have a lot of entities, you can choose to turn off the **Export Entities** option. This can be done by modifying the property `ui.asset.grid.export.enable`

If `ui.asset.grid.export.enable` = True, then **Export Entities** appears in the **More Actions** drop-down.

If grid.csvexport.all = True, then the users will be able to export entities to CSV files.

Contextual Reports of Entities

You can generate reports on more than a single entity or entity collection. For example, you can see all of the vulnerabilities that exist on a dynamic group containing your Windows and Linux servers. Or, you can generate a consolidated report showing the compliance status of all servers that a specific employee is responsible for.

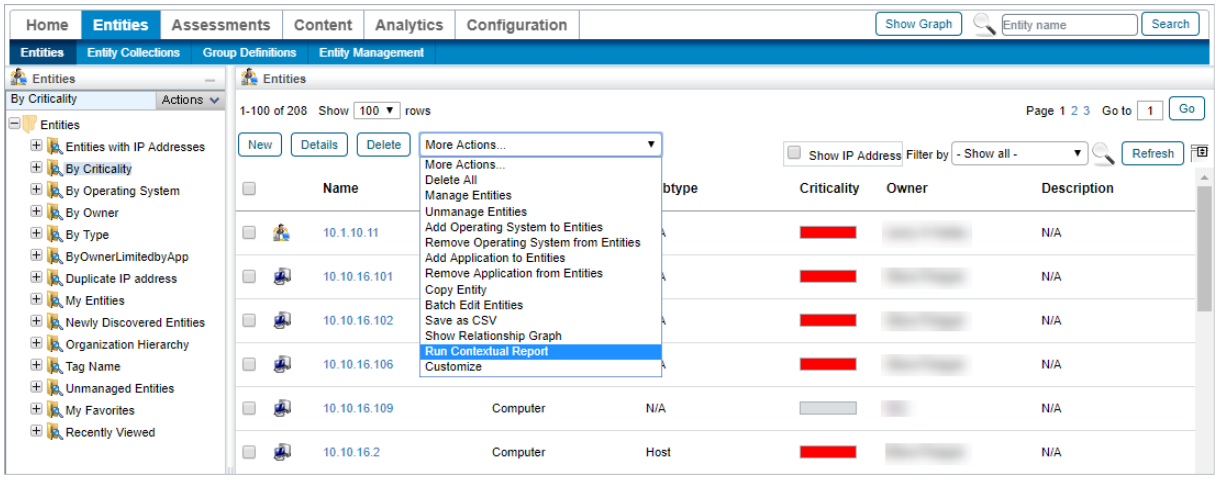
With contextual reports you can:

- View reports on dynamic groups. For example, it would be easy to create a contextual report on a given owner's entities and entity collections, a given type of entity, or any other attribute that can be represented by a dynamic group.
- Use the **Advanced Search** to precisely define the list of entities or entity collections you want to see and then create a contextual report on these entities or entity collections. For example, you can search by IP address, discovery source, and entity risk, and then run a contextual report.

The contextual reporting feature works with both reports that come with RiskVision and reports you define yourself.

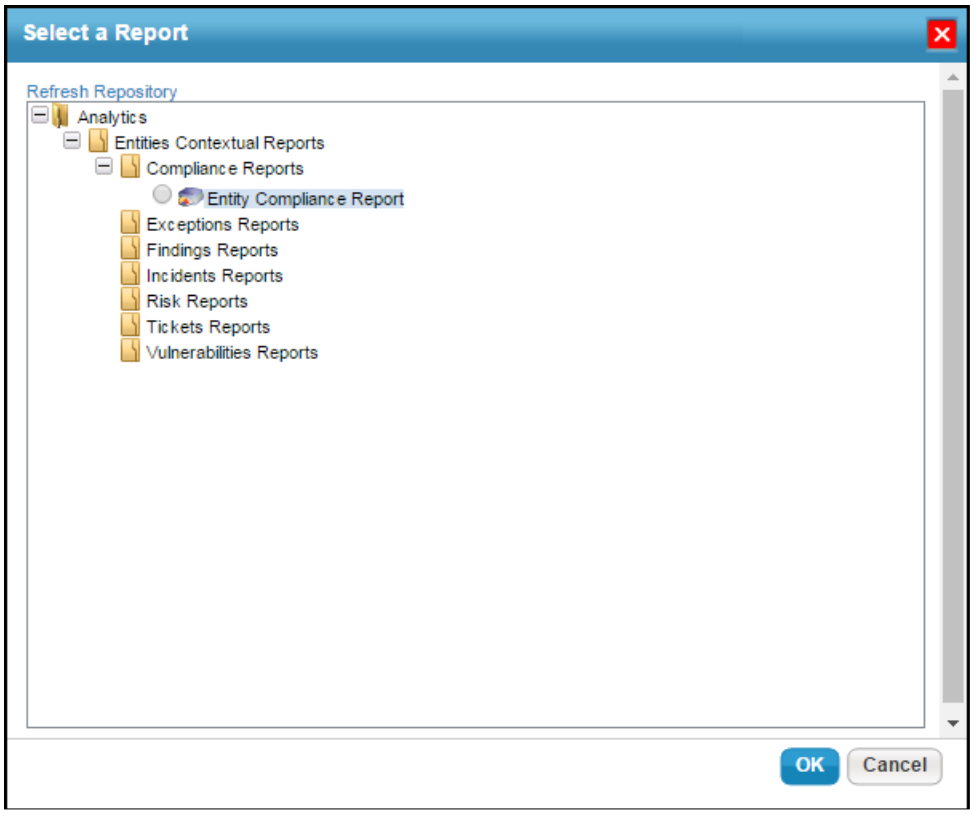
To view a contextual report:

1. Open the Entities page.
2. Select the required entities, then click **More Actions** > **Run Contextual Report**.



Running a contextual report.

3. Browse and select the required report. These reports can also be created in JasperReports and run directly from the **Entities** page.



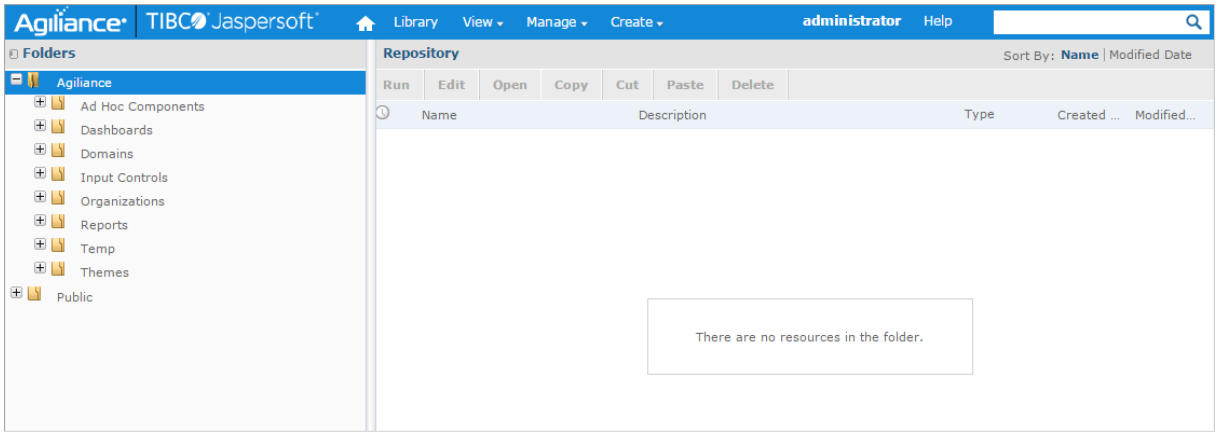
Selecting a report in the Select a Report dialog.

A contextual report related to the selected entities is generated based on the parameters configured for the selected report in JasperReports Server. The entities you have selected are passed to the report as parameters.

Create a Contextual Report in JasperReports Server

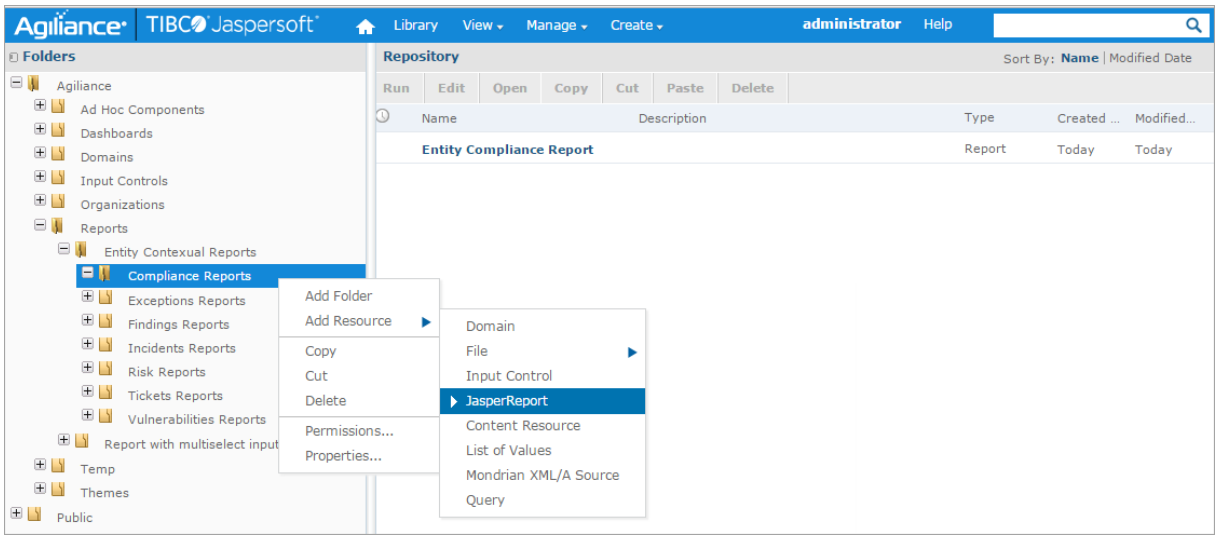
To create a contextual report to report against entities:

1. Click **Analytics** > **R7 charts** to open the **JasperReports Server** page.
2. Click **View** > **Repository**.

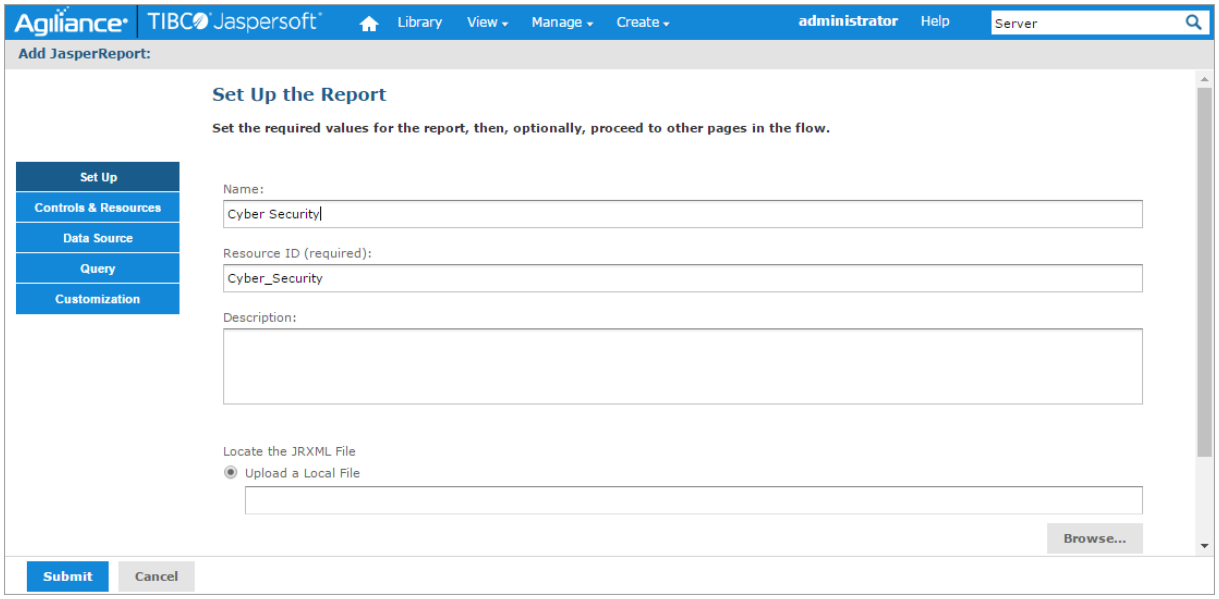


The Repository page.

3. Click **RiskVision** > **Reports** > **Entity Contextual Reports**.
4. Right-click on the type of contextual report that you want to create, then click **Add Resource** > **JasperReport**.



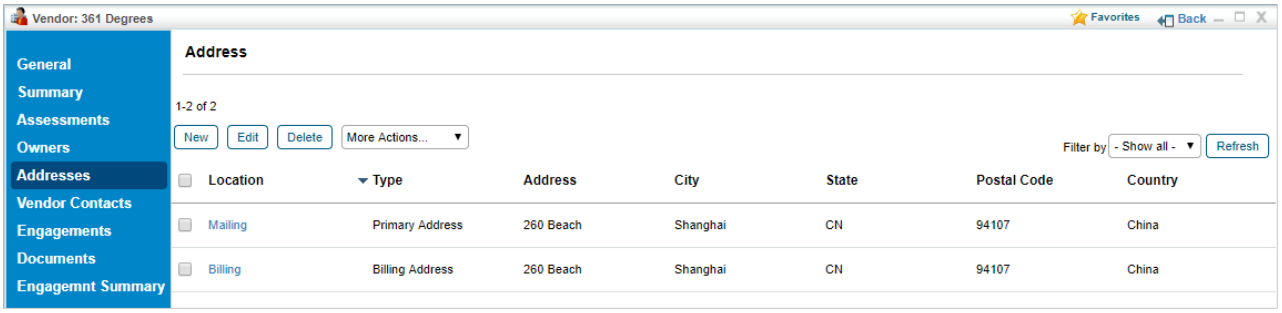
5. Follow the onscreen instructions to create a new report.



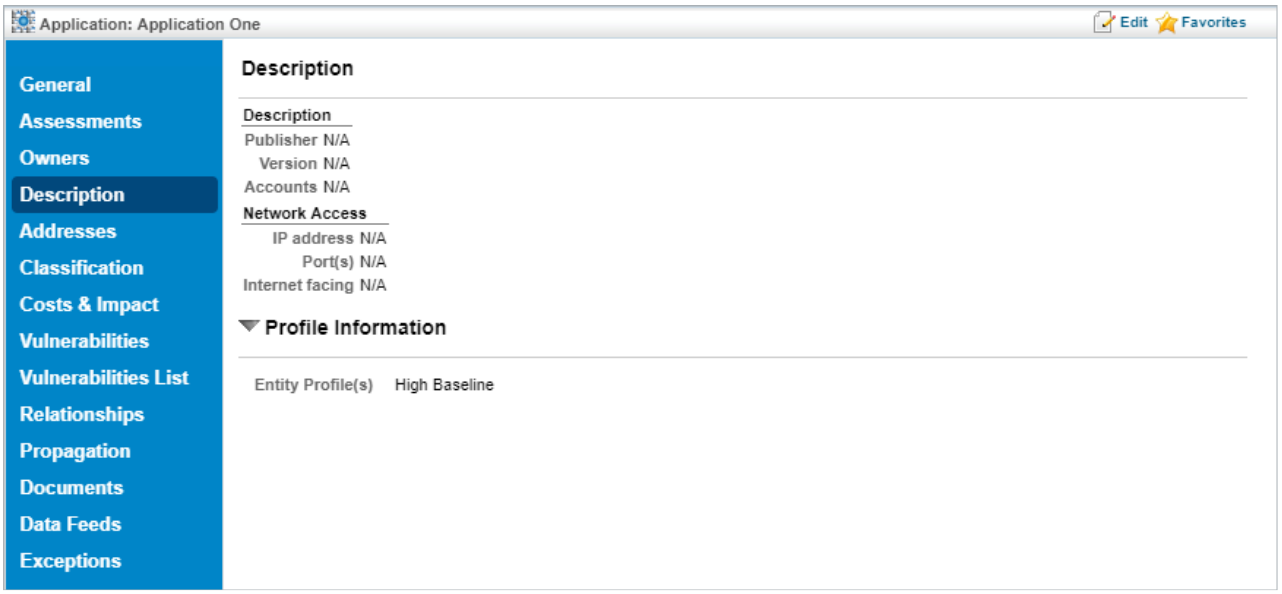
After you have created a report, you can generate this contextual report from the **Select a Report** pop-up.

Entity Attribute Screens

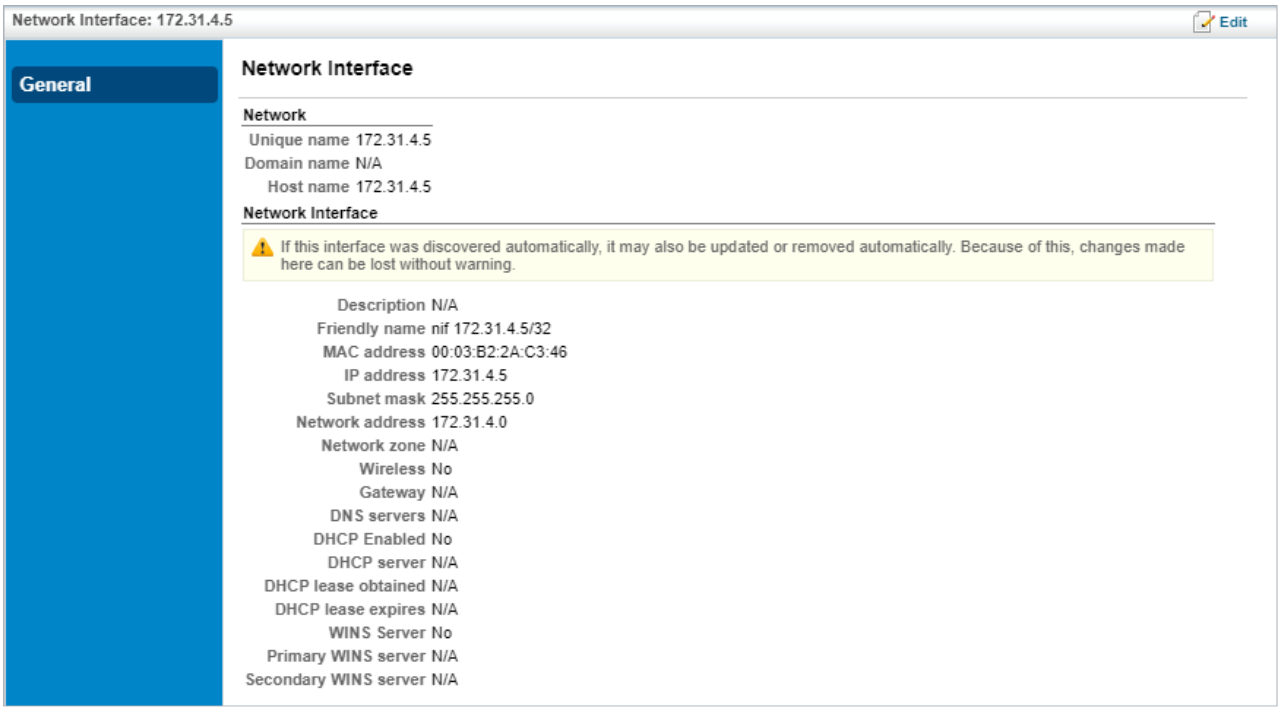
This section provides the list of **Entity** attribute screens in RiskVision.



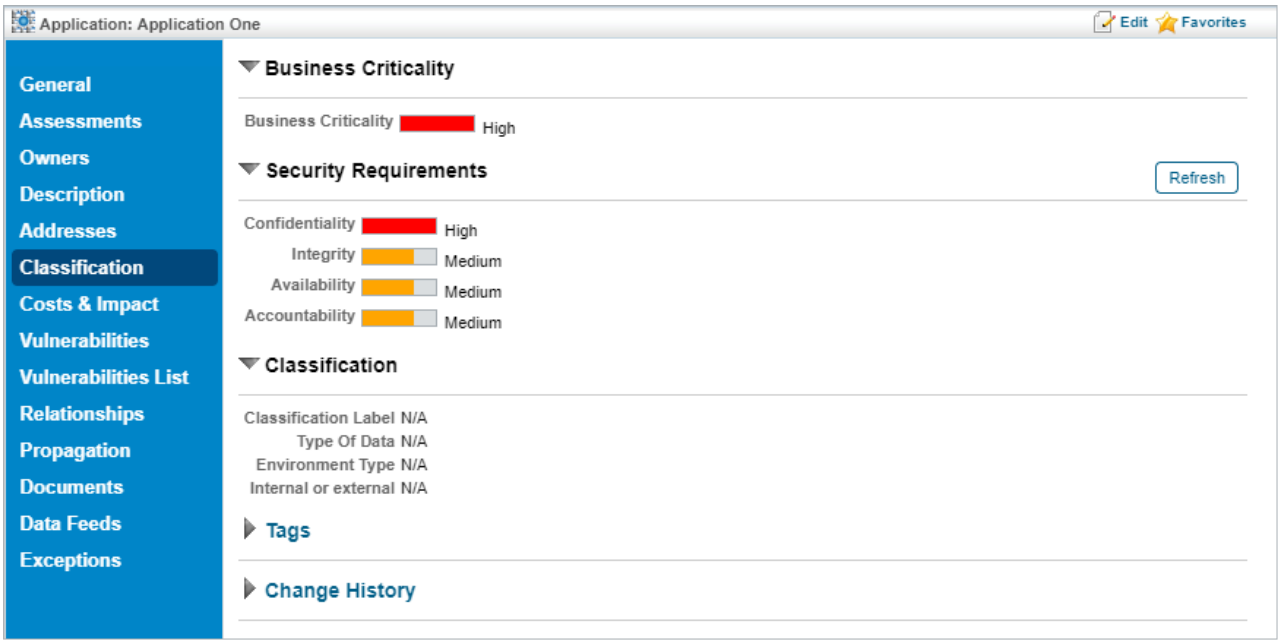
The Addresses tab of a vendor.



The Description tab of an application type entity.



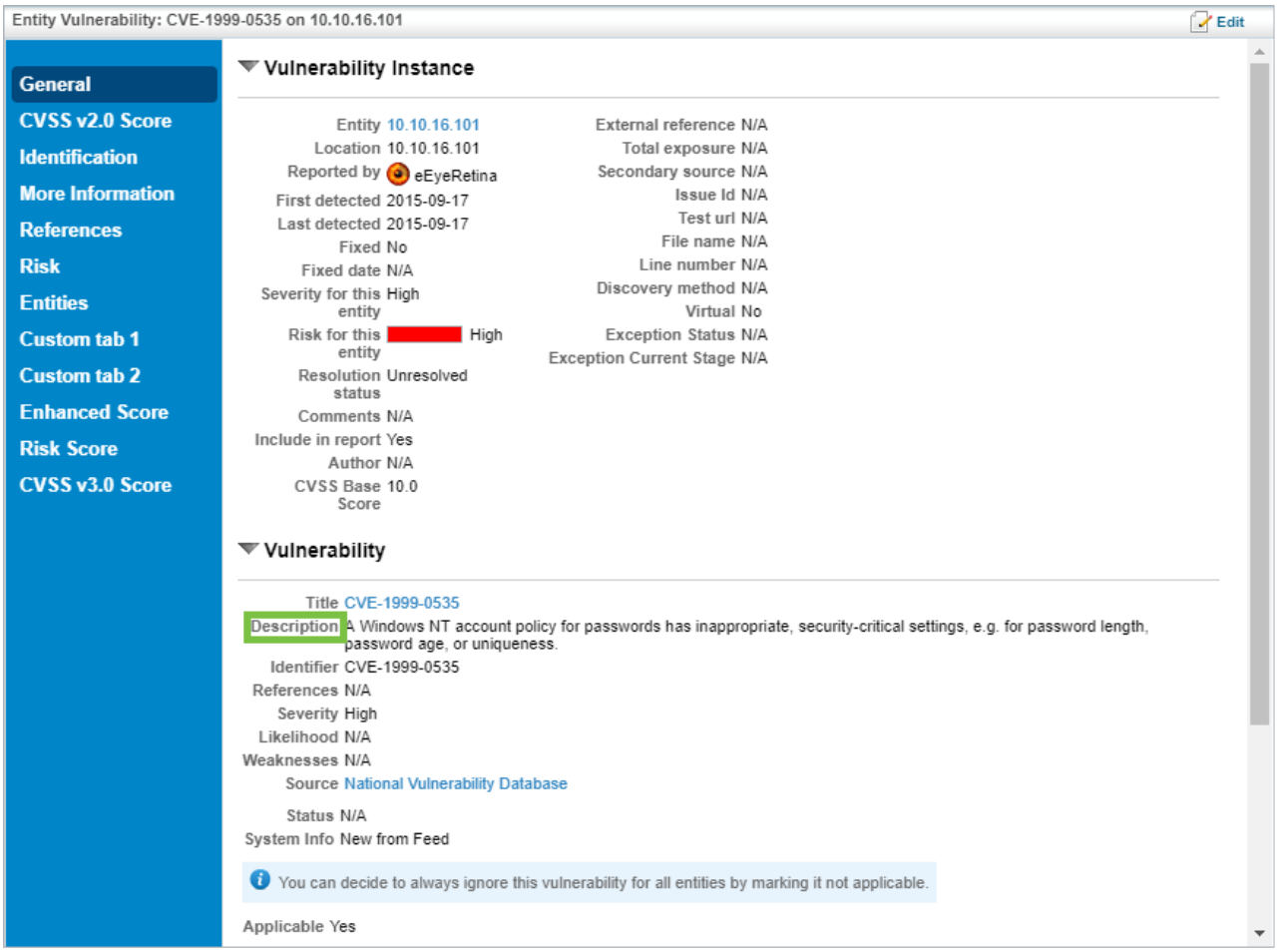
The General tab of a network interface.



The Classification tab of an application type entity.

Clicking the **Refresh** button will:

- Update the criticality based on the classification survey; and
- Update any changes made to the classification through the entity user interface.



The Description of an Entity Vulnerability.

About Entity Collections

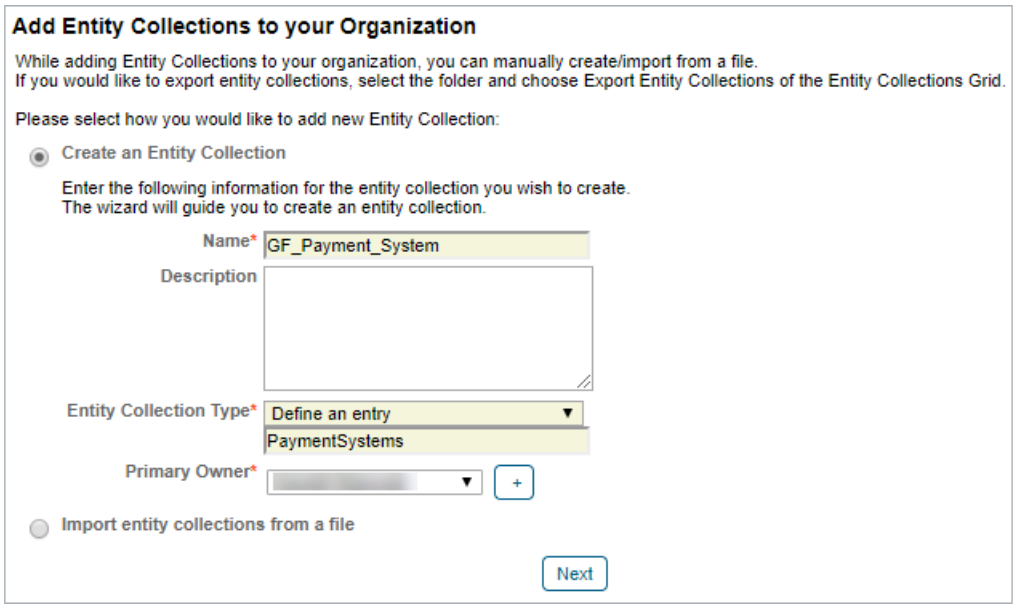
An entity collection system is a type of entity (or asset) that behaves as an entity, but refers to a set of entities, such as a system, process, or department. If you prefer to use a name other than entity collection, for example, "System," you can rename the term in the UIDictionary.xml file.

Dynamic groups and organization hierarchy containers with entity collections as members will appear in the navigation pane. An entity collection will appear in the **By Criticality**, **By Type**, or **Organization Hierarchy** pre-configured groups in the **Entity Collections** grid, by default. To add more pre-configured groups to the **Entity Collections** grid, go to **Entities** > **Group Definitions**, click **Add Pre-Configured Groups**, check the box next to the dynamic groups, and then click **Add Groups**.

The Entity Collections tab.

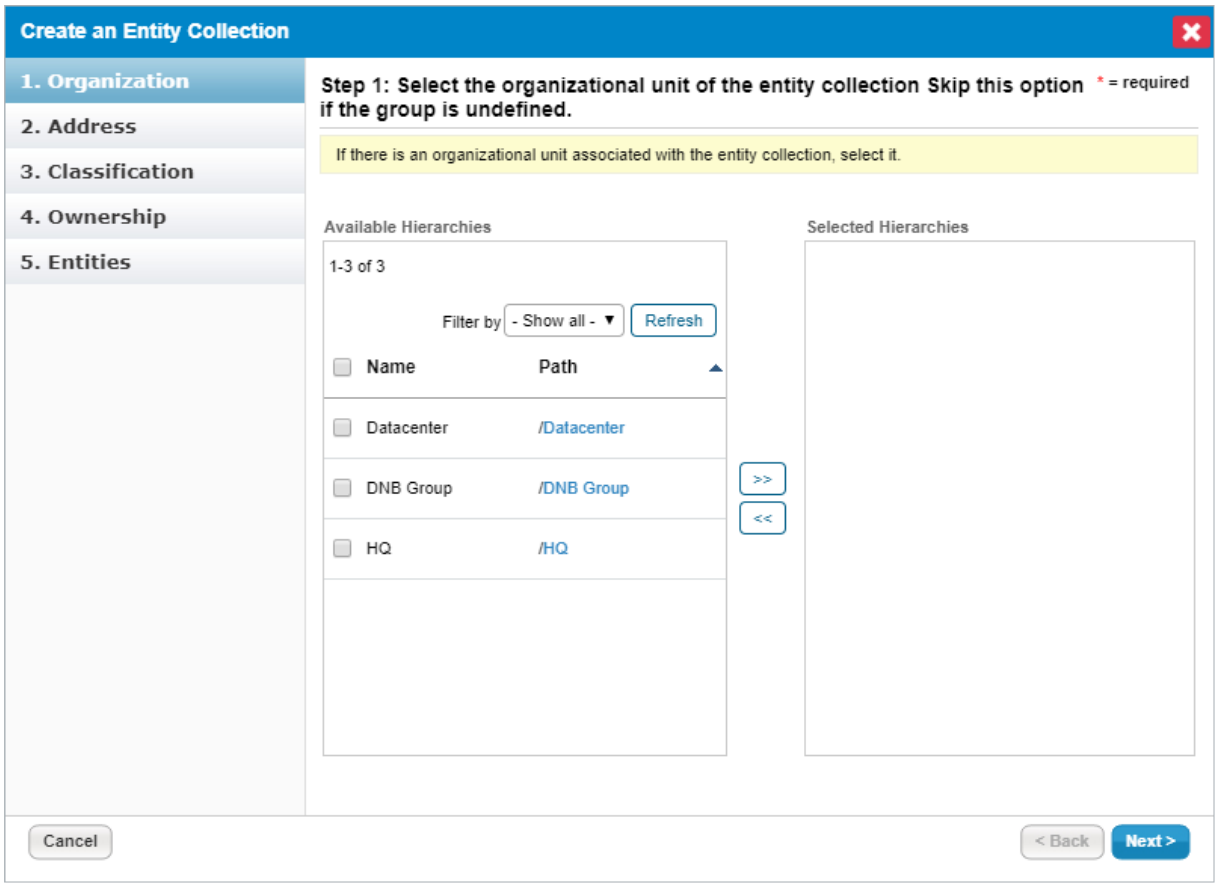
To create an entity collection:

1. Go to **Entities** > **Entity Collections** and click **New**.



The Add Entity Collections to your Organization screen.

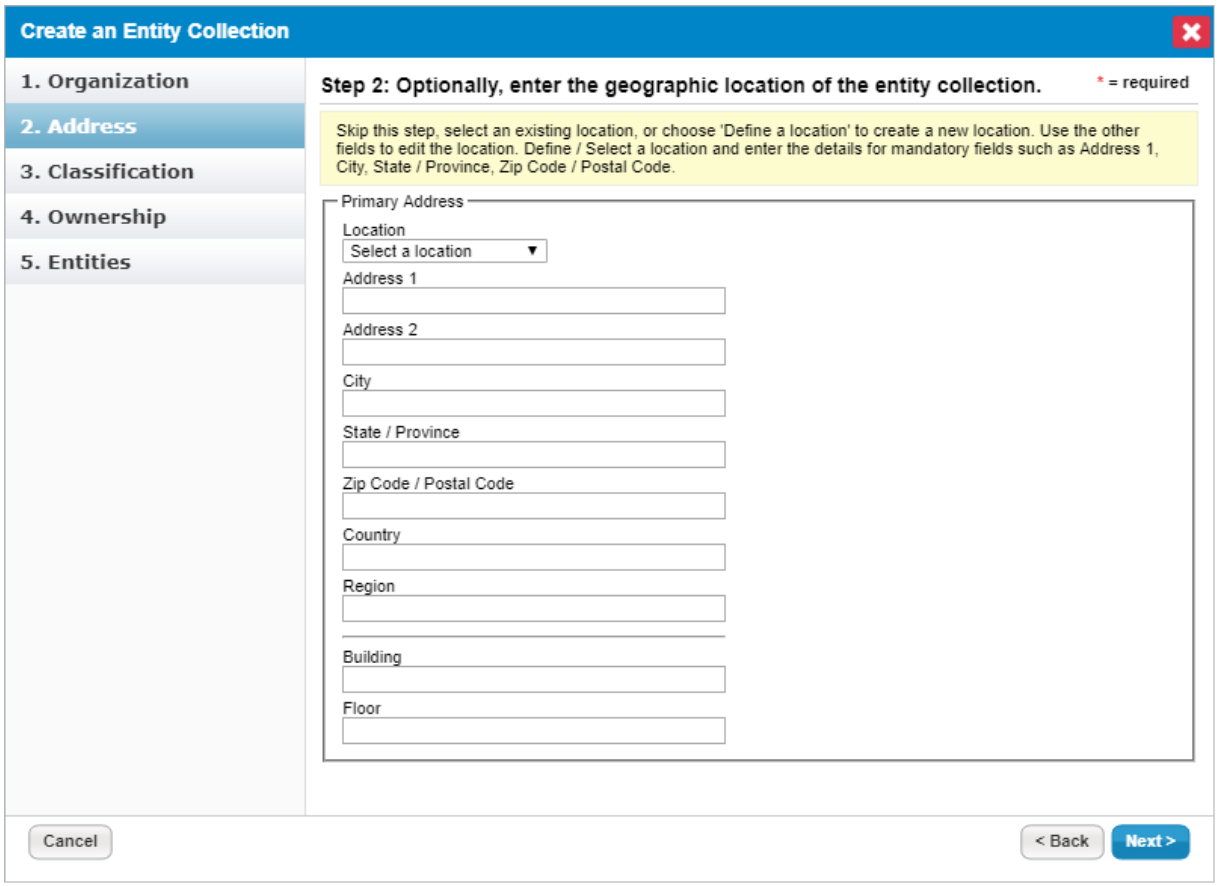
2. Enter a name in the **Name** field.
3. **Optional:** Enter a description in the **Description** field.
4. Click the **Entity Collection** Type dropdown and select a sub type, or define a new subtype. As a logged in user, you will be the primary owner for the entity collection by default. To change the primary owner, choose a name from the **Primary Owner** dropdown list or click **+**.
5. Click **Next**.
6. Select an organizational hierarchy container from the **Available Hierarchies** section, if available.



The Organization step of the Create an Entity Collection wizard.

7. Click **Next**.

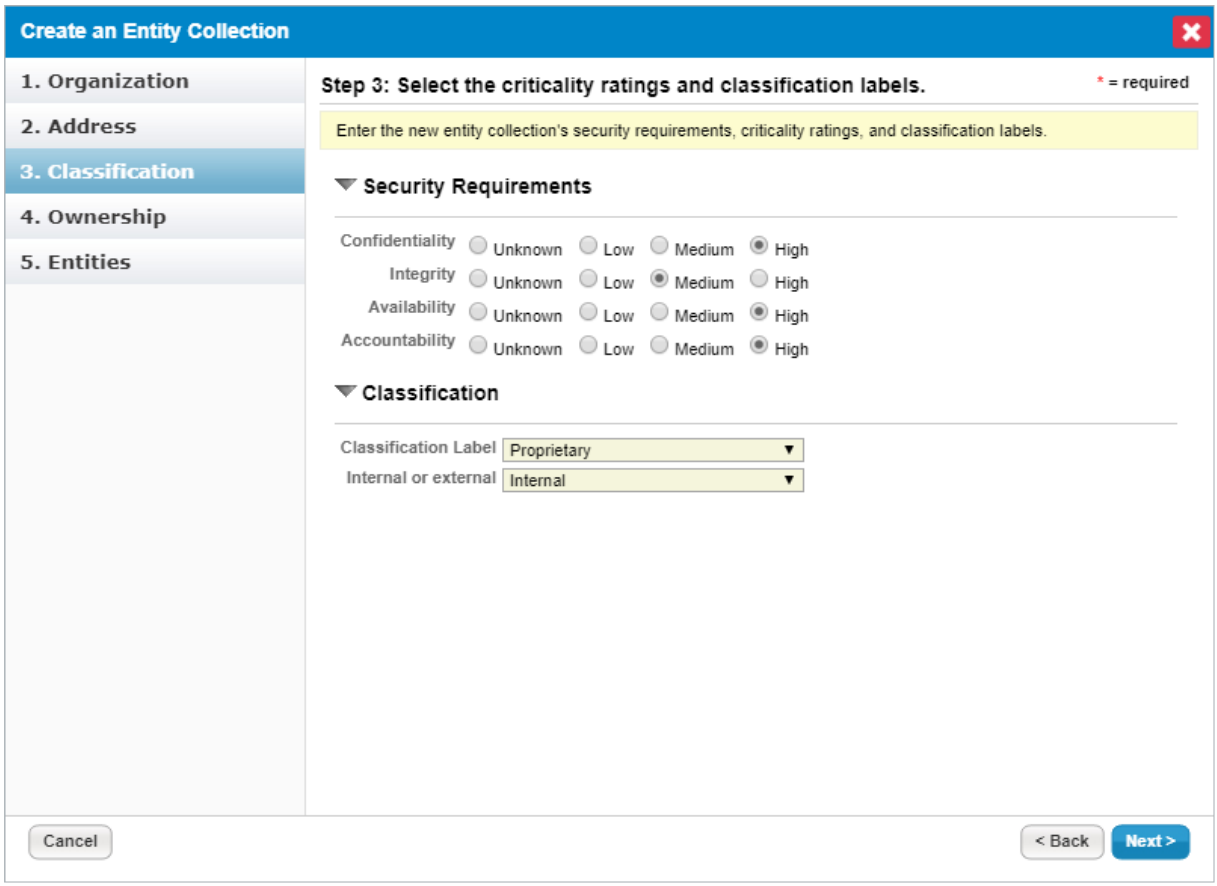
8. **Optional:** Enter the entity collection's geographic location.



The Address step of the Create an Entity Collection wizard.

9. Click **Next**.

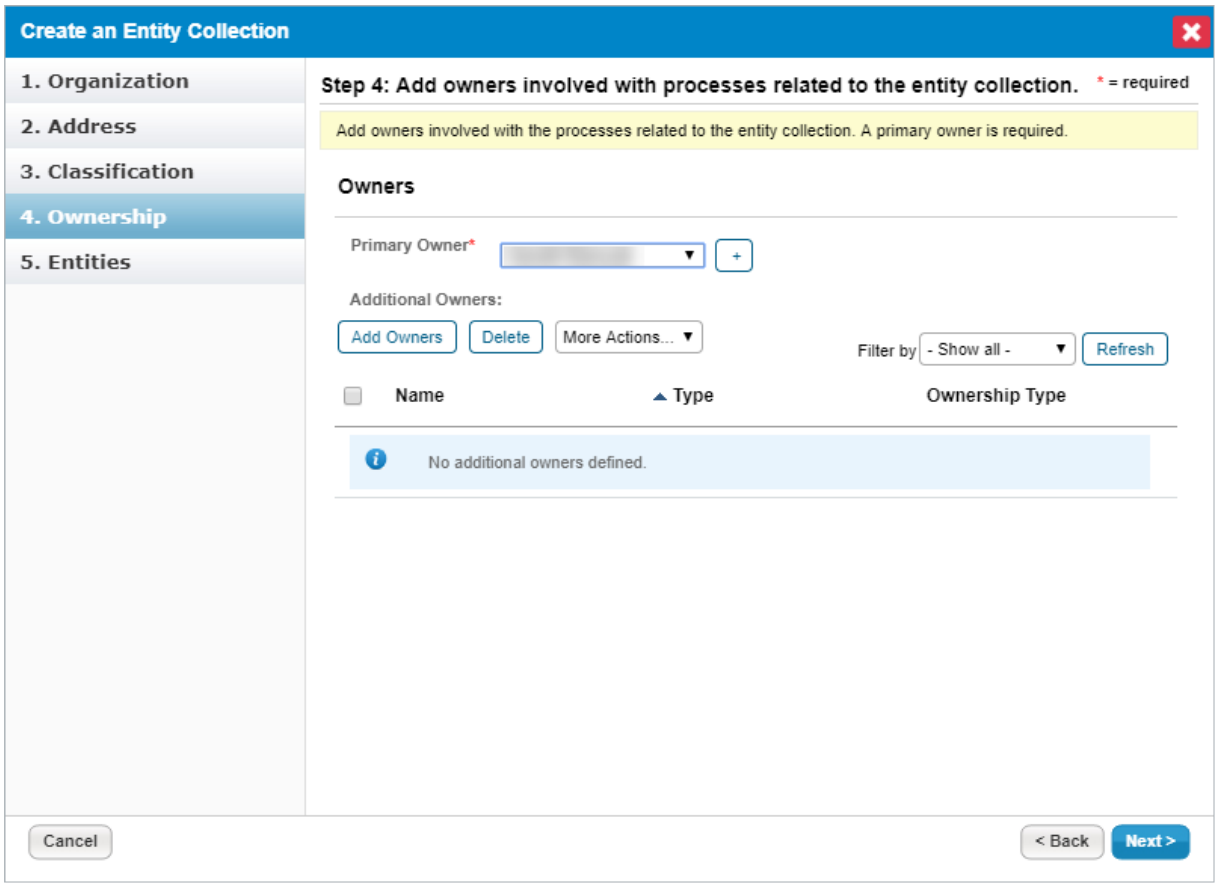
10. Classify the new entity collection in terms of confidentiality, integrity, availability, accountability, and classification, and specify if it's internal or external.



The Classification step of the Create an Entity Collection wizard.

11. Click **Next**.

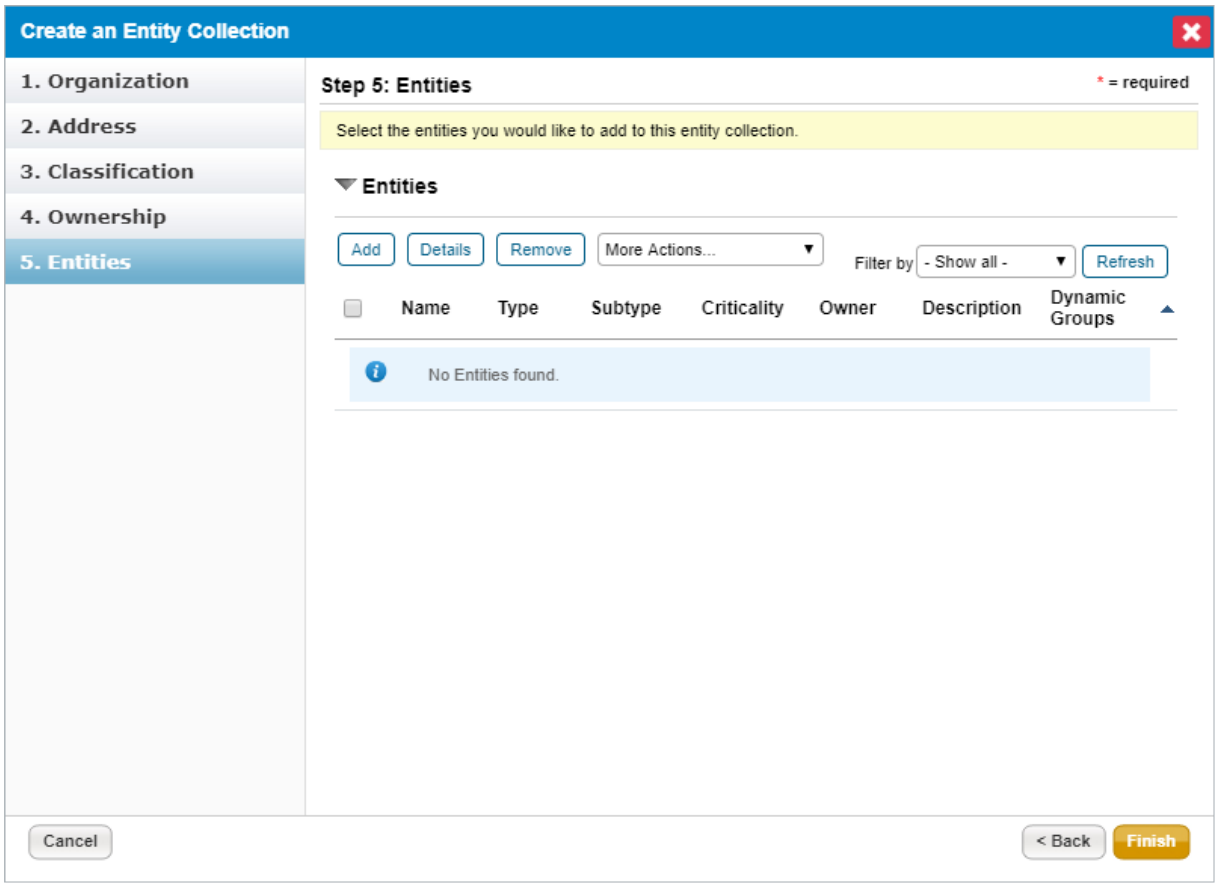
12. Select a different primary owner, if appropriate. The entity collection must have a primary owner. You can also specify additional owners.



The Ownership step of the Create an Entity Collection wizard.

13. Click **Next** to continue.

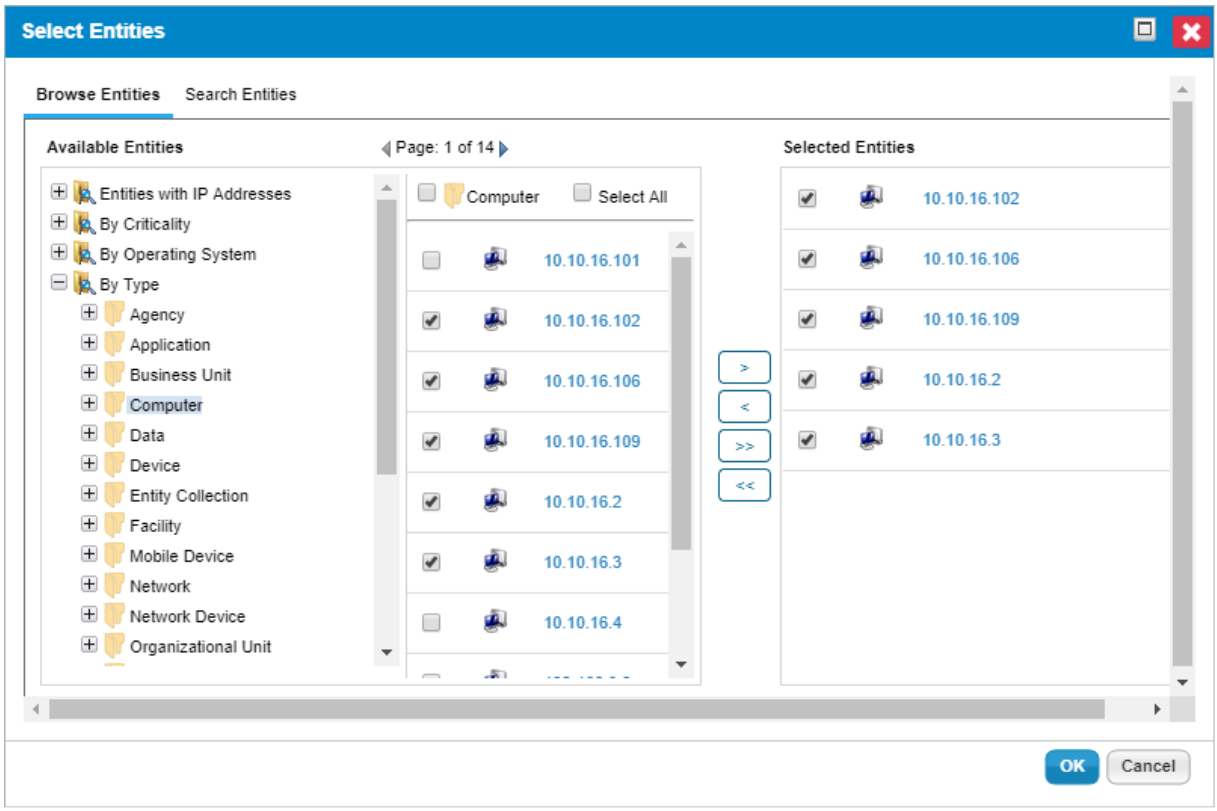
14. Click **Add**.



The Entities step of the Create an Entity Collection wizard.

15. Go to the **Browse Entities** tab > **Available Entities** and select a group. Or, click **Search** to search for an entity. After the entity(s) or group is found, select any appropriate entities, or **Select All**, or select the dynamic group.

16. Click **>>** to move the entity(s) or group to the **Selected Entities** box, then click **OK**.



The Select Entities dialogue.

When adding a dynamic group or its members:

- Selecting only specific entities within a dynamic group will associate only those entities as members of an entity collection.
- Selecting a dynamic group will associate all entities as members of an entity collection. When members are added or removed from a dynamic group, those dynamic members within an entity collection are updated automatically.
- Select All will associate all entities as members of an entity collection, but not the dynamic group. When members of a dynamic group are added or removed, those dynamic group members within the entity collection are not updated.
- Entities that are a part of more than one dynamic group will be added only once to an entity collection, even if you add all dynamic groups containing that entity.

17. Click **Finish**.The new entity collection will be an 'entity collection' type entity.

To edit an entity collection:

1. Go to **Entities** > **Entity Collections** and locate the entity collection that you want to edit using the tree and grid views.
2. Click an entity collection name to open.
3. Select the tab with the information that needs to be edited, such as**General**, **Entities**, **Description**, or **Classification**.
4. Click **Edit** and make changes as needed.
5. Click **Save**.

To delete an entity collection:

Entity collections that are not associated with an assessment can be deleted.

1. Go to **Entities** > **Entity Collections** and locate the entity collection to be deleted using the tree and grid views.
2. Select the checkbox next to the entity collection to be deleted.
3. Click **Delete**, then click **OK**.

Entity collection task limitations

There is currently no predefined template for importing entity collections into RiskVision, so they must be entered manually.

Understanding Entity Collection Details

Unlike with entities, entity collection details tabs do not vary. When you create an entity collection, it's created as 'entity collection' type entity in RiskVision. As a result, tabs, such as General, Assessments, Owners, Description, Addresses, Classification, Cost & Impact, Relationships, Documents, and Data Feeds that are commonly available in details page of various entity types can also be found in the entity collection details page. As a primary owner of an entity collection, it is important to understand the following tabs to configure and manage an entity collection.

Tab	Description
Composition	Displays the number of objects grouped by type that constitutes an entity collection. Click an entity type to drill down into all the entities of that type.
Entities	Displays the objects available in an entity collection. The Entities tab allows you to manage entity collection members, such as, entities and dynamics groups. Use Remove option to remove entities that are a part of dynamic group or entity collection and choose Remove Dynamic Groups from the More Actions drop-down list to remove a dynamic group.

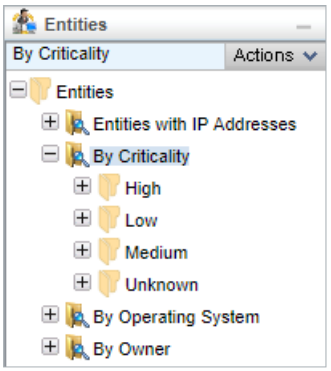
About Dynamic Groups

Dynamic groups include entities based on matching attribute values and filter conditions. Dynamic groups are used for assessments, displays and reporting. This feature is useful for managing very large collections of entities, called entity collections.

Dynamic group folders contain dynamic groups and child groups. Dynamic groups are displayed in a pane to the left of the entities and entity collections grid. For assessments and reports, you can select dynamic groups and child folders, but not top level folders.

Dynamic groups can contain entities and entity collections. When viewing dynamic groups in the **Entities** grid, you will only see entities. Similarly, when viewing dynamic groups in the **Entity Collections** grid, you will only see entity collections. Along these lines, if a dynamic group only has entities, then you will not see it in the **Entity Collections** grid, and if a dynamic group only has entity collections, you won't see it in the **Entities** grid.

The following example shows the default By Criticality group:



The default By Criticality group.

RiskVision automatically creates High, Low, Medium, and Unknown groups.

Performance Note

Be careful when creating dynamic groups that will create thousands of folders, because user interface performance will suffer. For example, do not create a dynamic group for "By Owner" in a system with 20,000 entities and 10,000 owners. This would create 10,000 folders, which would cause the system to respond slowly, making it difficult to scroll to the desired folder.

Default Dynamic Groups

The following table provides a brief description of the default groups available. To add, update or delete a custom defined dynamic group or a pre-configured group, you must have the Entity View and Entity Manage permissions.

Dynamic Group	Description
Type of Entity	Groups by Type and Subtype.
By Criticality	Groups all entities based on the business criticality score, which is, the average of the user defined CIAA (Classification > Security Requirements > Confidentiality, Integrity, Availability and Accountability) rating.
By Operating System	Groups computers and network devices by operating system settings (Entity Details > System Details).
By Subnet	Groups computers and network devices by the specific interface subnet range. (The range is calculated using the subnet mask set on the System Details > Network > Network Interface details panel.) If the subnet mask is null, the device shows in the top level folder only, even if the IP address is within a recognized range. Overlapping ranges are grouped separately.
All Vendors	Lists all vendor type entities.
All Processes and Objectives	Lists all process type entities for use with ERM method of risk assessment and calculation.
Active Directory	Groups Domain entity types. While using the AD Connector to import Active Directory data, the entities are automatically structured.
My Entities	Lists all entities that the current user is assigned to as any type of owner. User access is also limited by filters assigned to them and their roles.
Recently Viewed	Contains the last ten entities the current user viewed. Configure the maximum number of entities in the Recently Viewed group which is configured in the .properties file.
My Favorites	Entities that you identified as a favorite by clicking the Favorites link on the entity's detail page.
Newly Discovered Entities	Groups discovered entities (that is, an entity with the General > Entity Management > Status of Discovered) by operating system, network subnet, and entity type. When a connector finds a new entity and imports the details, the entity status is set to Discovered.
Unmanaged Entities	Lists unmanaged entities (an entity with the General > Entity Management > Status of Unmanaged). Many of the default groups are filtered by Managed status. They show only entities that have the Managed status.

Configuring the Dynamic Grouping

The RiskVision solution automatically creates a subgroup based on the selected entity attributes.

Grouping Applications

The following table describes the group-by options for Entity type applications:

Group by	Category	Description
ApplicationSystem Flags	Internet Facing	Creates True, False, and Unknown groups that include Entities of type application based on the Description > Network Access > Internet Facing attribute.

Grouping Entities By Attributes

The Entity options allow you to create groups by attributes that are common to all entity types. Use filters to limit the Entities by type.

The following table describes the group-by options for Entities:

Group by	Category	Description
Entity Address	Address	Creates a group for each unique street addresses.
	Building	Creates a group for each unique building names.
	City	Creates a group for each unique city names.
	Country	Creates a group for each unique country names.
	Name	Creates a group for each unique Location Names.
	Postal Code	Creates a group for each unique Zip/ Postal code.
	Region	Creates a group for each unique Region.
	State	Creates a group for each unique State.
Entity Classification	Availability Impact	
	Availability Score	
	Classification Label	Creates a group for Top secret, Highly confidential, Proprietary, Internal use only, and Public for the **Classification > Classification Label > Classification Label**.
	Confidentiality Impact	
	Confidentiality Score	
	Criticality	Creates a group for High, Medium, and Low or VH, H, M, L, and VL depending on your Entity Configuration settings for Criticality ratings. Groups entities by their Business Criticality score.
	Criticality Score	
	Integrity Impact	
	Integrity Score	

Group by	Category	Description
Entity Description	Compliance Level	
	Container Level1	Custom option that structures user-defined attributes.
	Container Level2	
	Container Level3	
	Container Level4	
	Container Level5	
	Container Level6	
	Division	Creates a group for each unique General > Organization > Division attribute. **Note:** Used in the structured Organization default dynamic group folder.
	Domain	Creates a group for each entity type Domain **General > Domain** attribute. Used for an Active Directory DN (distinguished name).
	Installation Date	**Organizational Unit, Domain, Computer, Network Devices**: Creates a group for each unique General > Maintenance > Installation date. Account: Creates a group for each unique Description > Create attribute.
	Internal or External	Create an Internal, Public Facing, and unknown group sorts by the Classification > Classification Label selection.
	Inventory Tag	
	Manufacturer	Creates a group for each unique General > Information > Manufacturer attribute.
	Model	
	Organization	
	Risk Assessment Status	
	Risk Assessment Next Review Date (by Month)	
	Sub Division	
	Subtype Type	Creates a structured group Type/subtype for each unique General > Information > Subtype.

Group by	Category	Description
Entity Ownership	User Id - All Owners	Creates a group, that has the **User & Roles > User > Username** field as the group name, for each user who owns an entity regardless of the ownership role.
	User Id - Direct Ownership	Creates a group, that has the **User & Roles > User > Username** field as the group name, for each primary owner.
	User Id - Indirect Ownership (through a team)	Creates a group that has the **User & Roles > User > First and Last Name** fields as the group name, for each user who owns an entity through a team regardless of ownership role.
	User Name - All Owners	Creates a group that has the **User & Roles > User > First and Last Name** fields as the group name, for each user who owns an entity regardless of the ownership role, including users who own the entity through a team.
	User Name - Direct Ownership	Creates a group that has the **User & Roles > User > First and Last Name** fields as the group name, for each primary owner.
	User Name - Indirect Ownership (through a team)	Creates a group that has the **User & Roles > User > First and Last Name** fields as the group name, for each user who owns an entity through a team regardless of ownership role.
Entity Stage	Stage	
Entity Tag	Name	
Entity Vulnerability	CVSS Score	Creates a group for each vulnerability CVSS score of vulnerabilities assigned to computer and device entities. **Note**: Use a filter to match only entities with vulnerabilities, such as an entity filter with the Vulnerability Name Not Null condition. Otherwise, the unknown group includes both entities without vulnerabilities and entities with vulnerabilities that do not have the CVSS score set.
	CVSS Vector	
	Description	Creates a group for each unique vulnerability description, see Vulnerability > Vulnerability List > Vulnerability Details > General > Vulnerability.
	Likelihood	
	Severity	Creates a group for each severity level of a vulnerability.
	Source	Creates a group for each vulnerability author or source.
	Type	Creates a group for each type of vulnerability.

Grouping Computer And Network Devices

The following table describes the group-by for Computer and Network Device type entities:

Group by	Parameter	Creates a group for each unique parameter
ComputerSystem Address	Building	Creates a group for each unique building name.
	City	Creates a group for each unique city name.
	Country	Creates a group for each unique country name.
	Name	Creates a group for each unique Location Name.
	Postal Code	Creates a group for each unique Zip/Postal code.
	Region	Creates a group for each unique Region.
	State	Creates a group for each unique State.
ComputerSystem Application	Application Name	Creates a group for each unique System Details > Application > Application Name attribute. **Note**: When multiple applications are installed, the system appears in multiple groups.
	Publisher	Creates a group for each unique System Details > Application > Publisher Name attribute.
	Type	
	Version	Creates a group for each unique System Details > Application > Version Number attribute.
ComputerSystem By Date	Installation Date	Creates a group for each unique General > Maintenance > Installation date.
	Month	Creates a group for each unique month and year of the General > Maintenance > Installation date.
	Week	Creates a group for each unique week and year, where the first day of the week is the previous Monday, of the General > Maintenance > Installation date.
	Weekday	Creates a group for each unique day of the General > Maintenance > Installation date.

Group by	Parameter	Creates a group for each unique parameter
ComputerSystem Classification	Availability Impact	
	Confidentiality Impact	
	Criticality	Creates a group for High, Medium, and Low or VH, H, M, L, and VL depending on your Entity Configuration settings for Criticality ratings. Groups entities by their Business Criticality score.
	Integrity Impact	
ComputerSystem Description	Domain	Creates a group for each unique Description > Identification > Domain Name attribute. **Note**: The System Details > Network Domain Name field is the same attribute.
	Host Name	Creates a group for each unique System Details > Network Domain Name attribute.
	Installation Date	Creates a group for each unique General > Maintenance > Installation date.
	Inventory Tag	
	Manufacturer	Creates a group for each unique General > Information > Manufacturer attribute. **Note**: The General > Information > Manufacturer and Description > Physical Description Manufacturer field are the same.
	Subtype	Creates a group for each unique General > Information > Subtype. **Note**: Computer and Network Device entity types are grouped together unless you set a filter.
ComputerSystem Network	Subnet	Creates a group for each unique subnet range. The subnet range is automatically calculated from the address settings in the System Details > Network > Network Interface Card dialog. **Note**: Overlapping ranges are grouped separately.
	Subnet Mask	Creates a group for each unique subnet mask of the System Details > Network > Network Interface Card > Subnet Mask.

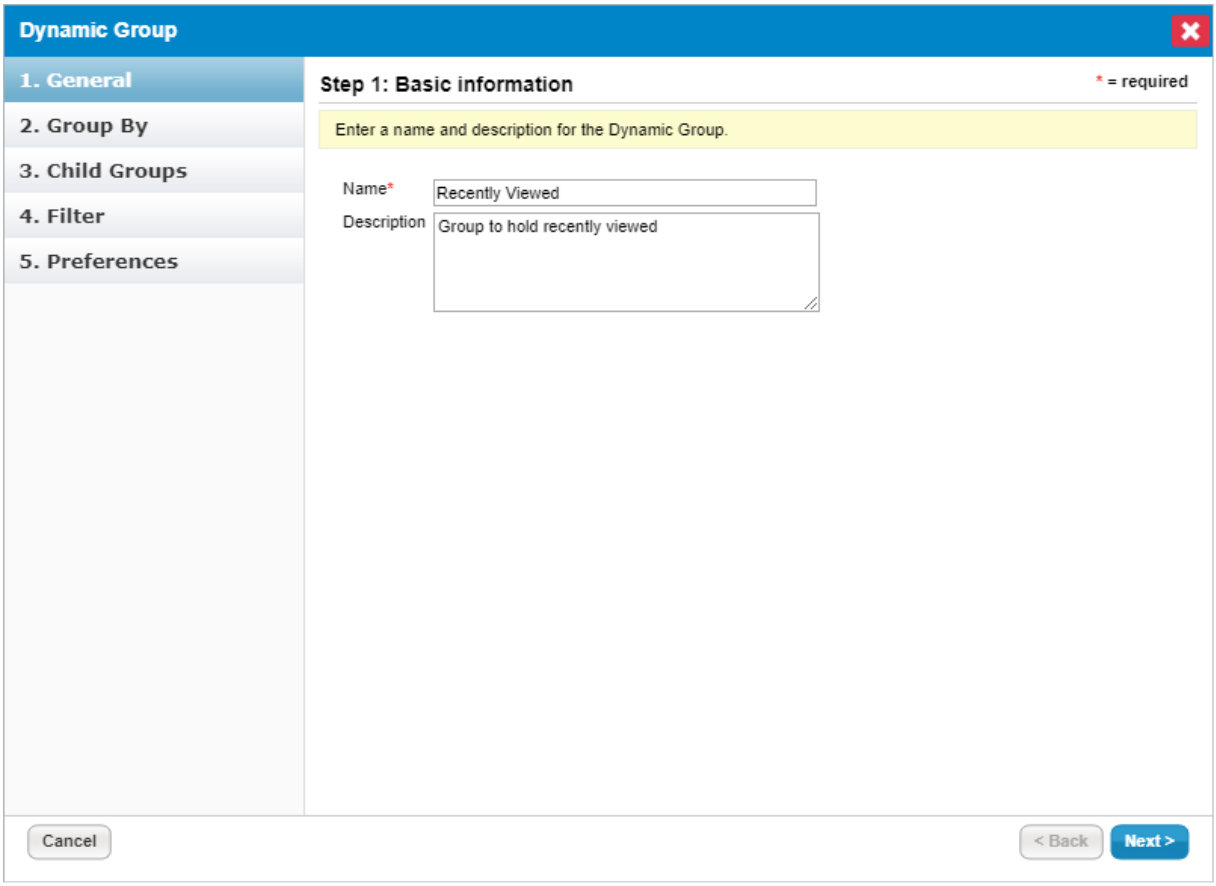
Group by	Parameter	Creates a group for each unique parameter
ComputerSystem OperatingSystem	OS Name	Creates a group for each unique System Details > Operating System > Name attribute.
	OS Version	Creates a group for each unique System Details > Operating System > Version attribute. **Note**: Some connector discovered computers have the version number in the OS name field.
	OS Version Name	Creates a group for each unique System Details > Operating System > Version Name attribute.
ComputerSystem Vulnerability	CVSS Score	Creates a group for each vulnerability CVSS score of vulnerabilities assigned to computer and device entities. **Note**: Use a filter to match only entities with vulnerabilities, such as an entity filter with the Vulnerability Name Not Null condition. Otherwise, the unknown group includes both entities without vulnerabilities and entities with vulnerabilities that do not have the CVSS score set.
	CVSS Vector	
	Description	Creates a group for each unique vulnerability description, see Vulnerability > Vulnerability List > Vulnerability Details > General > Vulnerability.
	Likelihood	
	Severity	Creates a group for each severity level.
	Source	Creates a group for each vulnerability author or source.
	Type	Creates a group for each vulnerability type.

Configuring Dynamic Group Folders

Modifications to an existing folder take effect immediately. When a group or child folder is part of an assessment, the newly matching entities are automatically added to the assessment. If the modification removes entities from the group or child folder, the assessments for the entities are automatically removed from the program. In order to modify an existing dynamic group or create a dynamic group, you must have Entity View and Entity Manage permissions.

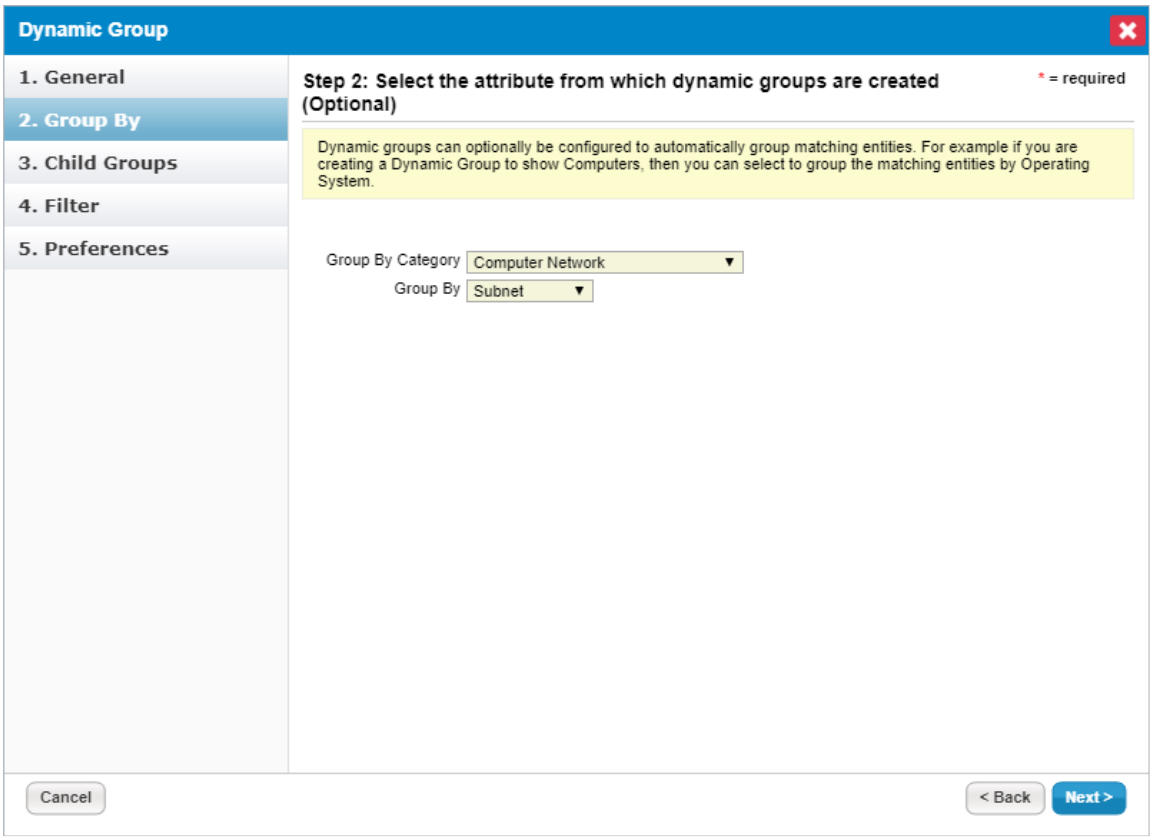
To modify an existing group:

1. Go to **Entities** > **Group Definitions**.
2. Click the group, then click **Edit** to open the **Dynamic Group** wizard.
3. Enter a Name and Description.



Step 1 of the Dynamic Group wizard.

4. Click **Next**.
5. **Optional**: Configure the dynamic group settings:
    - To group applications by flags, click the **Application System Flags** and **Internet Facing** checkboxes.
    - To group entities by an attributes, select the options from the Grouping Entities table.
    - To group computer and network devices, select the options from the Grouping Computer and Network Device table.
    - If you skip this option, the folder will display a list of the entities that match the filters.

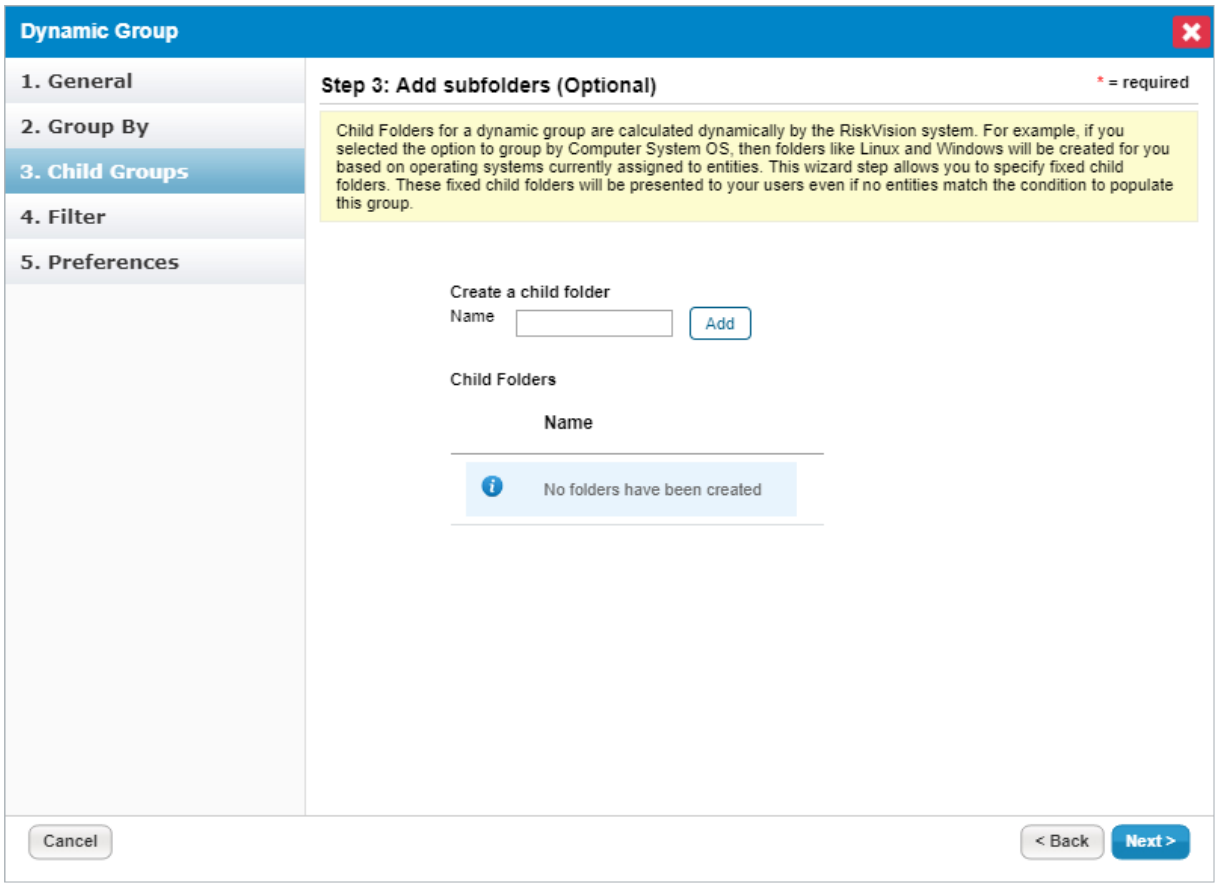


Step 2 of the Dynamic Group wizard.

6. Click **Next**.

7. Enter a name that's similar to the value of the attribute that you want to match, then click **Add**.

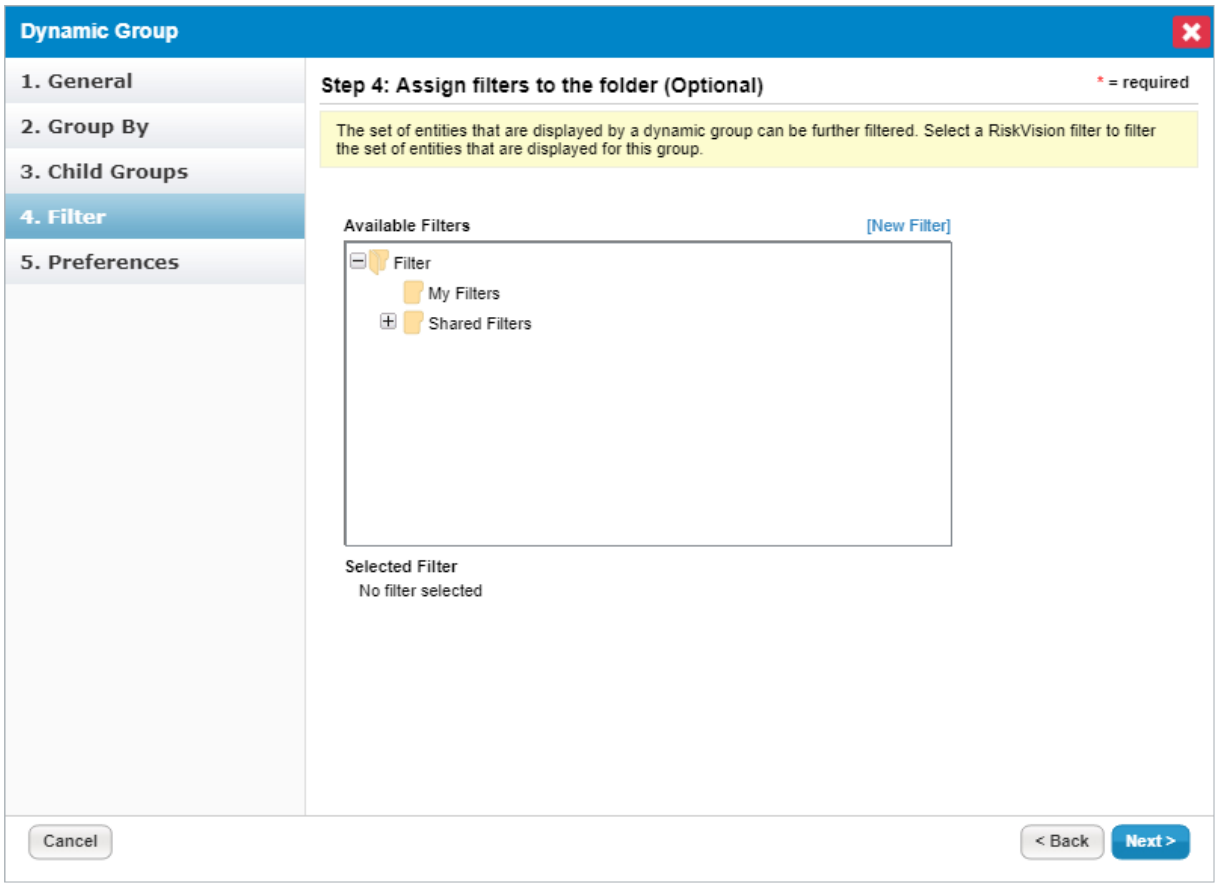
   The child folder will appear in the **Entity** and **Program Wizard Entity** selection trees. RiskVision sorts entities with a matching attribute value into the appropriate folder and allows prepopulation of values during entity creation for organizations. For example, if you create a Division child folder called Engineering, the Engineering folder displays on the Organization page of the Entity Wizard. When it is selected, the Entity Organization/Division is automatically set to Engineering.



Step 3 of the Dynamic Group wizard.

8. Click **Next**.

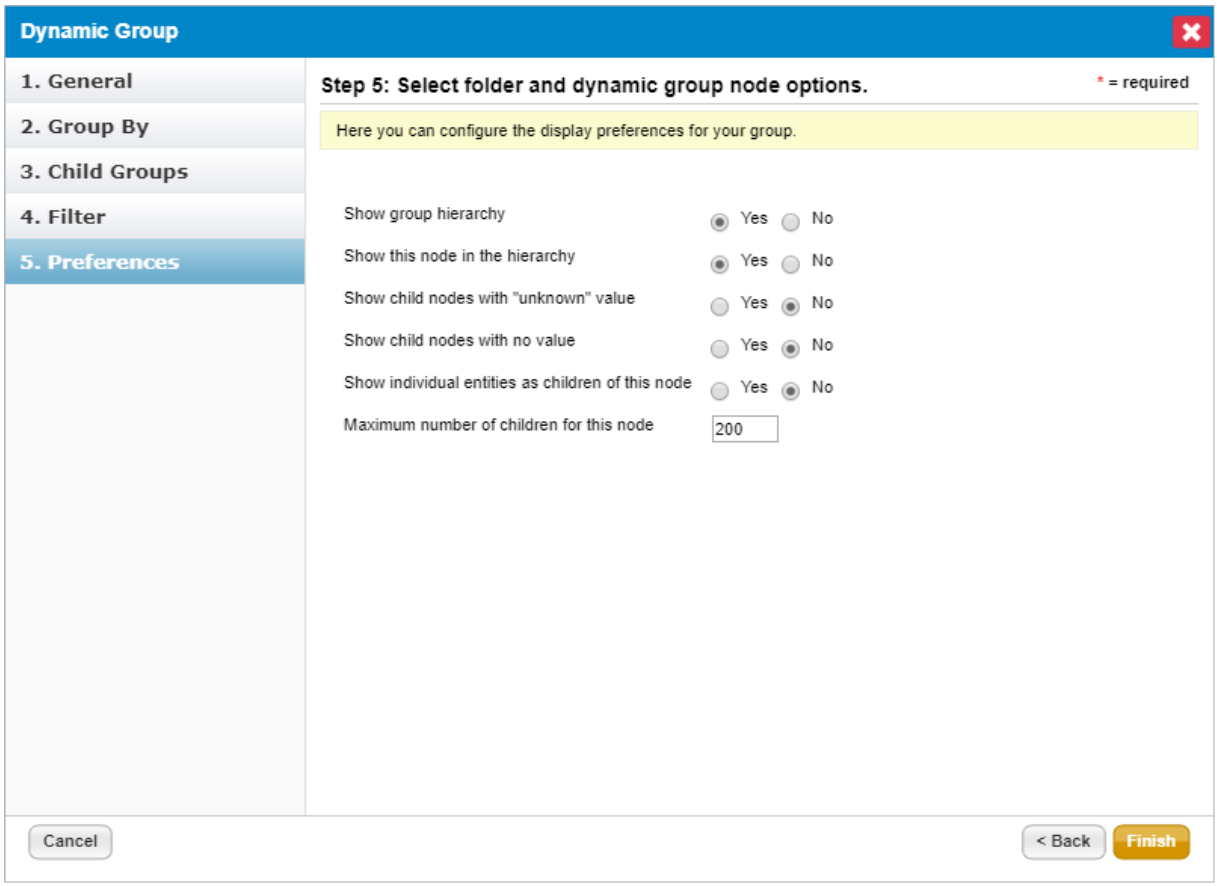
9. Select a filter to limit the entities grouped or listed. You can select one filter. To use the Match Filter option to combine multiple filters, see Configuring filters.



Step 4 of the Dynamic Group wizard.

10. Click **Next**.

11. Select the folder and dynamic group settings, then click **Finish**.



Step 5 of the Dynamic Group wizard.

The dynamic group folder displays in the list and entities matching the settings are dynamically grouped on the **Entities** page.

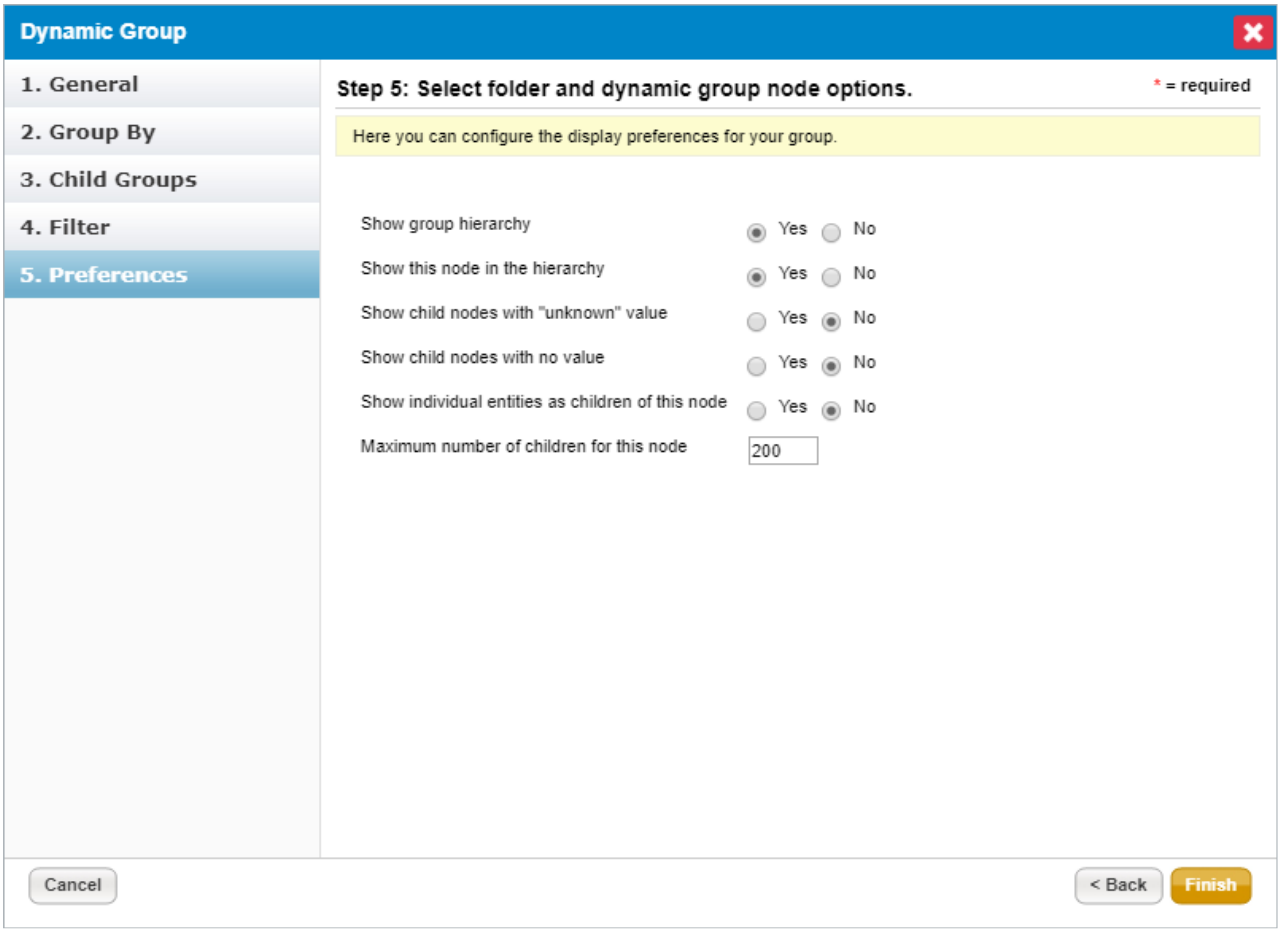
Setting the Name and Description

Specify the following fields:

- Name. Identifies the folder that contains the dynamic groups and/or child groups.
- Description. The Summary that displays on the Group Entities page.

Setting Folder and Grouping Preferences

Folder preferences control how dynamic and child groups display in the **Entities** tree and **Program Wizard Entity** selection tree.

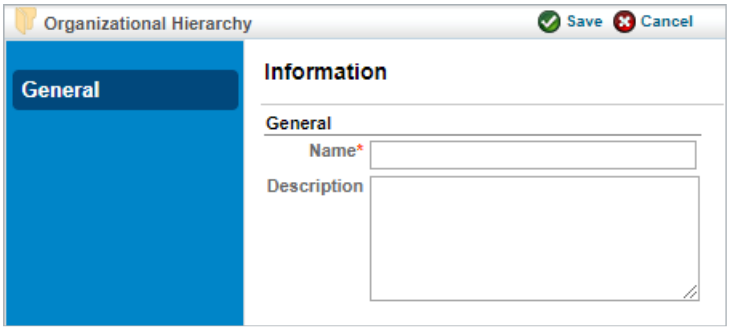


The folder and grouping preferences in the Dynamic Group wizard.

SETTING	DESCRIPTION
Show group hierarchy	Displays dynamic groups in the folder. If disabled, the group will be hidden from users.
Show this node in the hierarchy	Hides the folder that contains the dynamic groups in the Entity and Program Wizard pages.
Show child node with Unknown value	Displays Unknown group that contains entities that the group by category attribute that matches Unknown.
Show child node with no value	Displays N/A group that contains entities for which the matching group by category attribute is not defined.
Show individual entities as children of this node	Displays entities in the Entities and Program Wizard Entities tree.

Understanding Organizational Hierarchy

The names and relationships of divisions, departments, and other organizational units within an enterprise can be modeled in RiskVision, and individual organizational units can be associated with other components of the system.



The New Organization Group screen.

Organizational units represent a "tree" of nodes. Each node has a single parent node and may have child nodes.

When adding an organization hierarchy node to a profile or other component, use 'Contains.' Do not use the '==' operator.

Organization Hierarchy Actions

Each node and its child nodes in an organization hierarchy tree can be moved, copied, or deleted using the Actions pull-down menu that appears when you select a node, or, when you use the Actions drop-down box that appears on the top right-hand corner of the General tab when you open a node's details.

To add an organization hierarchy node:

1. On the **Entities** menu, click **Group Definitions**.On the **Vendors** menu, click **Group Definitions**.
2. In the **Organization Hierarchy** tree, search the node, and then select it. Any child nodes that are available, appear in the child hierarchies section.
3. If you want to move all the child nodes of a node, choose **Cut** from the Actions pull-down menu of the organizational hierarchy tree. Select a node to which you want to move a node and then choose **Paste** from the **Actions** pull-down list of the organizational hierarchy tree.
4. To move a child node, select the node to open its details. Choose **Move To** from the **Actions** drop-down box, and then click **Go**. The **Move Hierarchy** dialog appears. Select a hierarchy and click **OK**.

To delete an organization hierarchy node:

1. On the **Entities** menu, click **Group Definitions**. On the **Vendors** menu, click **Group Definitions.**
2. Find the node to delete in the **Organization Hierarchy** tree.
3. To delete a root node, select a node in the organization hierarchy tree, choose Delete from the Actions pull-down menu and then confirm the action. To delete a child node, select the node to open its details. Choose **Delete** from the **Actions** drop-down box, click **Go** and then confirm the action. This provides the ability to retain the significant child nodes if you do not want to delete the complete node from the organization hierarchy tree.

To copy and paste an organization hierarchy node

1. On the **Entities** menu, click **Group Definitions**. On the **Vendors** menu, click **Group Definitions**.
2. In the **Organization Hierarchy** tree, search the node, and then select it. Any child nodes that are available, appear in the child hierarchies section.
3. If you want to copy all the child nodes of a particular node, choose **Copy** from the **Actions** pull-down menu of the organizational hierarchy tree. Select a desired node to which you want to copy a node and then choose Paste from the Actions pull-down list of the organizational hierarchy tree.
4. To copy a child node, select the node to open its details. Choose **Copy To** from the **Actions** drop-down box and then click **Go**. The Copy Hierarchy dialog appears. Select a hierarchy and click **OK**.

To move an organization hierarchy node:

1. On the **Entities** menu, click **Group Definitions**. On the **Vendors** menu, click **Group Definitions**.
2. In the **Organization Hierarchy** tree, search the node, and then select it. Any child nodes that are available, appear in the child hierarchies section.
3. If you want to move all the child nodes of a node, choose **Cut** from the Actions pull-down menu of the organizational hierarchy tree. Select a node to which you want to move a node and then choose **Paste** from the Actions pull-down list of the organizational hierarchy tree.
4. To move a child node, select the node to open its details. Choose **Move To** from the **Actions** drop-down box, and then click **Go**. The Move Hierarchy dialog appears. Select a hierarchy and click **OK**.

Enabling the Organization Hierarchy Selection

When you create a node under the organization hierarchy tree, by default, the nodes are not visible for you to make a selection in the entity wizard or when you want to assign an organization group to an existing entity. Configure the following properties to enable the selection for RiskVision users.

1. **entity.organization.assignment.through.hierarchy= [true |false]**

   This property displays the new organization hierarchy in entity details pane when it is set to true. By default, the property is set to false.

2. **entity.organization.through.hierarchy= [true |false]**

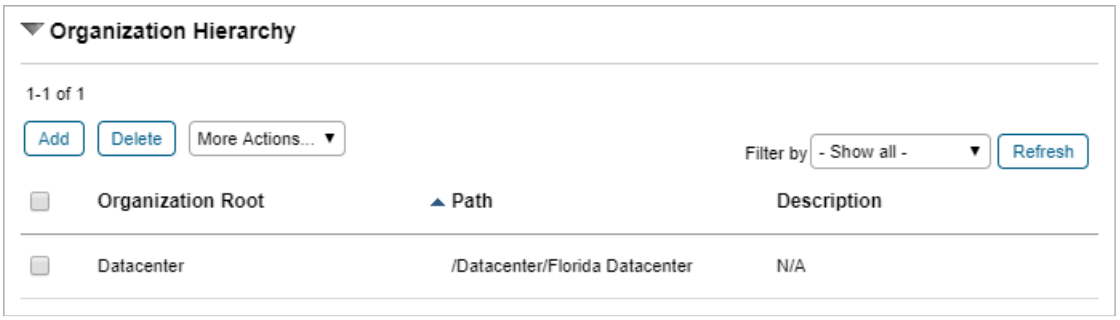
   This property allows you to select new organization hierarchy in entity wizard when it is set to true. By default, the property is set to false.

Defining a New Organization

Entities can be associated with multiple nodes in an enterprise's organizational hierarchy. For example, the hierarchy might be defined by location and division. An entity might belong to a particular department and may be located in a particular facility.

In previous versions of RiskVision, each entity had single-value fields for organization, division, and subdivision.

Associated nodes are in the organizational hierarchy with an entity on the **General** tab of the entity.



The Organization Hierarchy in the General tab of an entity.

Your organizational hierarchy defines your enterprise. You can define various hierarchies and combine them to cross-categorize your entities. For example, your organizational trees might be defined based on:

- Organization: Division, subdivision, department, group.
- Location: Country, region, facility, building, floor, section.
- Function: Retail/b2b, industry, market.

To create an organization node:

1. Go to **Entities** > **Group Definitions** and click **Organizational Hierarchy** in the tree.
2. Click **New Organization Group**, or navigate to an existing node and click **Actions** > **New Child**.
3. Click **Go** and enter the new child node's name and description.
4. Click **Save**.

Note:

- Nodes can also be copied, moved, and deleted using the **Actions** dropdown menu.
- From release 6.5 SP1 HF3 on, the organizational hierarchy supports a maximum number of 15 nodes.

Entity Management

The **Entity Management** page provides on-going information about entities present in the RiskVision system using dashboards that are available on each tab. To view dashboards, you must have the Entity View and Entity Manage permissions. The following table lists the tabs available on the **Entities** > **Entity Management** menu and describes what information each tab represents.

Tab	Description
Summary	Displays dashboards that provides you the managed, unmanaged, discovered, and entity type wise count of entities.
Reconciliation	Displays a vertical bar chart that provides you the count of entities that came from multiple sources, for example, scanner and other sources, and user created.
Manage	Displays a grid for entity types that provides you the count of discovered, managed and unmanaged entities for each entity type.
Classification	Displays dashboards that provides information on managed entities' classification, criticality and ownership data. Each dashboard shows "Yes" and "No" followed by a count of entities. The "Yes" followed by a count denotes that many managed entities have classification, criticality, and ownership. And the "No" followed by a count denotes that many managed entities have no classification, criticality, and ownership.
Assessment Progress	Displays a dashboard that provides the workflow stage wise count of entities.
Vulnerabilities	Displays a dashboard that provides the count of entities affected by the vulnerabilities and entities that have no vulnerabilities.
Controls & Questions	Displays a dashboard that provides you the count of entities that have controls and questionnaires assigned to them.

About the Content Folders

The Content navigation pane is a hierarchical tree, differentiating -provided content from your organization's content.

- **RiskVision Content Library**-- provides Resolver -defined read-only content (documentation, templates, controls, and subcontrols) to enforce, monitor, and calculate compliance and risk scores based on common industry standards, such as NIST SP 800-53. To enforce controls, the library includes both automated and manual/questionnaire control checks. In the case of automated controls, the appropriate Resolver connectors run checks on targeted entities and return results to the Resolver System. For manual control checks, the RiskVision solution automatically distributes questionnaires to the appropriate entities stakeholders and collects the results from responses to questionnaire questions.

  Controls and subcontrols for the NIST SP 800-53 standard are provided in the Content library by default. Controls and subcontrols for other standards are available for purchase from Resolver.

- **Organization Content** - The Organization Content tree is designed to hold the collection of controls you want your organization to use for compliance and risk measurement. By default, the Organization Content section includes some predefined groups for linking in your own organization's policy documents, control framework, and individual controls and subcontrols, but you can also create additional subgroups or folders within the current hierarchy to meet the needs of your own organization.

  Although users can assign controls directly from the Content Library hierarchy, it is recommended that you assign controls from the Organization Content hierarchy. Controls in the hierarchy that are linked or copied from the Content Library can be customized for your environment in the Organization Content hierarchy. Plus, by defining controls in the Organization Content hierarchy, you have more choices and can better manage updates when you synchronize with changes to the RiskVision Content Library.

Default Organization Content Folders

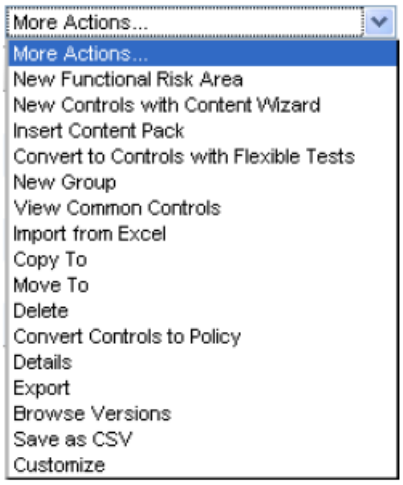
This section discusses the Organization Content folders that you will find under Controls & Questionnaires in the Content menu. These folders can be seen in the Compliance Manager, Enterprise Risk Manager, Vendor Risk Manager, and Policy Manager applications.Most of the folders are common to the applications specified above, except the Category folder, which is available in the Vendor Risk Manager and Policy Manager. The following table lists different folders and their purpose.

Check Templates	Default root folder for managing check templates for automated subcontrols. • Resolver Content folder provides predefined check templates. • Organization Content folder is empty by default and provides options for creating the custom check templates.
Organizational Documents/Policies	Default root folder for an organization's policy documents.
Organizational Documents/Contracts	Default root folder for an organization's contracts.
Controls	Default root folder for an organization's controls.
Choice Templates	Location of user-defined choice templates.
Questionnaires	Default root folder for managing questionnaires that are not associated with controls.
By Category	User-defined group folders for managing controls and other content.

Content Actions Overview

The RiskVision solution allows you to use RiskVision Content, out-of-the-box, and apply or assign read-only controls from the RiskVision Content library to entities in your enterprise. Create your own customized framework and hierarchy of controls under the Organization Content node in the Controls & Questionnaires navigation pane. By defining controls in this area, you can leverage existing RiskVision Content by choosing the frameworks, standards, and regulations for which you will measure compliance and risk, and then tailor and customize the controls to fit the exact requirements of your organization.

This section describes the actions available for tailoring and customizing content in the Organization Content hierarchy.



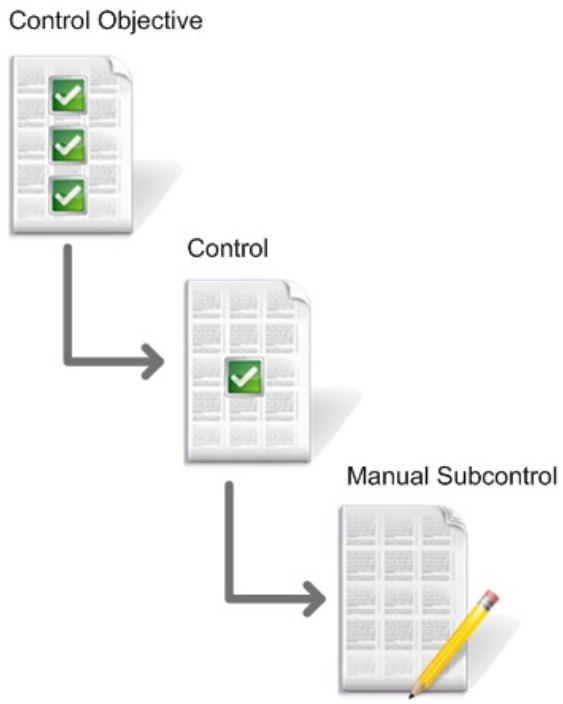
New functional risk area	Group	Create KRI functional risk area that contains key risks. This type of control and subcontrol uses the Key risk indicators (KRIs) model. The sub controls (questionnaires) also have additional attributes to hold scoring thresholds as well as input values for number, time and frequency-based reporting. For example, a user may enter multiple sets of values for a questionnaire question, where each value corresponds to a point in time. For example, if the question is "Average BCP Test delay (in days)," the user may enter a value for January, February, and March etc. The user also defines entities in the program for which assessment questionnaire answers are used to calculate risk scores.
	Content Pack	Allows you to group customized content into a package that is processed, from draft to approved state, tracks changes between content versions, and is published for use in assessments.
New Controls with Content Wizard	Group	See Selecting Domain-specific Controls.
	Content Pack	
Insert Content Pack	Group	Allows you to create a content pack in a group folder.
Convert to Controls with Flexible Tests	Group	See Using Configuring Control Testing.
	Content Pack	
	Control Objective	

New Control Objective	Content Pack	Allows you to create a control object.
New Control	Content Pack	Allows you to create a new control.
	Control Objective	
Promote to Group	Control Objective	Changes a control objective to a group.
New group	Content Pack (More actions)	Allows you to create a hierarchical structure in the Organization Content root directory, in a content pack, or control objective.

About Controls

Under any defined group, subgroup, or Control Content Pack in Organization Content, you can create one or more new control objectives as the starting point to define one or more controls and subcontrols that address the new control objective.

The following graphic shows the basic control objective structure:



Notes: See About Automatic Controls for more details on checks.

- **Control objectives**: State the desired result or purpose to be achieved by implementing control procedures in a particular process. Control objective titles display in the user questionnaire.

  You may have a high-level company policy that specifies:

  "Access to information, information processing facilities, and business processes must be controlled on the basis of business and security requirements. Access control rules must take account of control objectives and controls for information dissemination and authorization."

  In that case, you might specify the following control objective:

  "To ensure authorized user access and to prevent unauthorized access to information systems."

- **Controls:** Address an aspect of the control objective. Under any existing control objective in the Organization Content hierarchy, you can create one or more new controls, each of which specifies an action or process. The control title is the section title of user questionnaires.

  For example, suppose you have the following control objective:

  User Access - "To ensure authorized user access and to prevent unauthorized access to information systems."

  One of several controls you may put in place to support this objective might be to implement a user registration control. A statement of that control could be the following:

  "There must be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services."

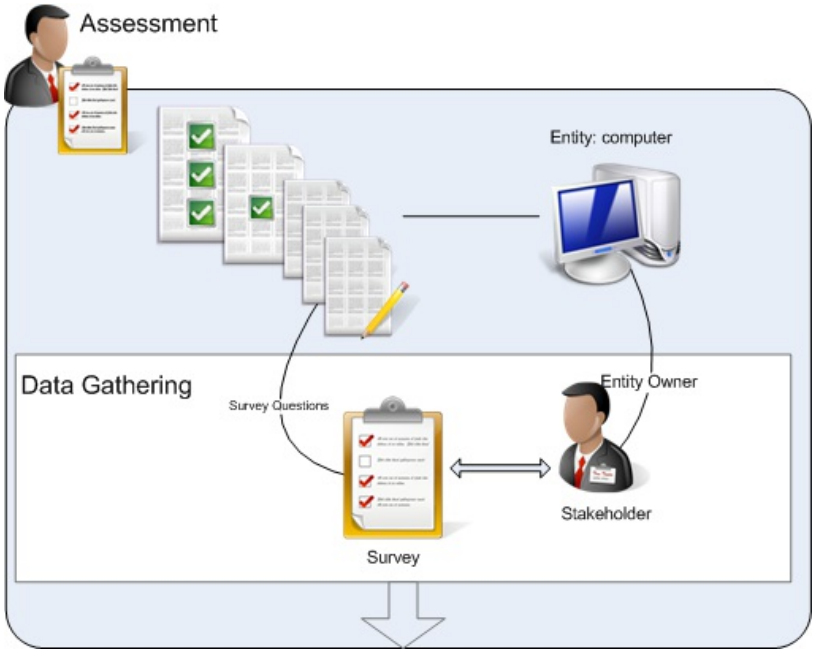
- **Subcontrols:** Specify a check or procedure used to enforce or evaluate compliance with the associated control. Under any existing control in the Organization Content hierarchy, you can create one or more subcontrols (either automatic or manual). The subcontrol Question and choices display in the main pane of the user's questionnaires.

  For example, suppose you have the following control:

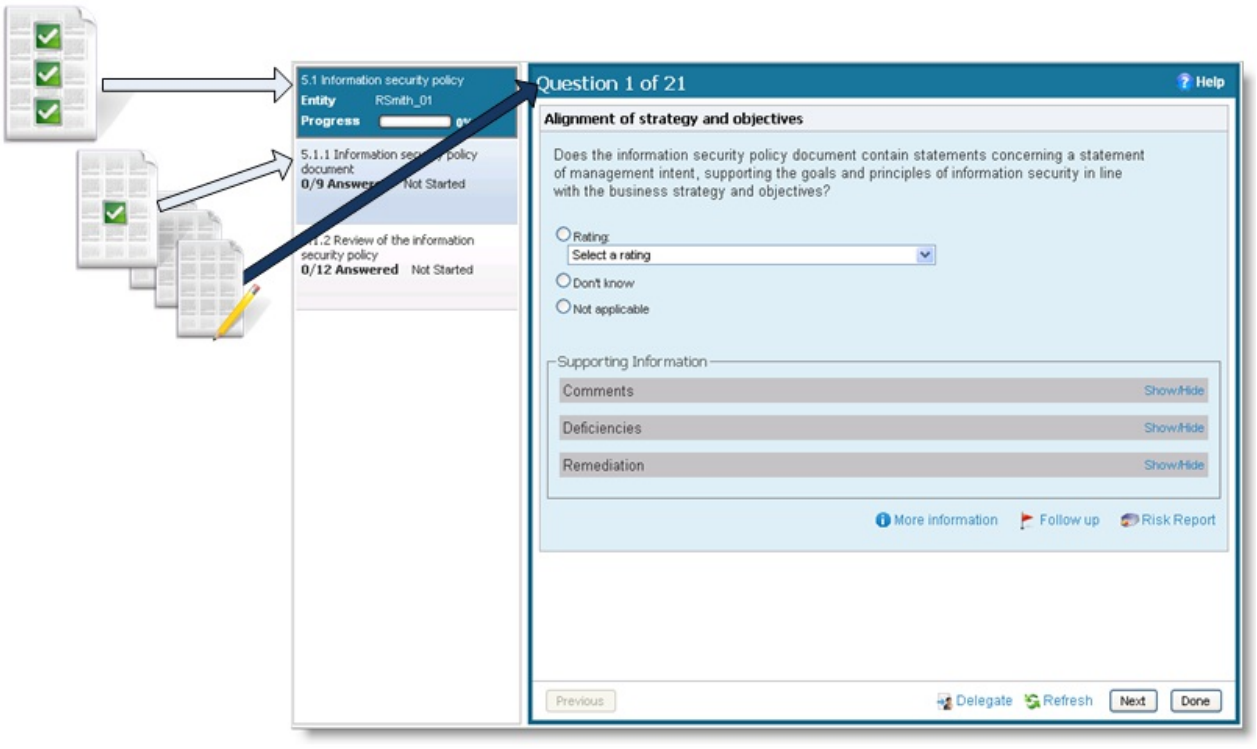
"There must be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services."

One of the subcontrols you may put in place to support or verify compliance with this control might be to actually check if there is a process in place and possibly test the process to determine how well it works. To implement a subcontrol you can specify automated tests of a control or create questionnaire questions that can measure satisfaction of the control and control objectives.

You can assign control objectives or controls to entities in an assessment. If the subcontrol is manual -- that is, if users provide answers to questions -- the questionnaire is assigned to the entity owners identified as stakeholders of the information-gathering stage of the workflow process, as shown below:



The system produces a questionnaire from the object selected in Selecting Controls and Questionnaires, where the highest level is the questionnaire title. The following example shows the questionnaire that is created when the program author selects the ISO-5.1 Control Objective and assigns it to an entity:



If the program author selected ISO-5.1.1 only, then the questionnaire title would be 5.1.1 Information security policy and the questionnaire would only contain the questions from the 5.1.1 subcontrols.

About Controls and Questionnaires

One of the key benefits of the RiskVision solution is the very simple way in which you can organize and assign entire groups of controls (both automated and manual questionnaire checks) to entities as part of assessments. The RiskVision solution then takes care of automatically distributing the controls in a way that ensures you can enforce or verify compliance with designated controls, measure and calculate overall risk and compliance, and respond with different measures to track, mitigate, or remediate control violations or failures. With automated controls, results for controls are checked by whatever various connectors are available for your system. For manual controls (that are verified or evaluated by responses to individual questionnaire questions), the questionnaires are automatically distributed to entity stakeholders and the questionnaire answers and completion results are returned to the RiskVision solution

To help in your effort in choosing the controls that you want your organization to adopt in the first place, Resolver provides an extensive out-of-the-box control library, from which you can choose the most common frameworks, regulations, best practices, and standards-based controls to use in your own environment. (The RiskVision Content Library provides literally thousands of control objectives, automated and manual controls, and control checks to monitor and verify compliance with the regulations and standards most widely in use today.)

Understanding Controls and Questionnaires

Before jumping into the creation or customization of your own Organization's policy and control framework, it is important to have a basic understanding of terminology as well as the basic elements or components needed to build a policy and control "framework".

- **Policy and Control Framework or Group Hierarchy.** At the highest level in the policy, the hierarchy is the organization's policy or control "framework" or grouping hierarchy that groups high-level policies and control objectives. The grouping of control objectives can be based on or include the "domains" or broad categorization provided by standards-based frameworks such as CobiT, ISO 17799, PCI-DSS, NIST SP 800-53 or SP 800-66. For example, ISO 17799 has domains or categories that include such areas as security policy, system access control, computer and operations management, physical and environmental security, personnel security, entity classification, and control.

  The grouping hierarchy can also be of an organization's own design, such as defining a hierarchy of control objectives based on location, organizational structure, or stage of deployment. Or, you can combine both the hierarchy grouping reflecting the needs of your organization as well as take into account those of standards-based frameworks you wish to implement.

- **Content Packs.** Contains a group of control objectives, controls, and subcontrols, Questionnaires and topics, or Policy Documents for your organization that you want to develop using the same process and timeline.

- **Control Objectives.** Within the broader categories of a policy and control framework, policy and control objectives are statements that specify the objectives for developing and implementing controls (control checks or test procedures) that enforce, check, or verify compliance with higher level management goals and objectives. So, the control objective states the desired result or purpose to be achieved by implementing control procedures in a particular process. For, example, ISO 17799 specifies an Access Control domain to satisfy the high-level business requirement or policy to properly control access to information in an organization. So, the control objective, in this case, is that access to information, information processing facilities, and business processes must be controlled on the basis of business and security requirements. Access control rules must take account of policies and control objectives for information dissemination and authorization.

- **Controls**. The terms "Policy" and "Control" are often misunderstood. That is, they may be interpreted or have a different meaning to people from different backgrounds such as security, IT, regulatory compliance and auditing. In Resolver RiskVision, the terms "policy" or "control" means specific rules of behavior that can be enforced or verified either through automatically executed subcontrol checks and tests or responses to questionnaire questions distributed to business and technical owners, administrators, or other stakeholders for the relevant entities.

  For example, in the RiskVision Content Library hierarchy, under the ISO Section 11 "User Access Management" control objective, Resolver provides four unique controls, for user registration, privilege management, user password management, and review of user access rights. For each control, there can be many subcontrols that can be used to check conformance or compliance with the associated control.

- **Subcontrols.** For each Resolver control, users can define one or more sub-control checks implemented using automatically-run test procedures or manual control (questionnaire) questions. (For manual controls, questionnaire questions are distributed to the business owner or other parties (stakeholders) responsible for the associated entity(s).

  For example, in the RiskVision Content Library > Policies and Controls > Standards > ISO 17799 > 11 - Access Control > User Access Management hierarchy displayed in the RiskVision solution, the User Password Management control includes a half dozen or so manual control checks that enforce or verify compliance with the user password management control policy objectives.

- **Control Target Profiles**. Named collections of attribute values that define some group of entities as being similar for the purpose of choosing controls to evaluate and retrieve control results, since the entities matching the same profile have similar characteristics.

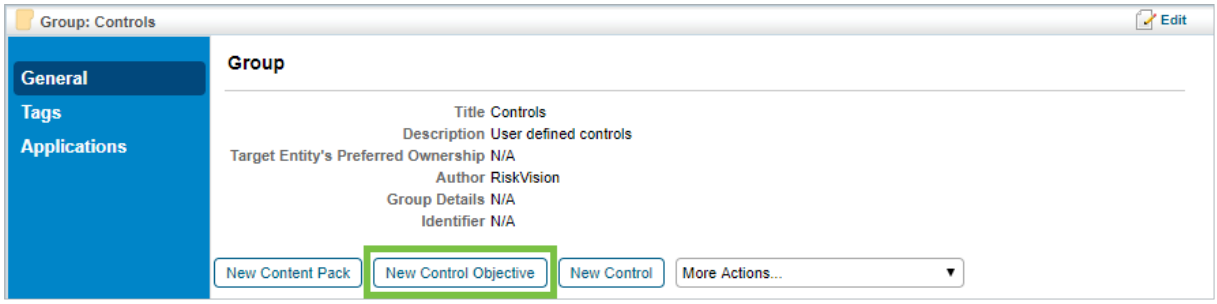
Control Objectives

Under any defined group or subgroup in **Organization Content**, you can create one or more new control objectives as the starting point to define one or more policy controls and subcontrols that address the new control objective. To create a control objective, you must have Control View and Control Author permissions.

To modify an existing control objective, click **Edit**.

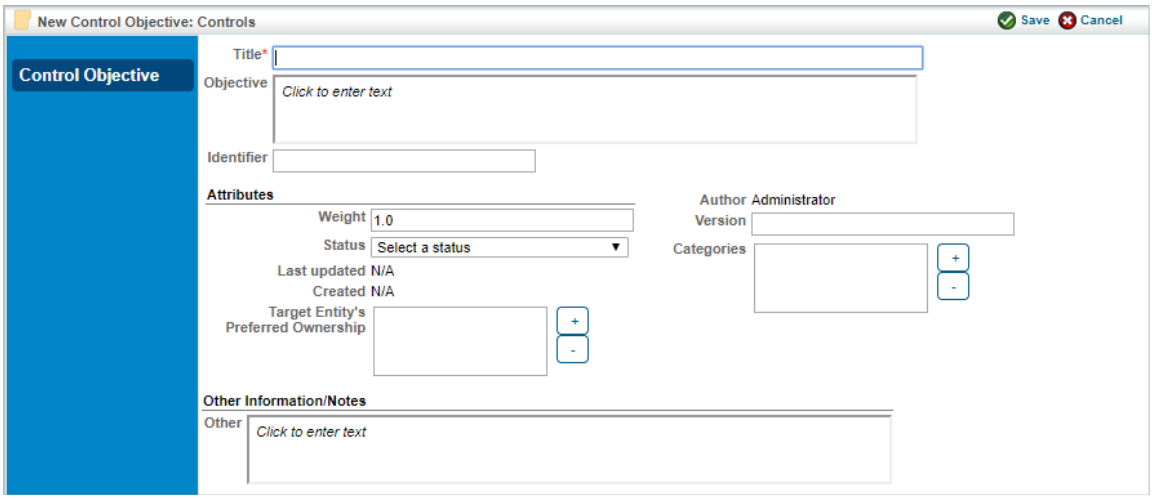
To create a control objective:

1. Go to **Content Risks** > **Controls and Questionnaires**.
2. Expand **Organization Content** and select a group.
3. **Optional**: Structure your content in a new root folder by creating a new group.
4. Click **New Control Objective**.



The General tab.

5. Enter the following fields:
    - **Title**: The label that identifies the control objective.
    - **Objective**: Specifies the purpose of supporting controls that enforce, check, or verify risk measurement and compliance with organization policies and goals.
    - **Identifier**: Enter an optional identifier for the new control
    - **Weight**: Indicates the weight assigned to this control objective when paired with others in an assessment. When compliance and risk scores are rolled up, values are calculated based on the percentage this control object's weight contributes to the total weight of objectives at the same level in a hierarchy.
    - **Status**: Lets you specify the stage of associated control development or completion. Later on, you can use this information to identify and track progress in various stages of completion.
    - **Version**: Enter the new control objective's version in any consistent format.
    - **Categories**: Assign a category to the control objective.
    - **Target Entity's Preferred Ownership**: Choose users, teams, and roles to be preferred owners of the new control objective.
    - **Other Information/Notes**: Enter additional information about the control objective.



The Create Control Objective screen.

6. Click **Save**.

Configuring Controls

Under any existing control objective in the Organization Content hierarchy, you can create one or more new controls, each of which specifies an action or process that will address the control objective.

To modify an existing control, clickEdit.

To create a control, see Creating a New Control.

In addition to entries on the General tab, you can optionally click on the Guidance and Risks tab to specify guidance information on how to check the control plus add risks that this control is meant to address.

Configuring Subcontrols

One of the subcontrols you may put in place to support or verify compliance with this control is to actually check if there is a process in place and possibly test the process to determine how well it works. To implement a subcontrol, you can specify automated tests of a control or create questionnaire questions that can measure satisfaction of the control and control objectives. In order to create a new subcontrol, you must have the Control View and Control Author permissions.

To create a new subcontrol:

1. In the RiskVision, go to **Content** > **Controls and Questionnaires**.
2. Expand **Organization Content** and select a control.
3. Click **New Subcontrol**. The **Create Subcontrol** wizard appears, showing the **Subcontrol Details** wizard page.
4. On the Create Subcontrol tab, complete the information as follows:
    - **Title.** The Title is the label that will be displayed for the control in the Organization Content hierarchy.
    - **Question text.** The Question text that displays in the user questionnaire.
    - **Description.** The Description provides an overview description of the subcontrol entered in WYSIWYG rich HTML format.
    - **Weight.** The Weight value indicates the weight assigned to this control. When compliance and risk scores are rolled up, values are calculated based on the percentage the control's weight contributes to the total weight of controls at the same level in a hierarchy.
    - **Reference Numbers.** The Reference Numbers field lets you specify information corresponding to related control framework or regulation reference numbers like ISO-17799 1.4.1 for example. To enter multiple reference numbers, you can include the reference numbers in a comma-separated list.
    - **Help text.** The help text for this question that displays in the user questionnaire.
    - **Assessment Procedures.** The procedural text for this question.
    - The Key Control field indicates whether this subcontrol must be included when a user selects control options only to implement or use key controls in measuring risk and policy compliance. In contrast to primary controls, where a user would generally pick one control to rely on for results, users can generally pick multiple key controls.
5. The **Responses** wizard page appears. In the **Responses** wizard page, set up the answers available to the user in the questionnaire.

   When you skip this step, the default answers are applied. See Default Question Settings.
6. The **Dependencies** wizard page appears. In the **Dependencies** wizard page, select subcontrols that apply when an answer is chosen.
7. Click **Finish**. Additional detail tabs specific to the subcontrol type appear.

Create a New Control

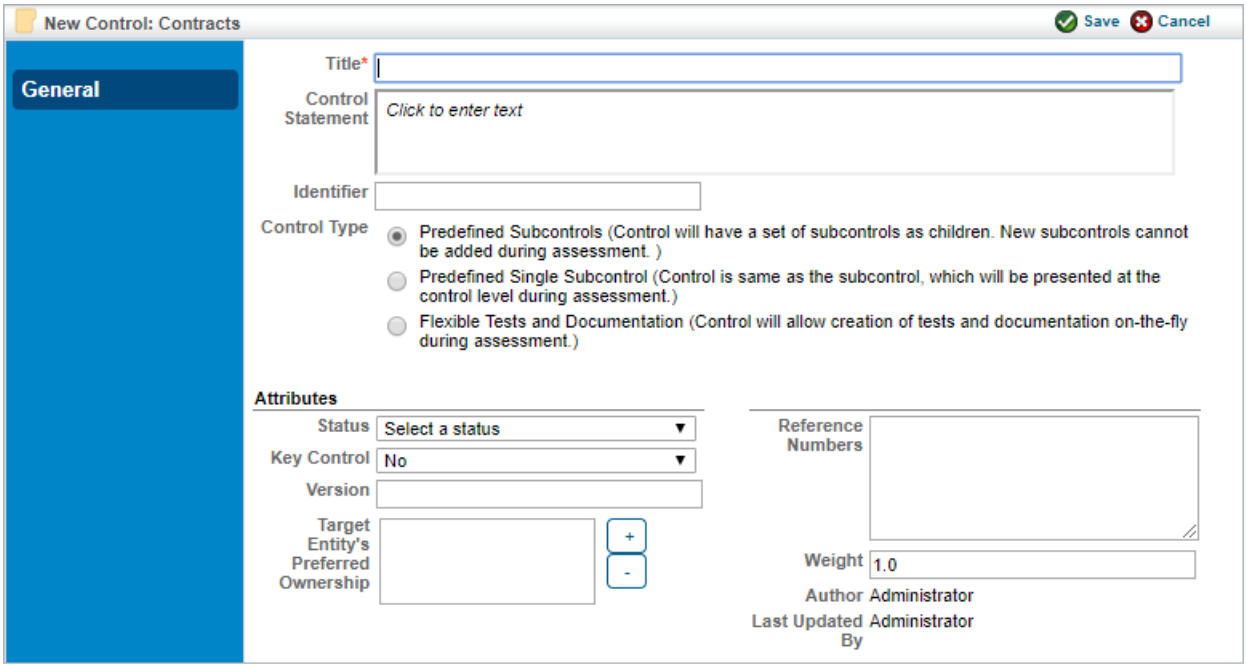
Creating a new control requires Control View and Control Author permissions. There are three types of controls:

- Control with subcontrols;
- Control with a single subcontrol; and
- Audit-friendly controls.

Control with subcontrols are the most common type of control. The control is a container for specific subcontrols. For example, the control might be "Ensure physical security" and the subcontrols might refer to specific aspects of physical security.

A control with a single subcontrol binds a control to a single subcontrol, creating a control that can act like a subcontrol if necessary. Use this type when a control does not have multiple aspects.

Audit-friendly controls include design and effectiveness tests in order to be self-documenting. For more information, see Using Audit-Friendly Controls.



The Create a New Control screen.

To create a new control:

1. Open RiskVision Compliance Manager.
2. Go to **Content** > **Controls and Questionnaires**.
3. Navigate to a writable control group in the **Organization Content** tree (Control groups in the Content tree, for example, are read-only) and click **New Control**.
4. Choose **Control Type.** Selecting the **Flexible Tests and Documentation** option changes the attributes in the lower part of the screen. For more information about creating that kind of control, see Using Audit-Friendly Controls.
5. Enter the parameters:

Parameter	Description
Title	Enter a name for the new control. This is the only required field.
Control Statement	Enter an optional statement to be associated with the new control. Clicking the field pops up the rich text editor. The control statement specifies the actions or checks that must be provided by supporting subcontrols (automated or manual/questionnaire).

Parameter	Description
Identifier	Enter an optional identifier for the new control.
Status	Select a status, such as Draft, In Testing, Final, or Review. The Status field lets you specify the stage of control development or completion. Later on, you can use this information to identify and track controls in various stages of completion.
Key Control	Choose Yes if this is a key control. The Key Control field indicates whether this control must be included when a user selects control options only to implement or use key controls in measuring risk and policy compliance.
Version	Enter the new control's version in any consistent format.
Target Entity's Preferred Ownership	Choose users, teams, and roles to be preferred owners of the new control.
Reference Numbers	Enter any meaningful reference numbers (for example, referring to specific internal or regulatory standards). This field lets you specify information corresponding to related control framework or regulation reference numbers, for example, ISO-17799 1.4.1. To enter multiple reference numbers, you can include the reference numbers in a comma-separated list.
Weight	Enter a weight for the new control. The default is 1.0. This value indicates the weight (between 0 and 1) assigned to this control. When compliance and risk scores are rolled up, values are calculated based on the percentage this control's weight contributes to the total weight of controls at the same level in a hierarchy.

6. Click **Save** to create the new control, or **Cancel** to return to viewing controls.

Creating Questionnaires

Resolver RiskVision has many default questionnaires available. Before creating a new questionnaire, you can also try editing a default questionnaire.

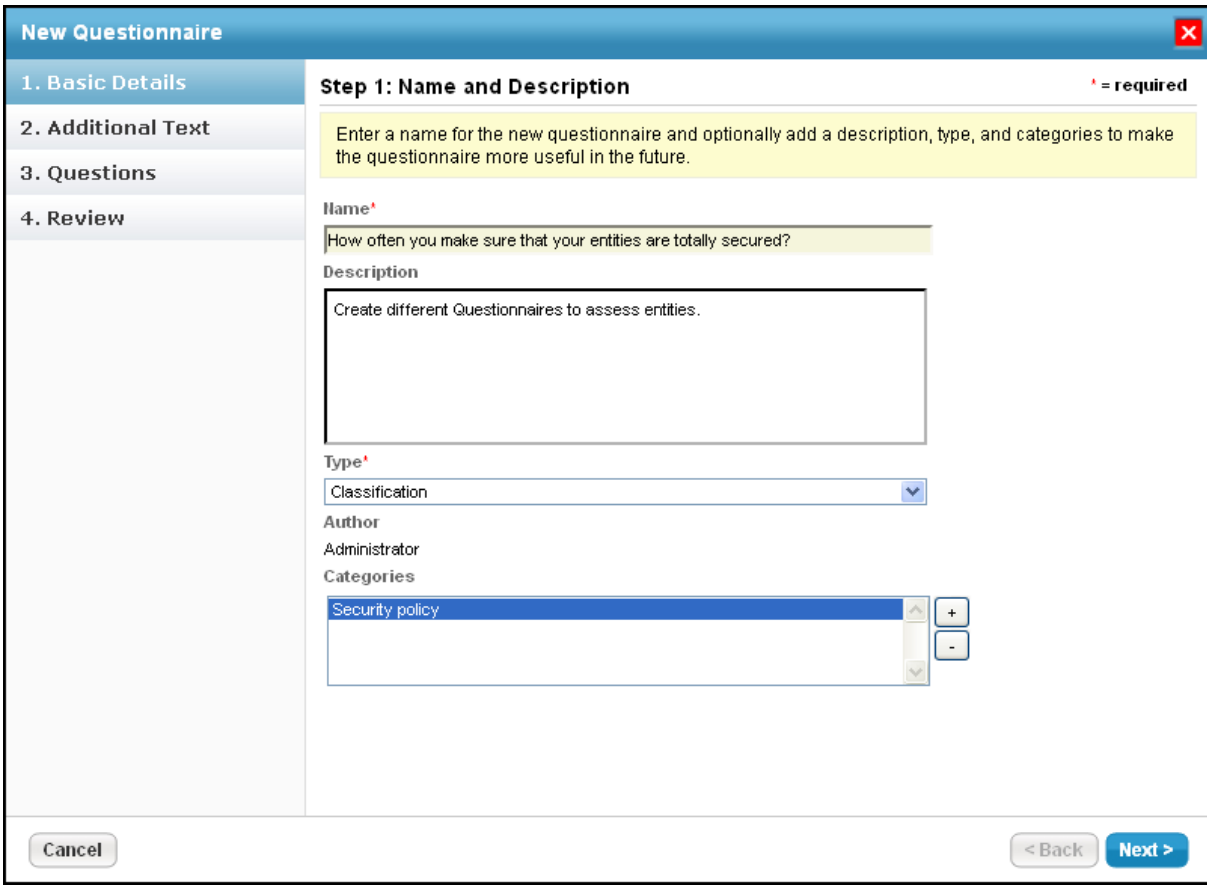
To edit a default questionnaire:

1. Copy the questionnaire.
2. In the **Controls and Questionnaires group**, create a custom-defined group.
3. Modify the questionnaire details.

If you'd prefer to create a questionnaire from scratch, note that you will need Control View and Control Author permissions. It's recommended you test the content thoroughly before deploying the custom questionnaire.

To create a questionnaire

1. Go to **Content** > **Controls and Questionnaires**
2. Expand the **Organization Content** folder.
3. Select the **Questionnaires** group, and click **New Questionnaires.**
4. Enter the name and description in the **New Questionnaire** wizard.
5. Select the questionnaire type in the **Type** drop-down list.



Note: The New Questionnaire wizard displays different pages depending on the questionnaire type.

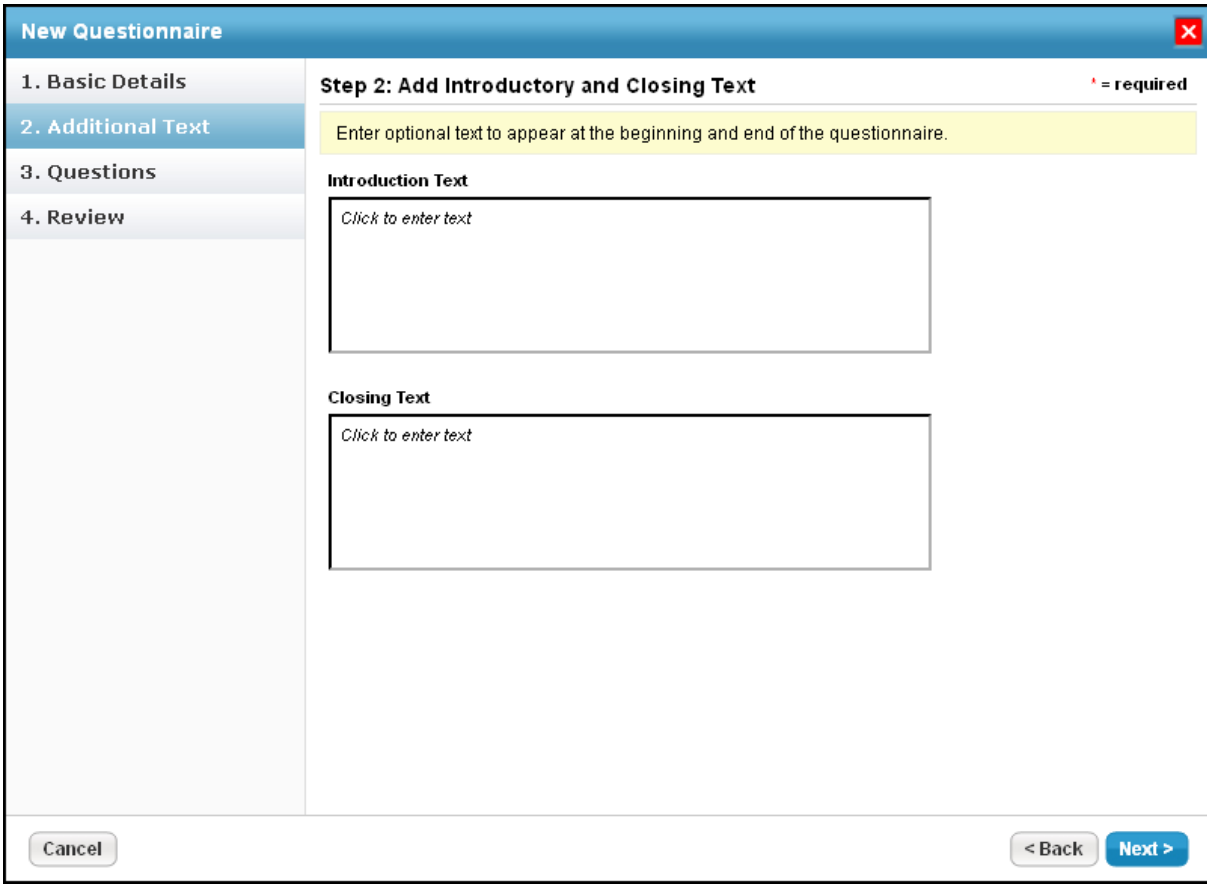
- Contract Awareness Campaign shows Contracts, Text, and Review pages.
- Policy Awareness Campaign shows Policies, Text, and Review pages.

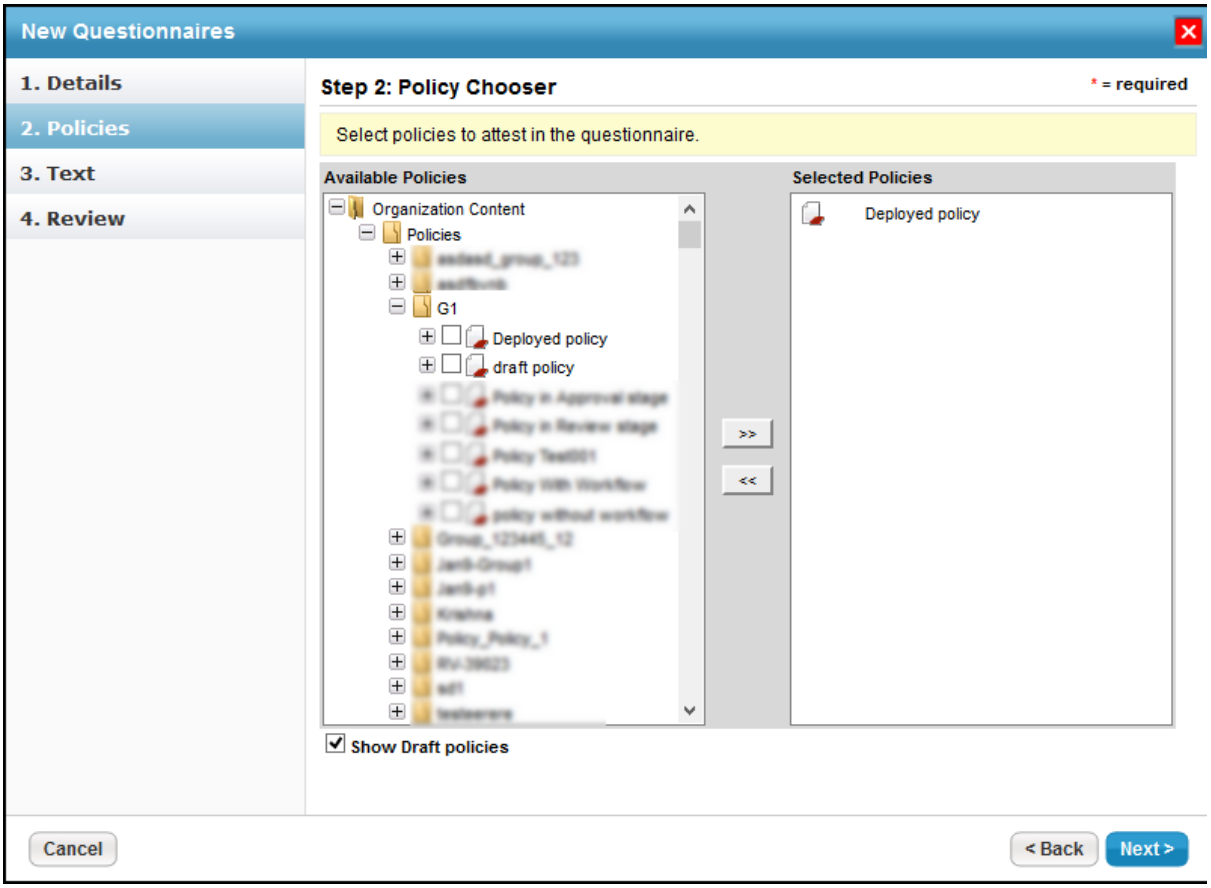
To assign a category to the questionnaire:

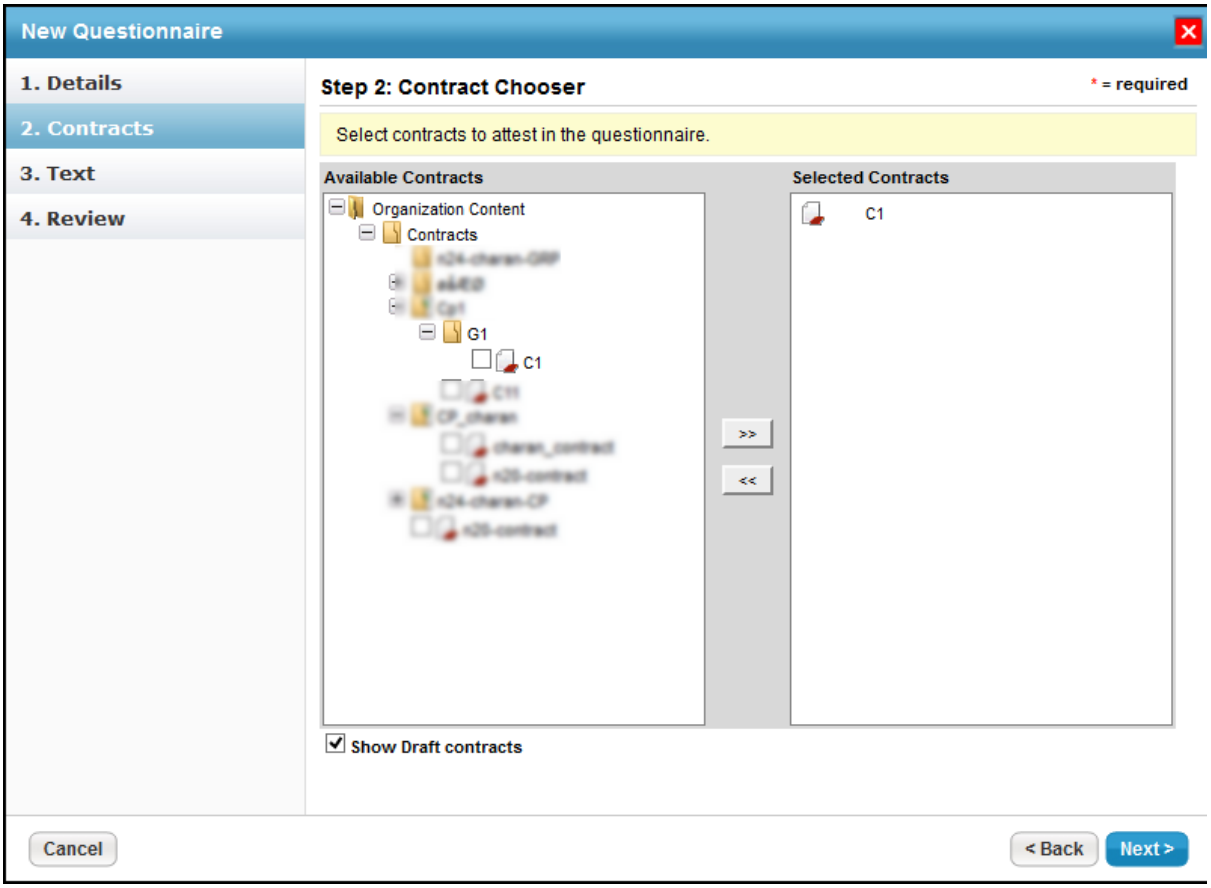
- Click the + next to the scroll box to open the **Select one or more Categories** dialog.
- Under the **Categories** folder, select different categories and click **OK**. If default categories don't apply to the questionnaire you're trying to create, enter a category name, and click **Add**.
- Select the category under the **Categories** folder.

Click **Next** to continue.

7. In the **Additional Text** wizard, enter text in the **Introduction Text** and **Closing Text** fields. These will appear at the beginning and end of the questionnaire, respectively.
8. Click **OK** to save.
9. The **Policies** wizard page will open.
10. Expand the **Organization Content** folder and select the policies you want to attest.
11. Click **>>** to move the policies into the Selected Policies box.
12. The **Contracts** wizard page will open.
13. Expand the **Organization Content** folder and select the desired contracts.
14. Click **>>** to move the contracts into the **Selected Contracts** box.
15.


New Questionnaire
1. Basic Details
2. Additional Text
3. Questions
4. Review
Step 2: Add Introductory and Closing Text
* = required
Enter optional text to appear at the beginning and end of the questionnaire.
Introduction Text
Click to enter text
Closing Text
Click to enter text
Cancel
< Back
Next >


New Questionnaires
1. Details
2. Policies
3. Text
4. Review
Step 2: Policy Chooser
* = required
Select policies to attest in the questionnaire.
Available Policies
Selected Policies
Organization Content
Policies
G1
Deployed policy
draft policy
Deployed policy
>>
<<
Show Draft policies
Cancel
< Back
Next >



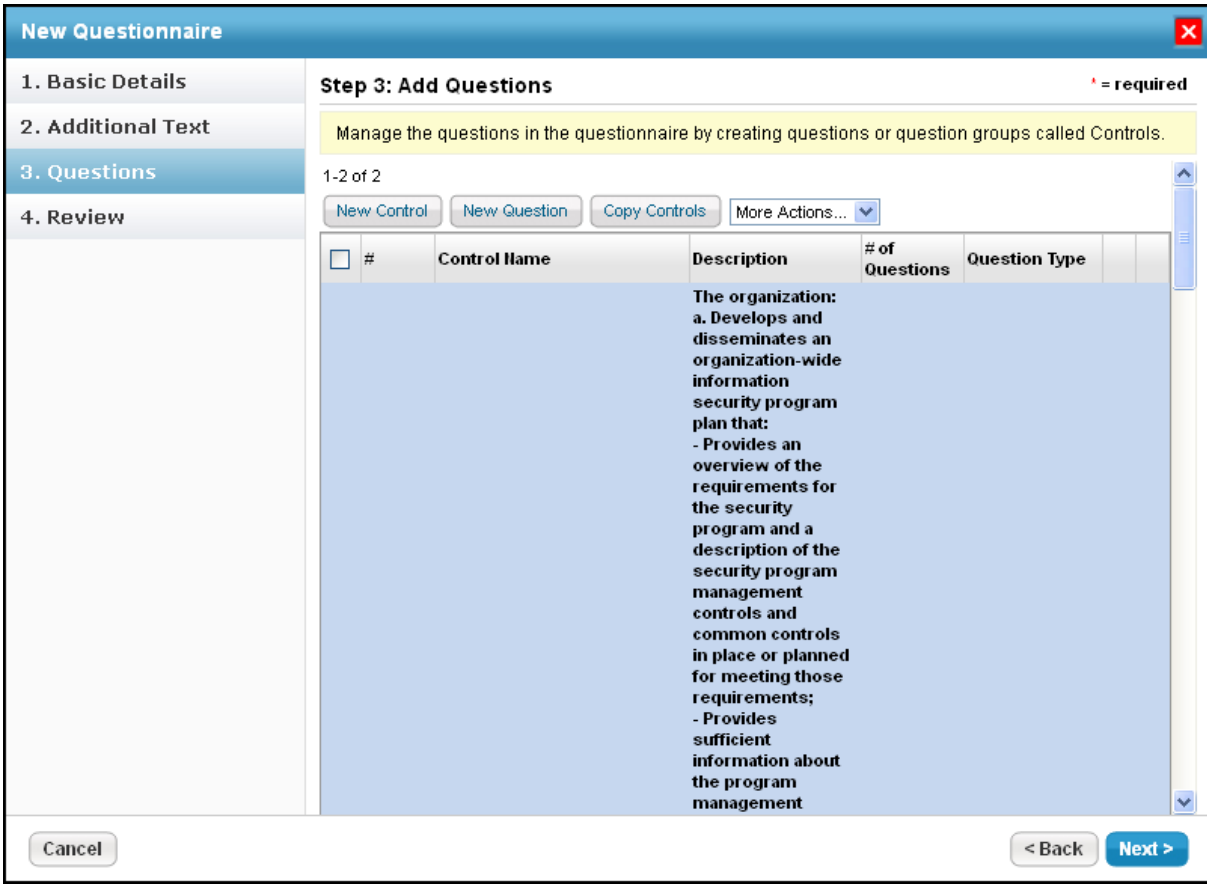
Click **Next** to continue.

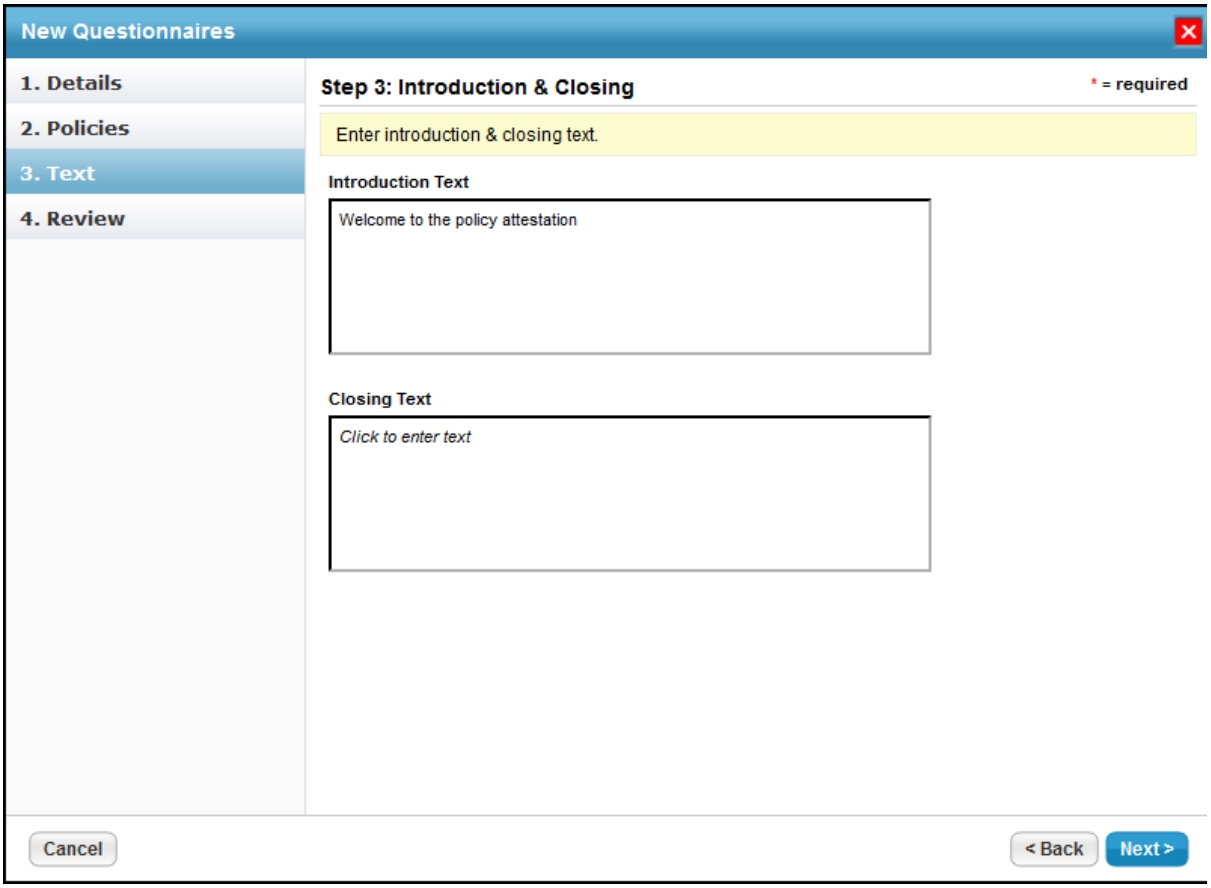
16. The **Questions** wizard page will open.

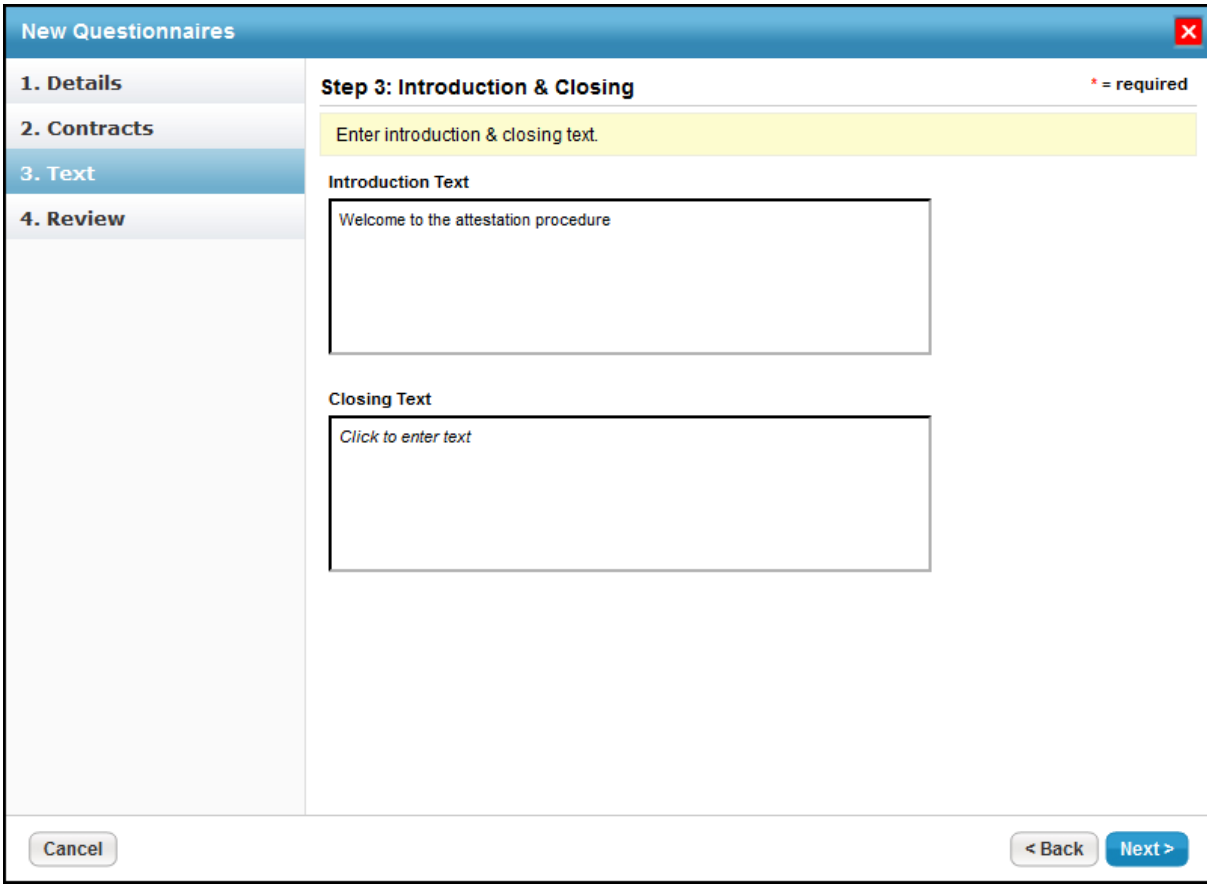
17. To create a new control, see Creating a New Control. To copy controls, expand the **Controls** folder to find the control you want to copy, check the box next to control, and click **OK**.

18. The **Text** wizard page will open.

19. Enter introduction and closing text and click **OK** to save changes.


New Questionnaire
1. Basic Details
2. Additional Text
3. Questions
4. Review
Step 3: Add Questions
* = required
Manage the questions in the questionnaire by creating questions or question groups called Controls.
1-2 of 2
New Control
New Question
Copy Controls
More Actions...
# of Questions
Question Type
The organization:
a. Develops and disseminates an organization-wide information security program plan that:
- Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
- Provides sufficient information about the program management
Cancel
< Back
Next >


New Questionnaires
1. Details
2. Policies
3. Text
4. Review
Step 3: Introduction & Closing
* = required
Enter introduction & closing text.
Introduction Text
Welcome to the policy attestation
Closing Text
Click to enter text
Cancel
< Back
Next >

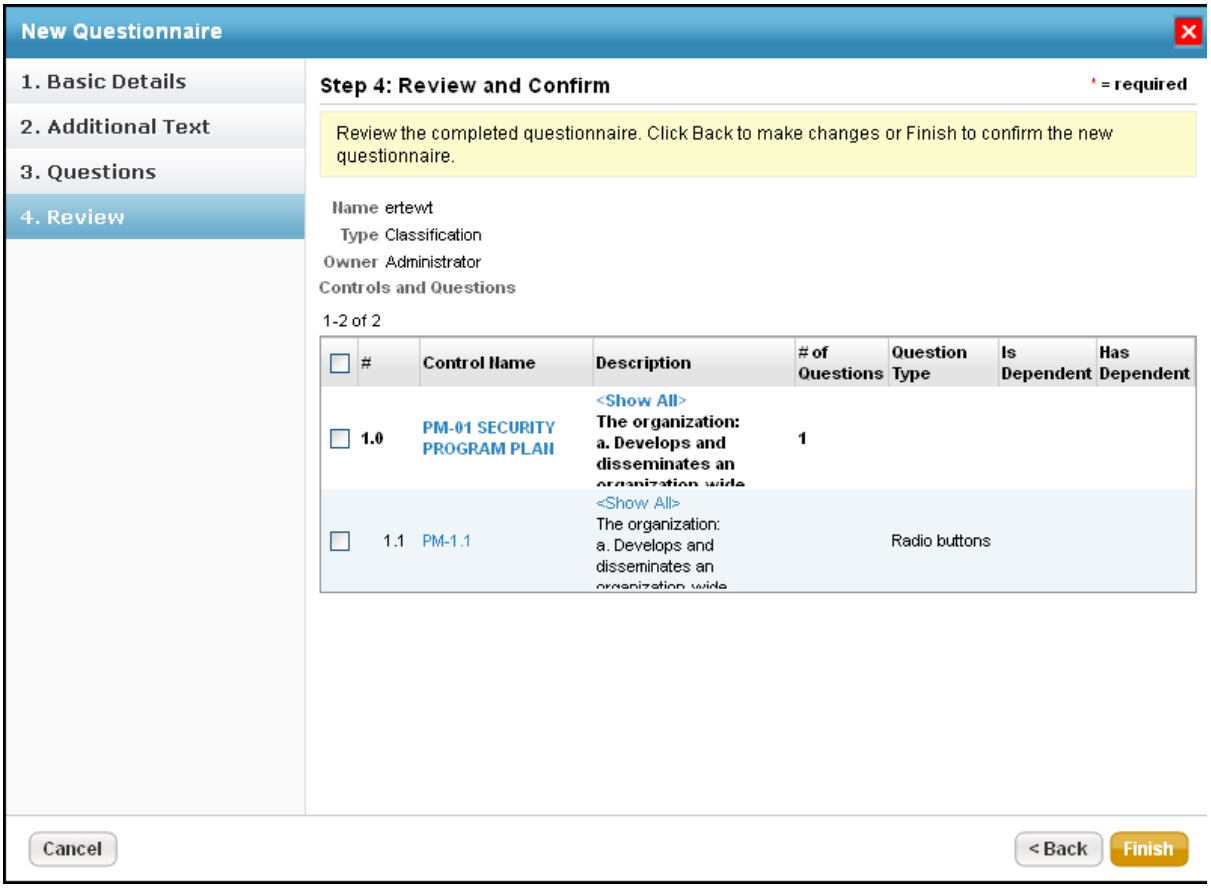


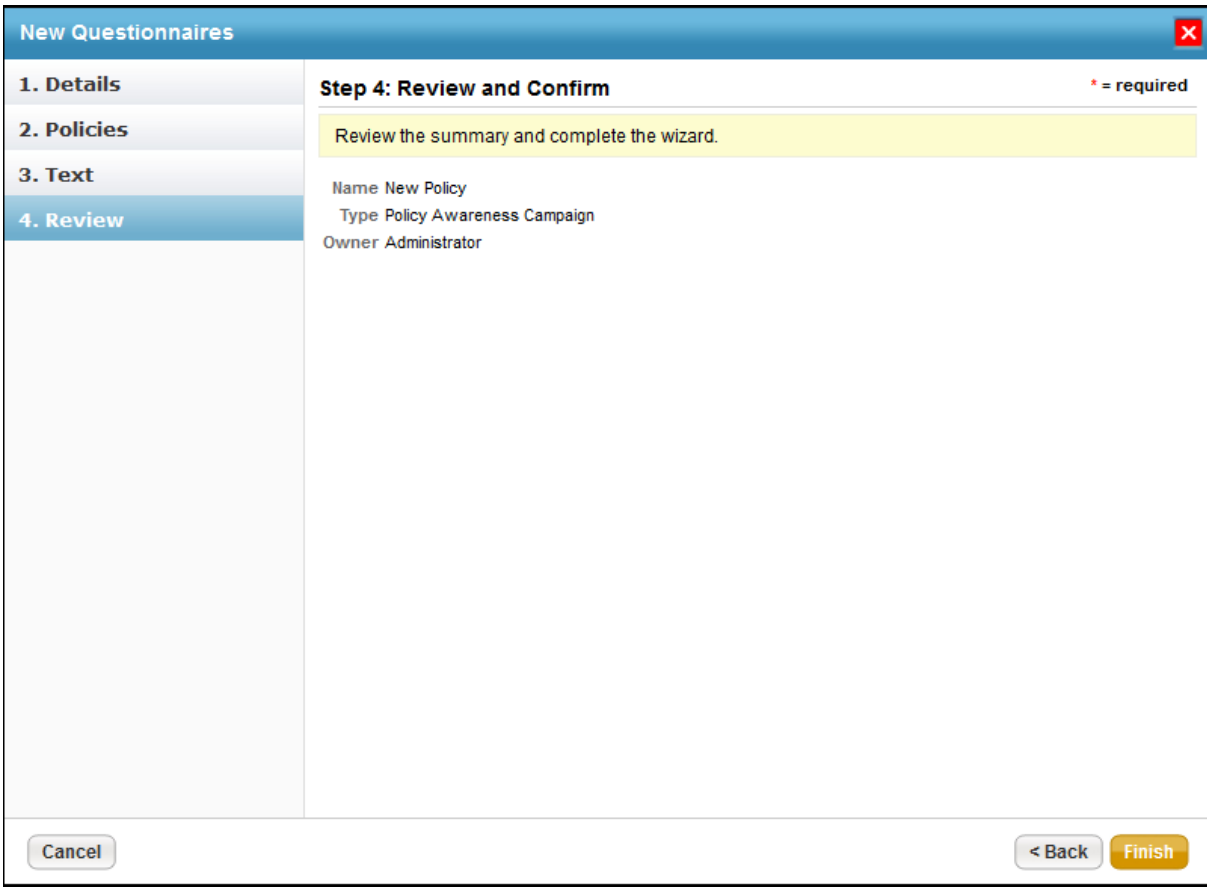
Click **Next** to continue.

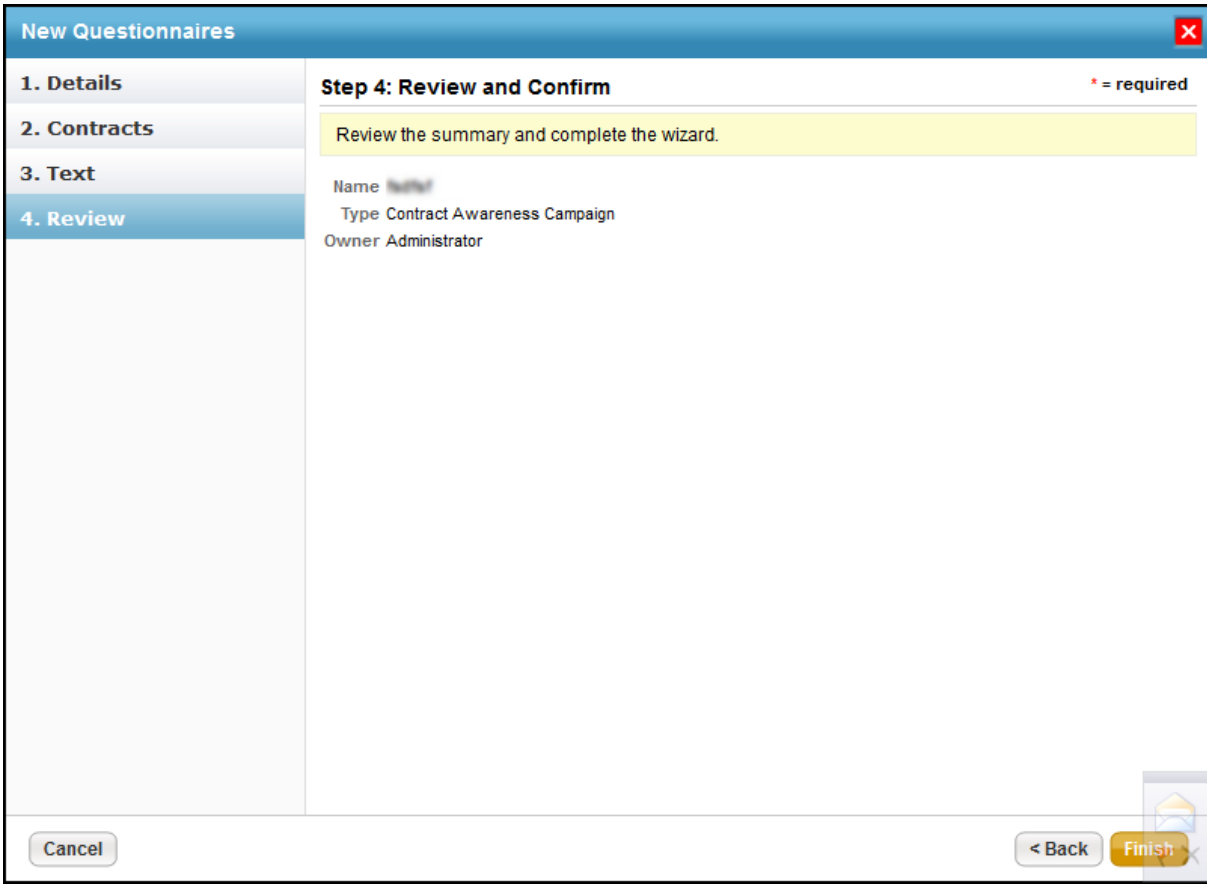
20. The **Review** wizard page will open. Verify the controls and the number of questions for each control.

21. Click **Finish** to create the questionnaire.

22. Review the summary and click **Back** to navigate to previous wizard pages if changes need to be made. Click **Finish** when the information you have entered is correct. The questionnaire is created.


New Questionnaire
1. Basic Details
2. Additional Text
3. Questions
4. Review
Step 4: Review and Confirm
* = required
Review the completed questionnaire. Click Back to make changes or Finish to confirm the new questionnaire.
Name ertewt
Type Classification
Owner Administrator
Controls and Questions
1-2 of 2
Control Name Description # of Questions Question Type Is Dependent Has Dependent
1.0 PM-01 SECURITY PROGRAM PLAN <Show All> The organization: a. Develops and disseminates an 1
1.1 PM-1.1 <Show All> The organization: a. Develops and disseminates an Radio buttons
Cancel
< Back
Finish


New Questionnaires
1. Details
2. Policies
3. Text
4. Review
Step 4: Review and Confirm
* = required
Review the summary and complete the wizard.
Name New Policy
Type Policy Awareness Campaign
Owner Administrator
Cancel
< Back
Finish



To enable Add Risk if Unselected:

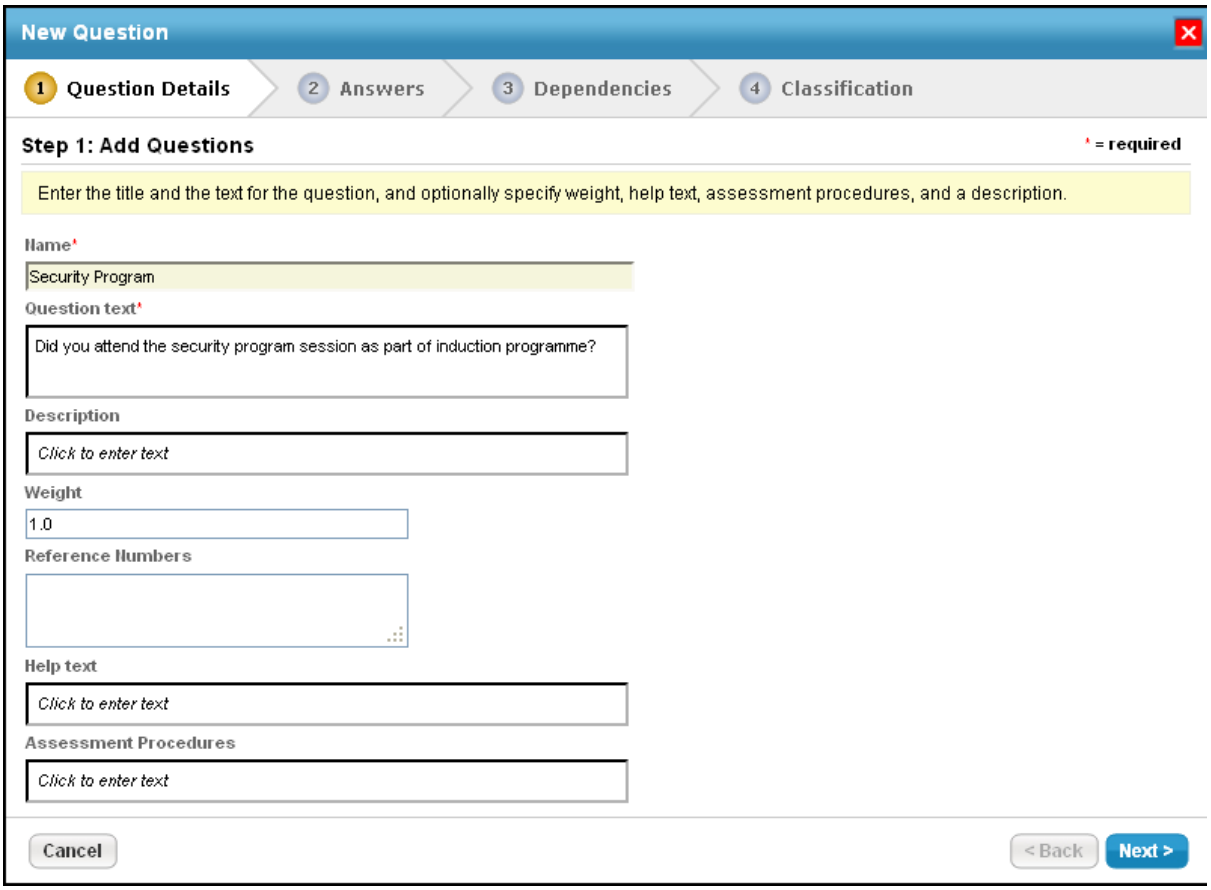
1. Open the *agiliance.properties* file. It is located by default in the *||server|config* directory.
2. The property is false by default. Change the following tags to **true**:
   `com.agiliance.risk.addToRiskWhenUnchecked.flag.show=false`
   `com.agiliance.risk.useClassificationSurveyRisk=false`

Creating New Questions

Create a new question on the fly while creating a new questionnaire, or after a questionnaire is created. In both scenarios, you must first ensure that controls are present in the questionnaire. Creating a new question requires Control View and Control Author permissions.

To create a new question:

1. Open the **New Question** wizard using one of the following methods:
   - ContentRisks > **Controls and QuestionnairesQuestionnaires**, expand the Organization Content group under the **Controls & Questionnaires** group, and select the **Questionnaires** group to open its details. Select the questionnaire or content pack to open its details, select a control, and click **New Question**.
   - On the **Questions** tab of the **New Questionnaire** wizard, select a control and click **New Question**.
2. Enter a name and text for the question. Optionally, enter the description, weight, reference numbers, help text, and assessment procedures.



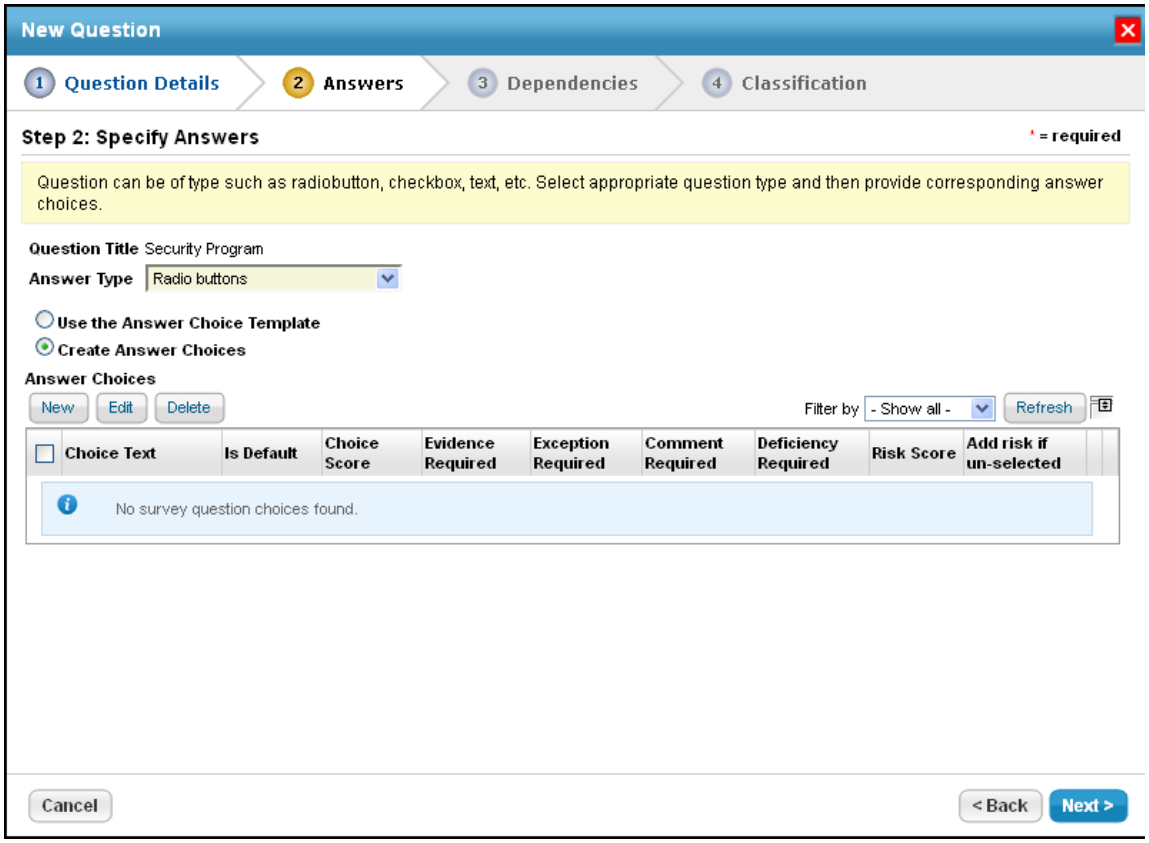
Click **Next** to continue.

3. The **Answers** wizard page appears. Select the type of answer that you want to make available for stakeholders to answer the question. You can select radio button, text box, check box, table, time series and date.

Answer Type: Table When the

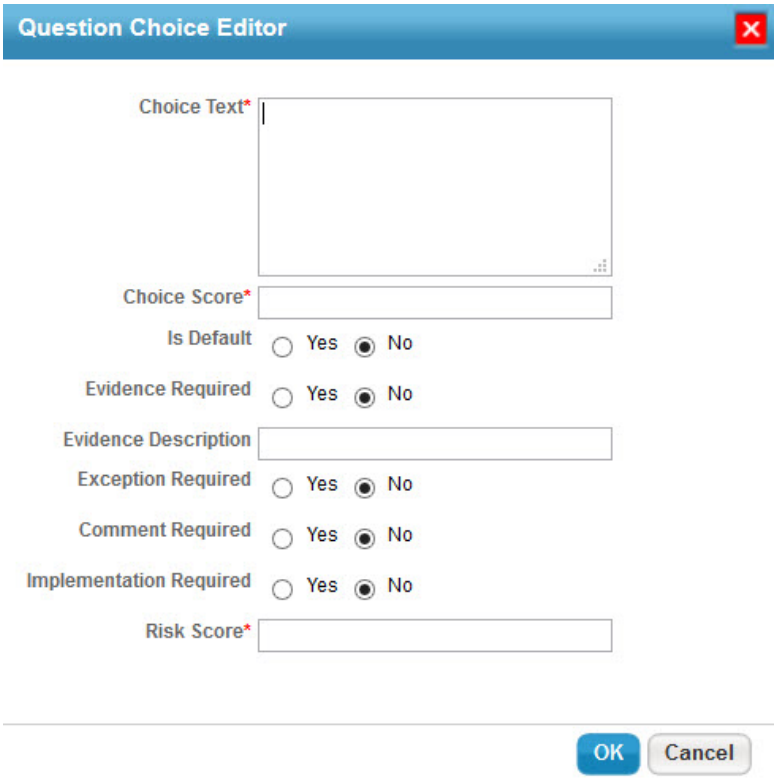
- When **Answer Type** is selected as **Radio buttons**, **Check boxes** or **Table**.

The wizard prompts you to select the **Use the Answer Choice Template**or **Create Answer Choice**option.



- If the **Use the Answer Choice Template** option is selected, a drop-down list containing default templates appear. Select one of the template to see the answer choices. If you want to create a new template, perform the following steps:
    - Click + next to the drop-down list to prompt the **New Choice Template** dialog.
    - Enter a title and description for the new template. Under the **Answer Choices** section, click **New** to prompt the **New Answer Choice** dialog and enter the details as described in step II (a). Click **OK** in the **New Choice Template** dialog and ensure that the new template is selected in the drop-down list.

1. If the **Create Answer Choices** option is selected, perform the following steps:



- Click **New** to bring on the **Question Choice Editor** dialog and enter the details as follows:
  - **Choice Text. Enter choice text for the question. For example, enter "Yes' as one of answers the question.**
  - Choice Score. Enter a positive numeric value between 0 and 10.
  - Is Default. Select to show the default answer choice.
  - Evidence Required. Select '**Yes**' if you want the stakeholders to attach evidence for the answer choice.
  - Evidence Description. Enter description for the evidence.
  - Exception Required. Select '**Yes**' if you want the stakeholders to create an exception for the answer choice.
  - Comment Required. Select '**Yes**' if you want the stakeholders to add a comment for the answer choice.
  - Implementation Required. Select '**Yes**' if you want stakeholders to enter deficiency for the answer choice.
  - Risk Score. Enter a positive numeric value between 0 and 10.
- Click **OK** to add the answer choice.

Answer Type is selected as **Table**, the questionnaire is in the tabular format. In the **Table Configure** section, users can configure the table format.

Click the **Add Columns** icon and **Add Row** icon, under the **Table Configure** section to add the required number of columns and rows required in designing the tabular format questionnaire. Enter the required Column Name and Row Name to be displayed on the table when answering the questionnaire.

- When answer type is selected as the Text box.

  The wizard will not require you to add answer choices.

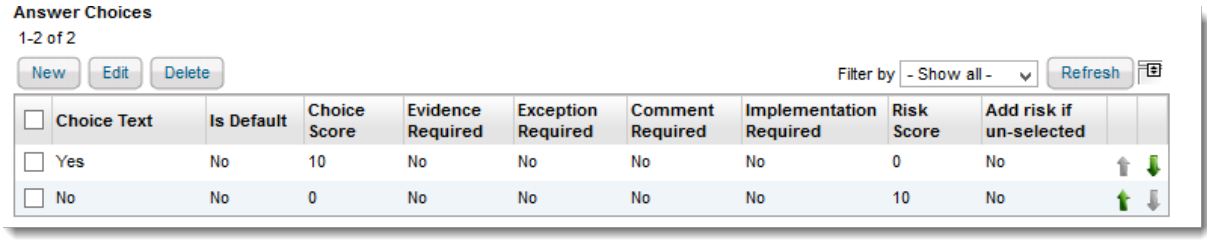
- When answer type is selected as Time Series.

  The wizard will require you to select the Collection Frequency **Formats, and units of metric**.

- When answer type is selected as Date.

  The wizard will not require you to add answer choices.

4. After the answer choices are added, the choices appear in the **Answer Choices** section. The answer choices appear in the **Questionnaire** window the order they appear in the **Answer Choices** section. To change the order, click the upward or downward arrow in the answer choice row.

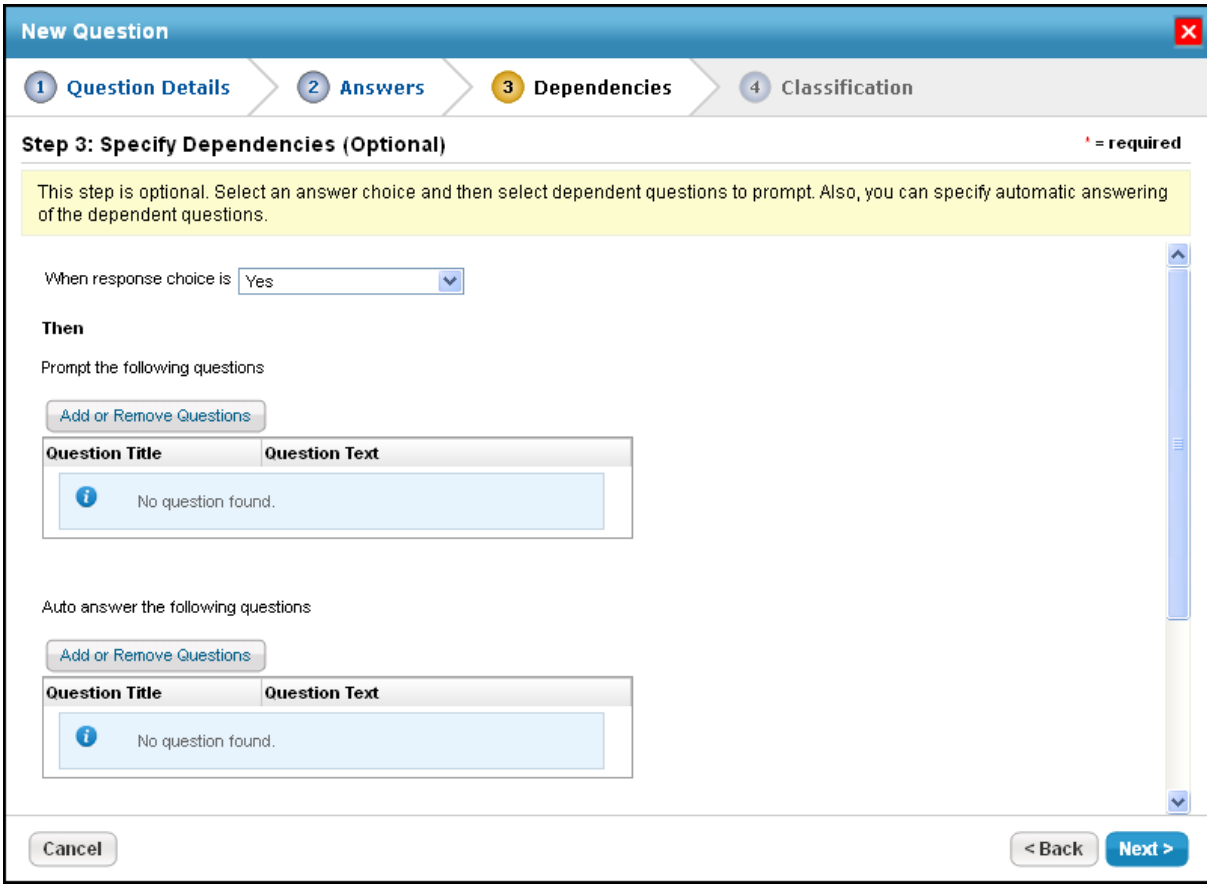


Click **Next** to continue.

Renaming choice text will not clear the answer choices of a question in target questionnaires. If you have to rename the choice text, delete the choice text you would like to change first, and then create new choice text to replace the deleted choice text.

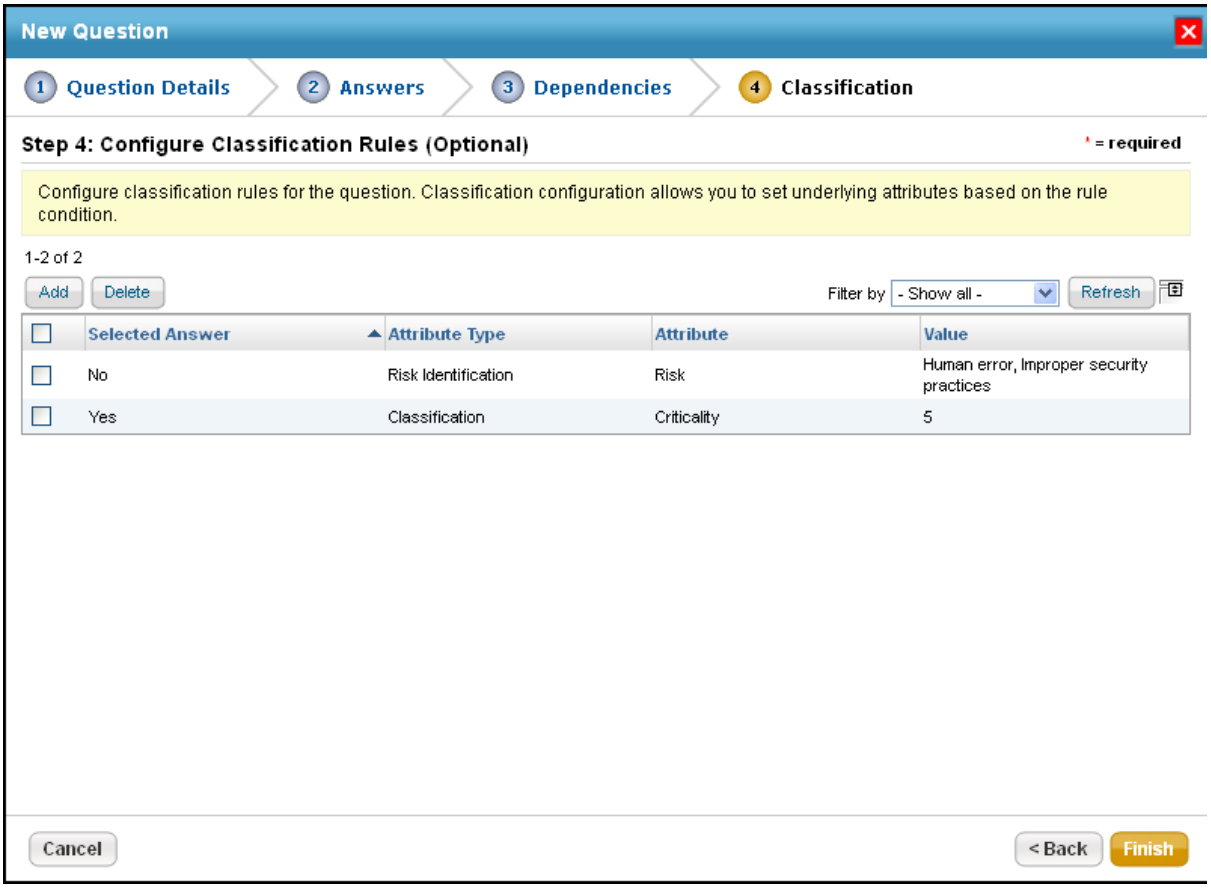
5. The **Dependencies** wizard page appears. This step is optional. You can add dependent questions only for **Radio buttons** and **Checkboxes** answer type. Use the answer choices you created in the **Answers** wizard page to further prompt stakeholders to answer more questions or add questions so that questions are answered automatically if a particular answer choice is selected.

   To add questions to be prompted or to be answered automatically, click **Add or Remove Questions** to open the **Must Answer Questions** dialog. Select questions in the **Available Questions** box and click the arrow pointing towards the right to move questions to the **Selected Questions** box. Then click **OK**.



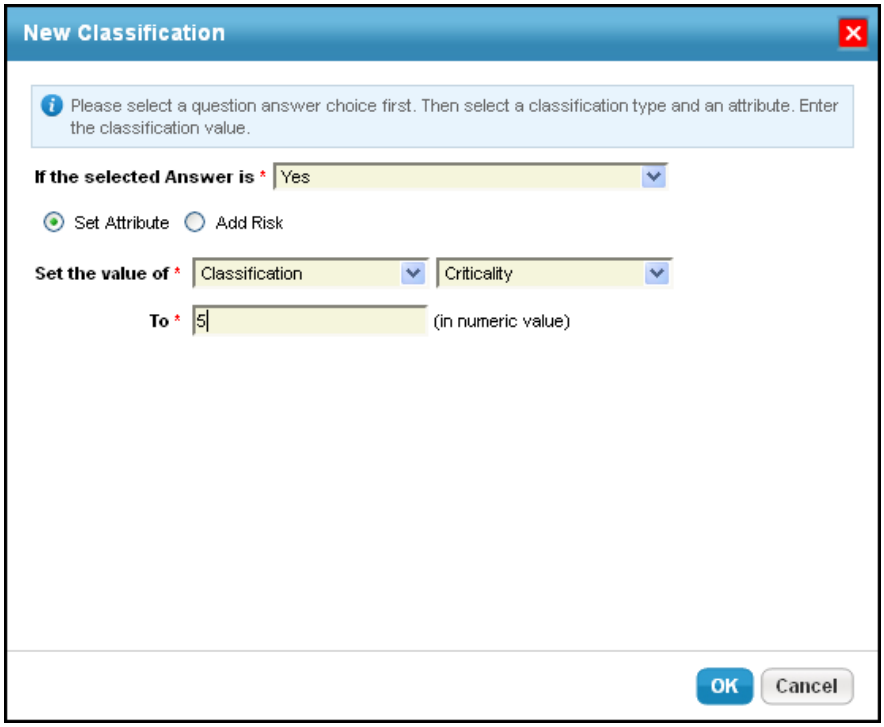
Click **Next** to continue.

- The **Classification** wizard page appears. This step is optional.



You can configure a classification rule only when answer type is **Radio buttons**, **Textbox, Table**, or **Checkboxes**. Click **Add** to bring on the **New Classification** dialog box. Select the answer choice in the If the selected Answer is a drop-down list and select **Set Attribute** or **Add Risk**.

- If the **Set Attribute** option is selected, select the attribute and its value in the respective drop-down lists, and enter a value in the **To** field.



1. If the **Add Risk** option is selected, click **Add Risk** to bring on the **Select one or more Risks** dialog. Expand the **Risks** folder, select risks, and click **OK**.

- Click **Finish** to add questions to the control and to exit the wizard. Clicking **Finish** will prompt a confirmation box, asking whether you want to add another question. Click **Yes** to add more questions or **No** to exit the confirmation box.

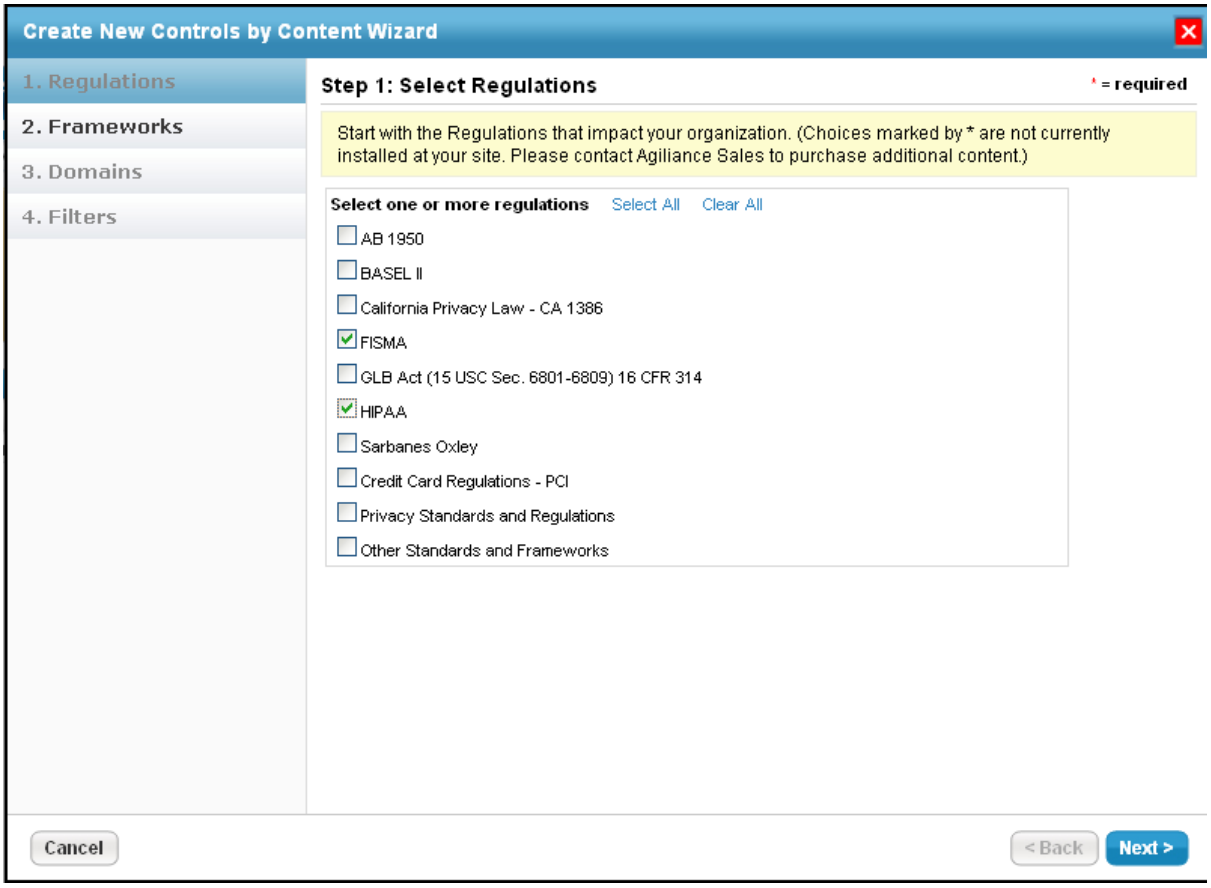
Selecting Domain-Specific Controls

Policy authors identify risks in different domains that significantly impact their organization. Creating a control using content wizard is a content action which provides the freedom to choose the industry standards, frameworks, and regulatory controls. A user can choose a regulation to build controls that can be enforced implicitly within a domain. Stakeholders use the content pack to assess the standard controls and subcontrols by performing various workflow stage actions such as draft, test and approve prior to control deployment.

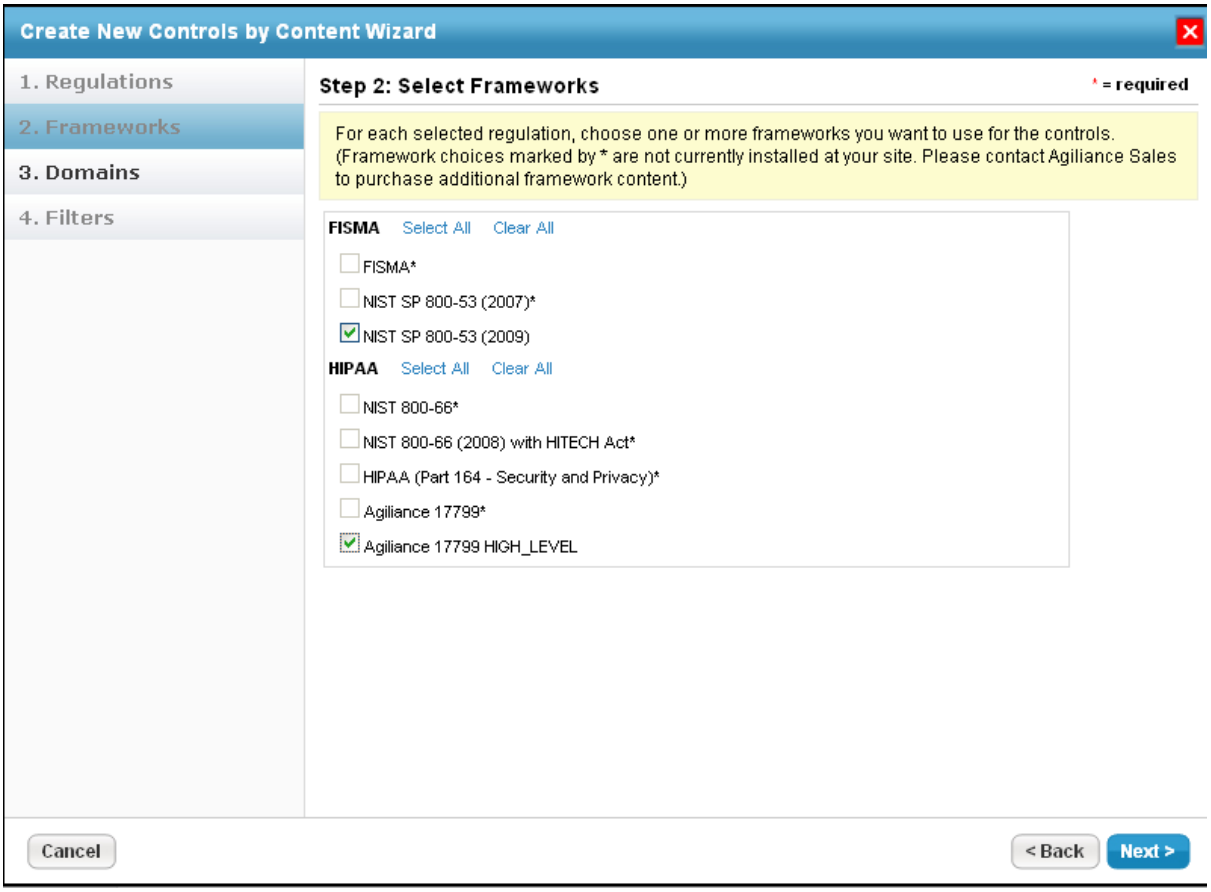
To select domain-specific controls:

1. In the RiskVision application, go to **Controls** > **Controls and Questionnaires**, and select the desired controls group. In the RiskVision application, go to **Risks** > **Controls and Questionnaires**, and select the desired controls group. In the RiskVision application, go to **Policies** > **Controls and Questionnaires**, and select the desired controls group.

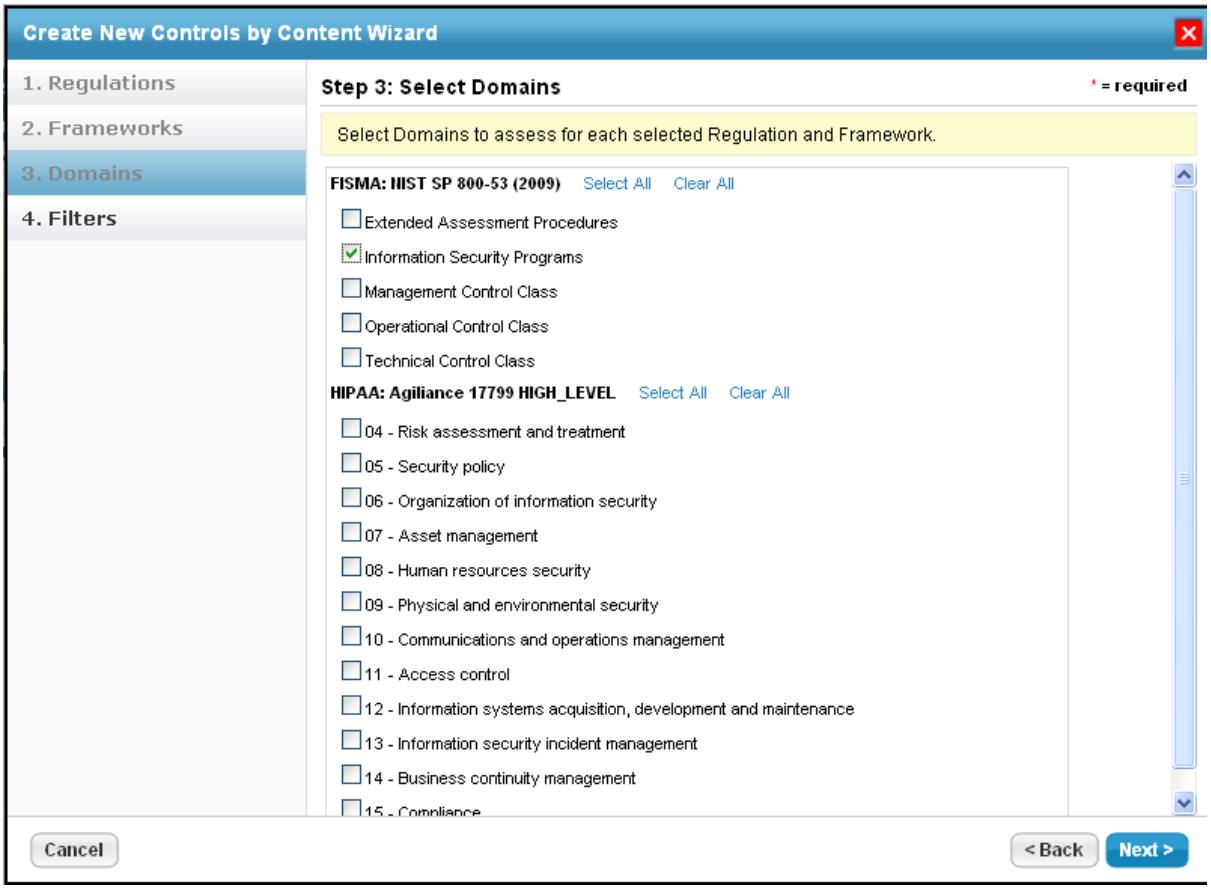
2. Select **New Controls with Content Wizard** in the **Actions** pull-down list to launch **Create New Controls by Content Wizard**, displaying the **Regulations** wizard page.



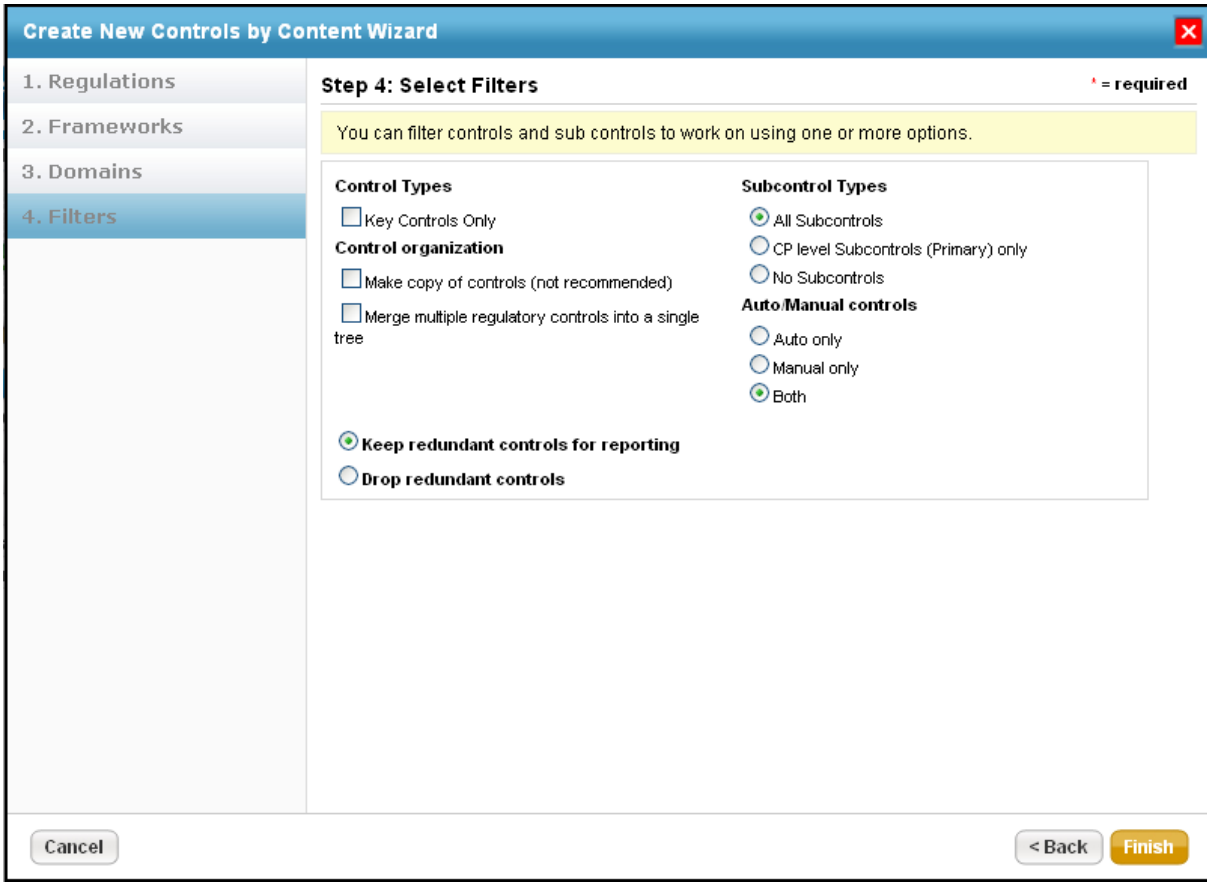
3. Select one or more regulations and click **Next**. The **Frameworks** wizard page appears.



4. Choose frameworks related to the regulations selected in the previous step and then click **Next**. The **Domains** wizard page appears.



5. Click **Select All** to choose all the domains related to a framework or select specific domains that are applicable to one of the many assessments. For example, to assess the security-related risks in your organization, you might choose the **Information Security Programs** domain. Click **Next** to display the **Filters** wizard page.



6. To match the business objective, you might want to run concise assessments by using various filters such as subcontrol types, control organization, auto/manual controls, and redundancy controls.

7. Click **Finish** to add domain-specific controls to create programs and assessments that assess your organization's risk with respect to the specified domains.

Configurable Control Testing

Flexible tests and documentation-type controls are designed to be self-documenting, providing a central place to find audit work, such as test scripts, walk-throughs, and evidence.

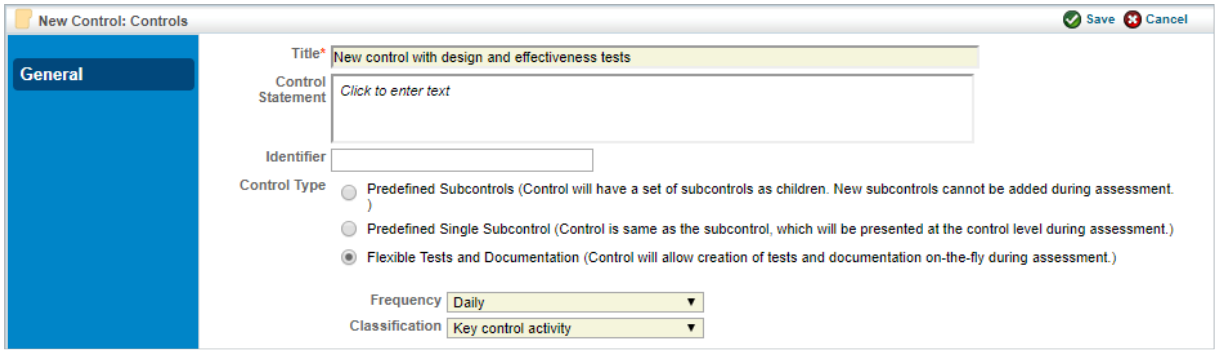
This type of control includes a design test and can have an unlimited number of effectiveness tests associated with it. Assessments can include ordinary controls and flexible types. Questionnaire responders can add effectiveness tests dynamically, but these tests will only apply to that particular assessment. Likewise, users with sufficient privileges can create tickets to mitigate deficiencies found when testing controls.

A particular role might be permitted to view effectiveness tests, but not to manage them, and to have no permissions regarding design tests.

Control Assessment-type programs can be used, and the content can include the Control Effectiveness Testing workflow. This workflow has stages for Control Design, Audit, Certify, and Closed.

To create a control for configurable control testing:

1. Go to the **Content** menu, then click **Controls and Questionnaires**.
2. Select a writable group in the **Organization Content** tree, then click **New Control**.
3. Complete the name and other fields. Click the **Flexible Tests and Documentation** radio button.
4. Click the **Frequency** and **Classification** dropdown lists and select a value.



The Create a new Control screen.

5. Click **Save**.

To convert an existing control into an audit-friendly control:

1. Open the **Content** menu, then click **Controls and Questionnaires**.
2. Select the group or content pack containing the control to be converted.
3. Check the box next to the controls to be converted.
4. Click **More Actions** > **Convert to Controls with Flexible Tests**.
5. Make a copy or export the original control if you want to preserve the old type. A design test is automatically created for the new audit-friendly control.

Configuring Default Manual Control Choices

While setting up manual subcontrol questions, you can use the default choices by leaving the choice field blank for radio button and checkbox type answers instead of defining your own.

The RiskVision solution applies changes to the existing default answers when a program is launched. Changes do not affect programs and assessments that are already in progress.

To change the settings:

1. Go to **Content** > **Controls & Questionnaires.** Navigate the tree to **Controls & Questionnaires** > **Organization Content** > **Choice Templates** and click on the choice template to change.
2. Click **Edit**.
3. Select the default answers and clear the ones that you want to remove.
4. Choosing any of the 0-1 answers displays the Rating drop-down with the selected answers.

   For example, if you select:

   0: Control is in place without exceptions

   3: Control is NOT in place but approved plan to implement

   5: Control is NOT in place with no current plan to implement

   A Rating drop-down with 0, 3, and 5 appears in the questionnaire
5. Click **Save**.

Migrating Draft Content into Versioned Content

Content that has no workflow associated with it or that has not been deployed yet is termed as draft content. If you use draft content in program assessments and change the draft content later, then you will encounter inconsistent and undesired results after updating the program to reflect the latest content changes. Therefore, always recommends using versioned content for your assessments because versioned content allows you to incorporate the latest content changes into program assessments consistently. The draft content attached to a program can be attached as a group, content pack, control objective, or questionnaire. This section provides instructions for migrating draft content used in your programs to versioned content.

Important!

- Please keep in mind that assessments must be in an open state when migrating draft content. If you have to migrate draft content in closed assessments, you must restart the closed assessments.
- Before making changes to draft content that was migrated to version 1 of a content pack, you should archive all assessments that need to be archived on version 1 of the content pack. Only after restarting the assessments should you update the program to use version 2 of the content pack.
- Log in to the RiskVision Administration application and deactivate all scheduled jobs. In some cases, the server may need to be rebooted to prevent jobs changed from automatic to manual from starting automatically.
- Seek to prevent any active users in the system (such as by turning off the LDAP connector and/or performing the migration at an off-peak time).
- Please do not edit and update the program prior to migrating from draft to versioned content. If you need to change some of the program options, RiskVision recommends doing this after you have migrated your content from draft to versioned.

Migrating draft content that is already part of a content pack

1. Go to the `%AGILIANCE_HOME%\config` directory, open the `agiliance.properties` file using a text editor, and add the following properties: `ui.migrateDraft.enable=true`
2. Log in to the server where the Resolver database is installed.
3. Log in to the database.
4. Start the tool that is available to run SQL commands.
5. Connect to the RiskVision database.
6. Execute the following query:

   update agl_policyset

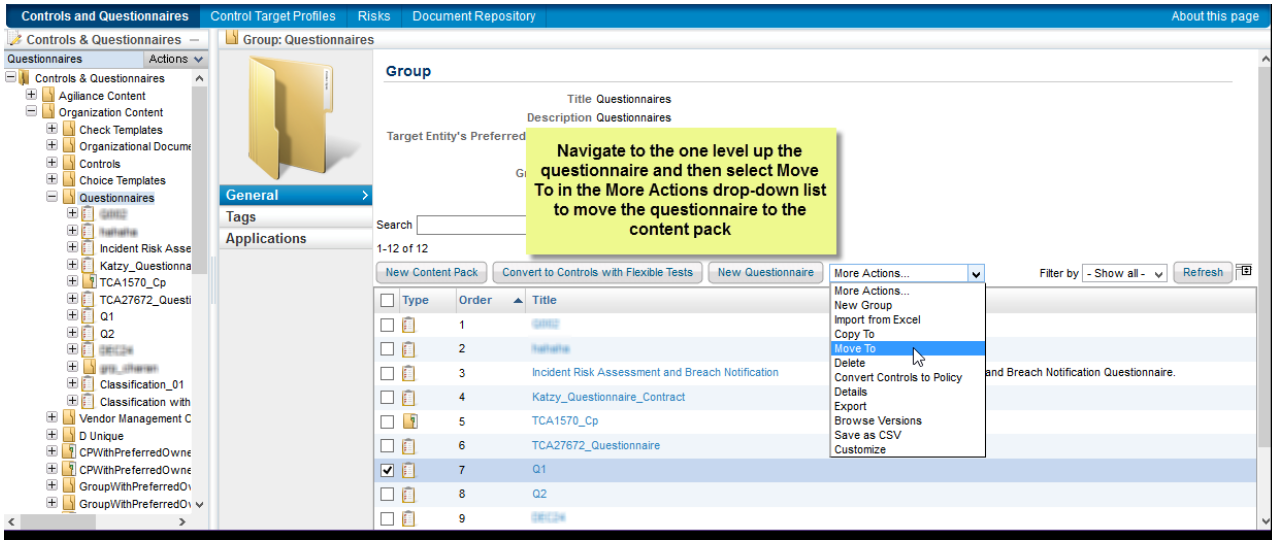
   set policyset_type = 'PolicyPack', policyset_subtype = 'subtype_nocontroldocument', policyset_flags = '134'

   where title like '';

   commit;

   Where is the group at the highest level in that hierarchy in which the content is present.

   Executing the query above converts the group to a content pack.
7. Restart the RiskVision Tomcat Application service.
8. Log in to the RiskVision application and navigate to the **Controls and Questionnaires** page.
9. Create a content pack and move the draft questionnaire to the newly-created content pack.



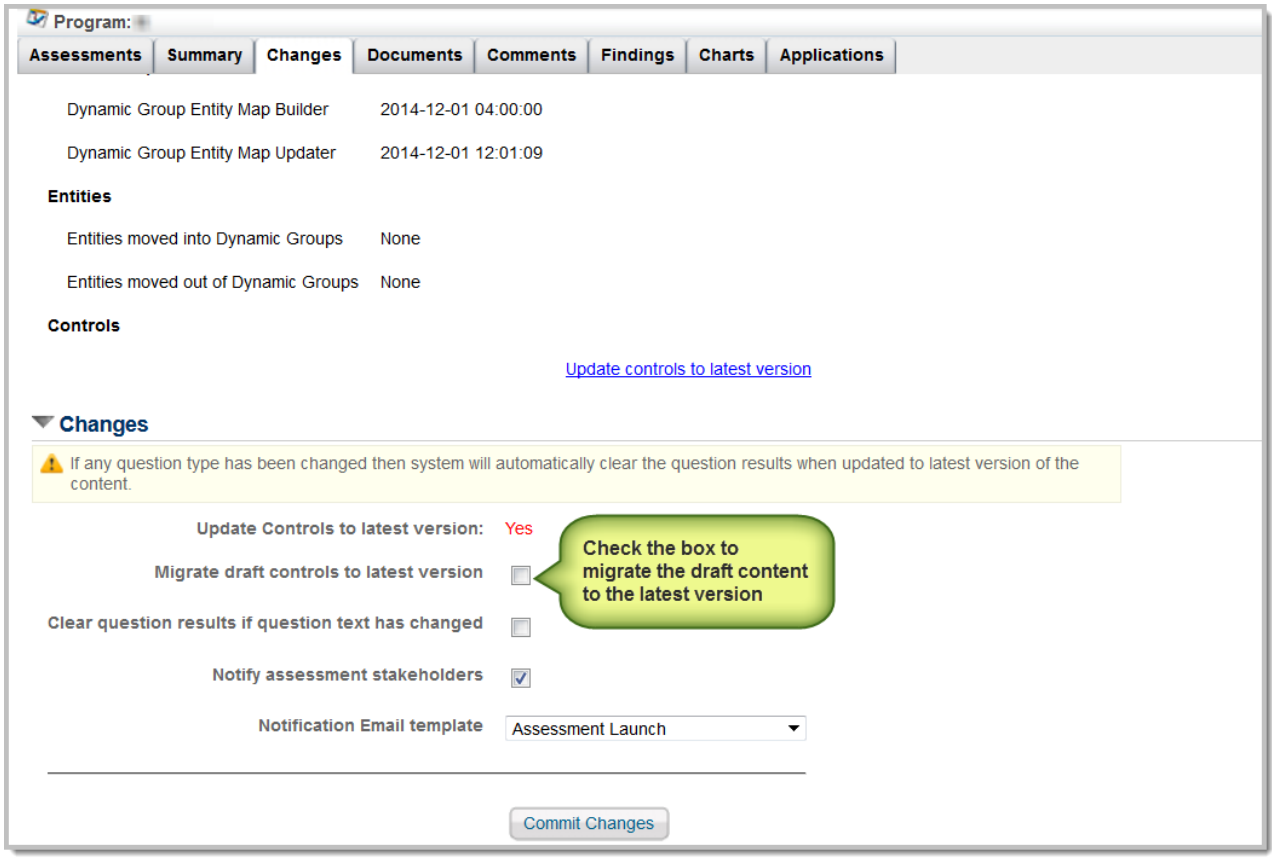
1. To update the primary owner, navigate to the **Ownership** tab, click **Edit** and click **Save.** Now the primary owner has permission to restart the workflow for the second time.

2. Click the **Workflow** tab, select a workflow in the drop-down list, and click Start Workflow. The workflow enters the first stage. Move the workflow to the closed stage so that the versioning is applied to the content. The content pack will now be in version 1.

3. Navigate to the **Assessments > Programs**, locate the program containing the draft content, and select it to open its details page.

4. Click the **Changes** tab.

5. From within the **Changes** section, check the box next to the **Migrate draft controls to latest version** option, clear the **Notify assessment stakeholders** option, and click **Commit Changes**.



Note: If there is more than one group or questionnaire in a program, RiskVision recommends converting all of the groups or questionnaires to a content pack before you update the controls to the latest version. You can use a single content pack for all of your draft content or multiple content packs.

Create a New Group

You can only add groups to the Organization Filters group.

To add a group:

1. Go to **Configuration** > **Filters**.
2. Select an organization group.
3. Click **More Actions** > **New Group**.
4. Enter a name and description.
5. Click **Save**.

Adding a Tag to a Group

Tags allow you to run reports on assessments of a group's content. That is, tagging a group refers to the group's controls and related risks. Tags allow you to gather information using questionnaires, run automatic checks, execute policy awareness campaigns, and so on.

When a user owns the permission to create a group, that user automatically has the access to add, update, or delete a tag associated with a group.

To tag a group:

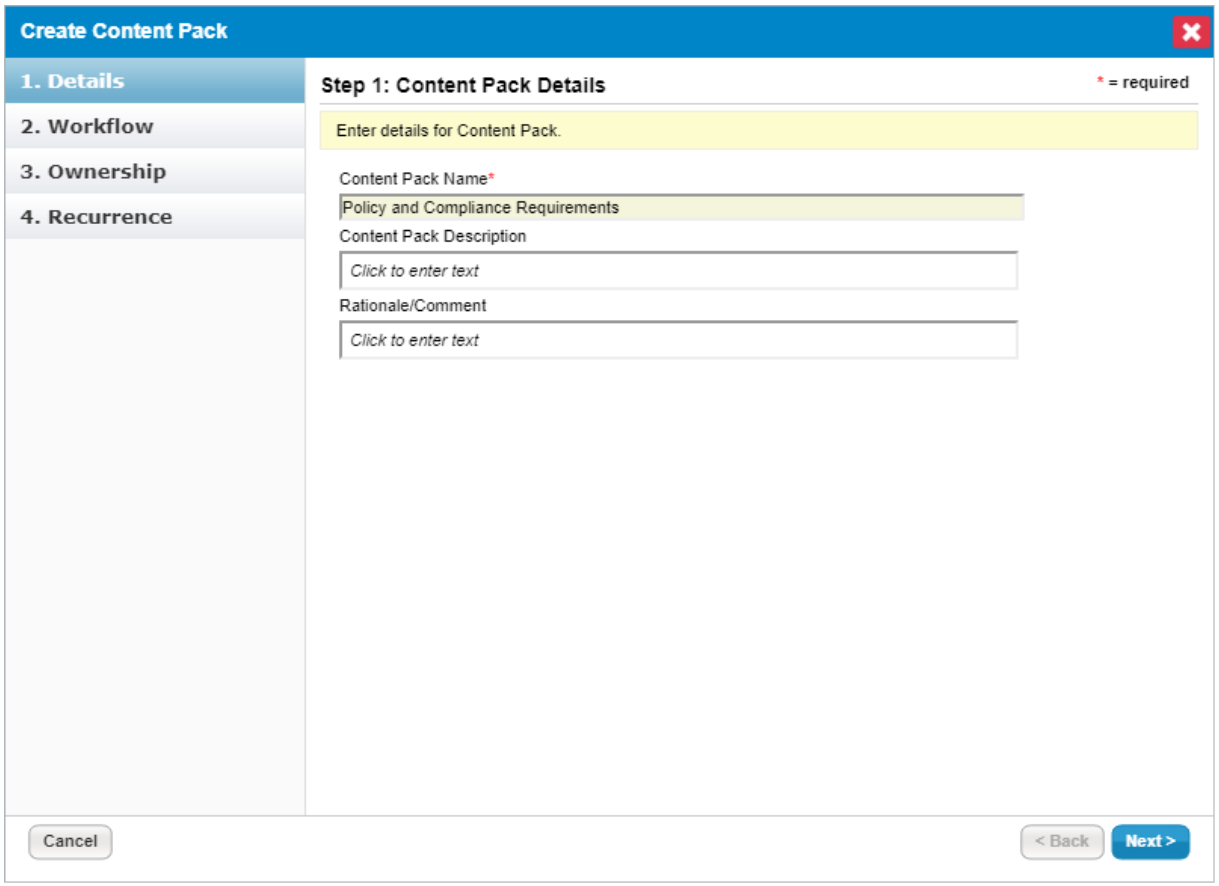
1. On the **Content** menu, click **Controls and Questionnaires**. (On the **Risks** menu, click **Controls and Questionnaires**. On the **Content** menu, click **Questionnaires**.
2. Select the folder that contains the group. The contents of the folder will be displayed in a table.
3. Select the group folder.
4. In the **More** actions, select **Details**.
5. Click the **Tags** tab. The tag table displays.
6. Click **New**. The **new tag** dialog displays.
    - Select the tag category or create a new one.
    - Select a tag or create a new one.
    - Click OK.

Creating a New Content Pack

Use content packs to develop and review organization specific content. To create a new content pack, your user role must have Control View and Control Author permissions.

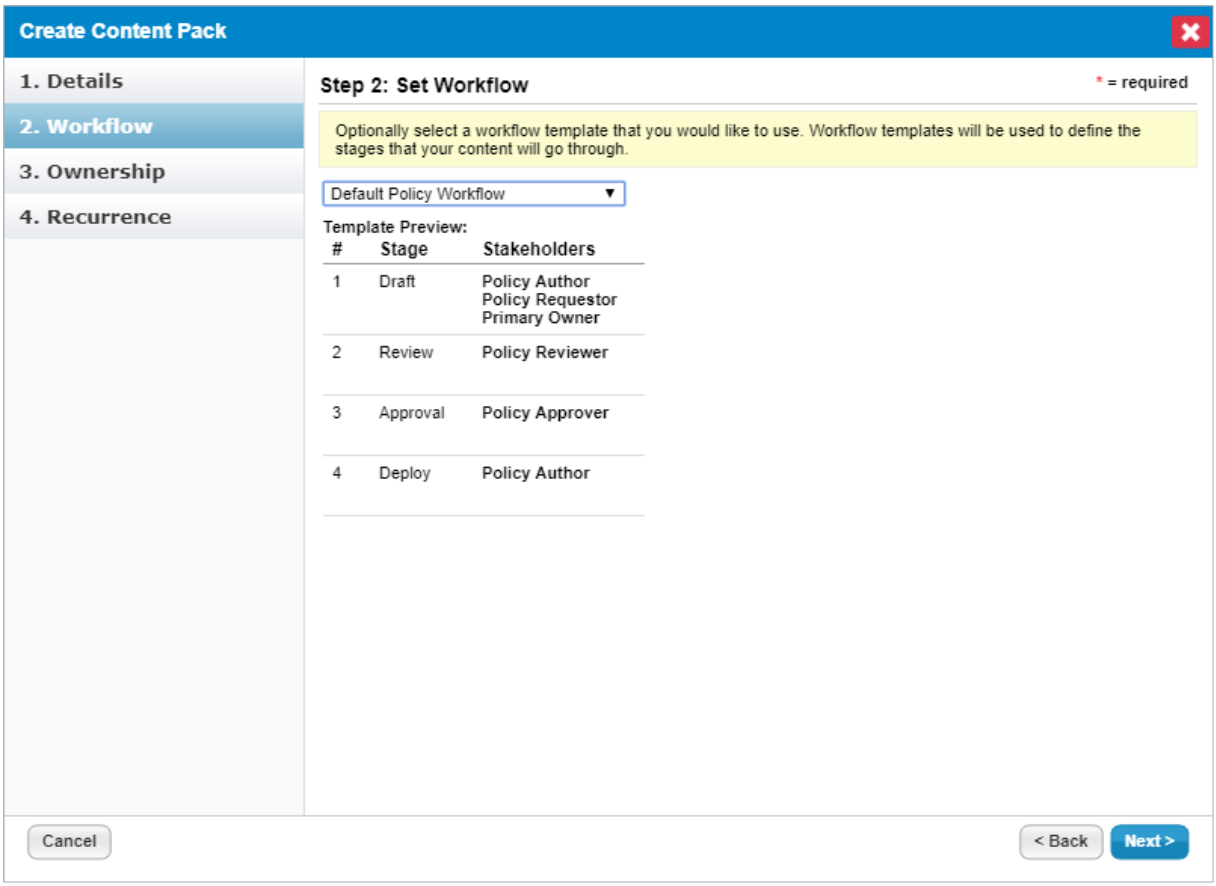
To create a new content pack:

1. On the **Content** menu, click **Controls and Questionnaires**.
2. Expand **Organization Content** and select the group where you want to create the pack.
3. Click **New Content Pack**.
4. Enter a name, description, and any comments you want to add to the version log.



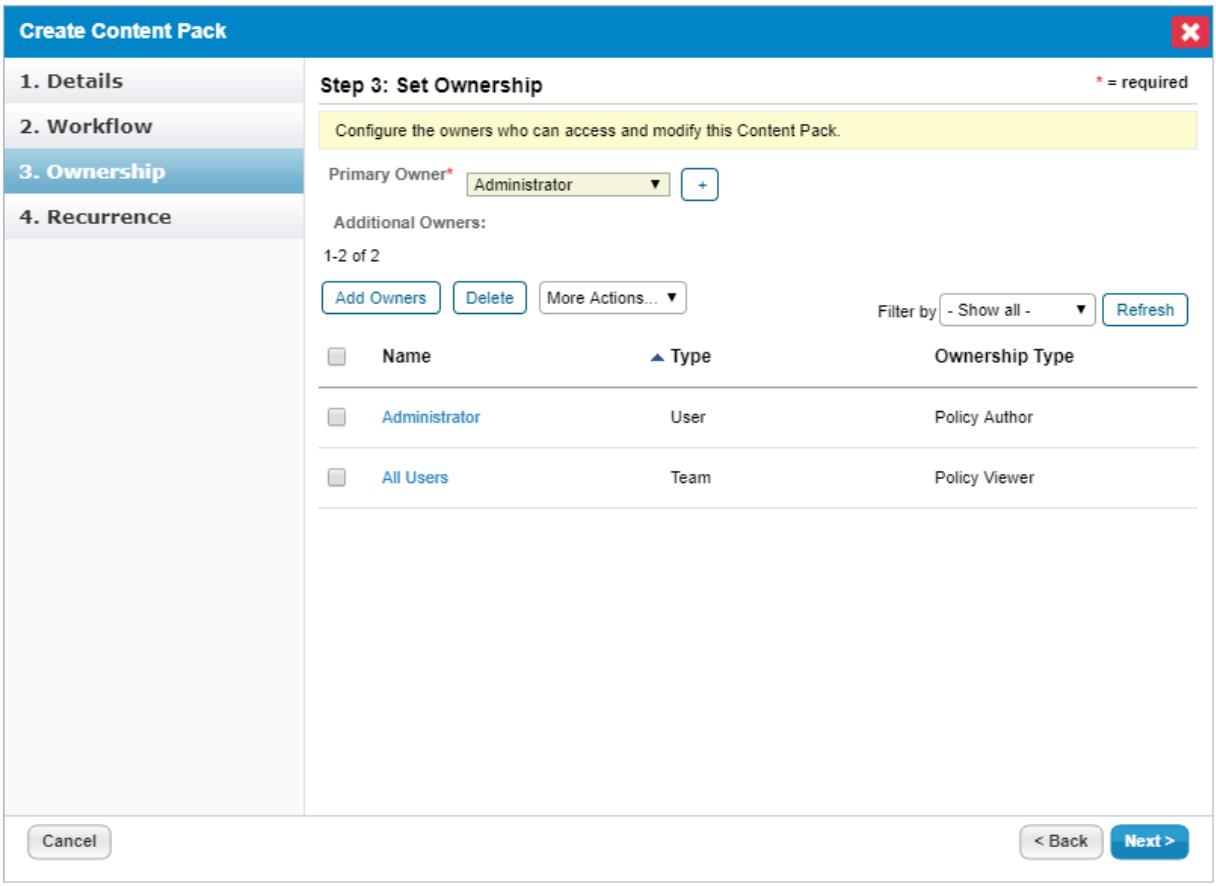
The Details page on the Create Content Pack wizard.

5. Click **Next**.
6. Select the workflow that you want to follow when creating this content pack.



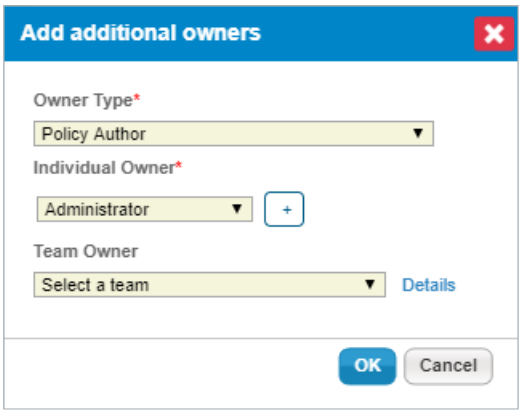
The Workflow page.

7. Click **Next**.
8. **Optional:**To change the primary owner, select a different user from the primary owner drop-down. To remove an owner, select the owner and click **Delete**.



The Ownership page.

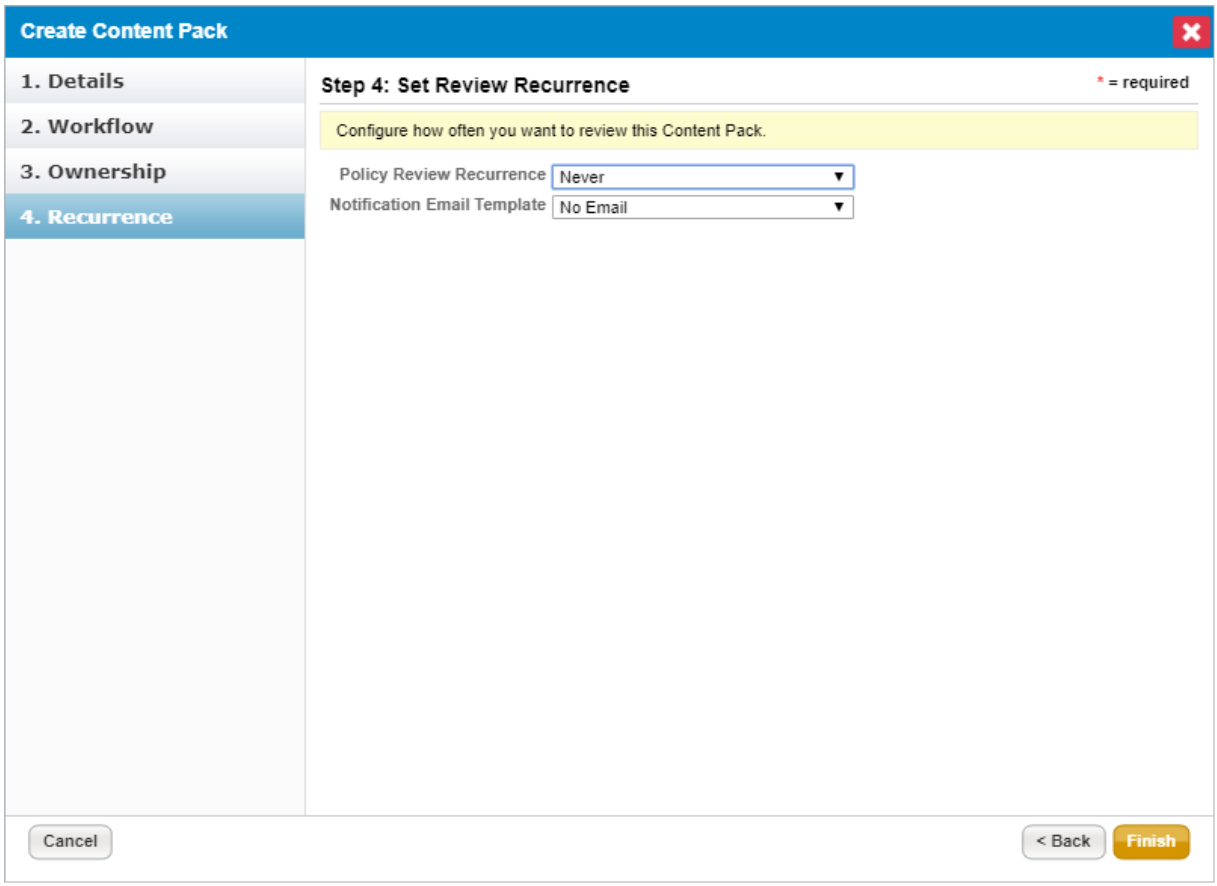
9. **Optional**: To add additional owners:
    a. Click **Add Owners**.
    b. Click **Owner Type** and select an owner type. For more information, see Configuring Ownership Types.
    c. Click **Individual Owner** and select a user. Skip this option to assign a team only.
    d. Click **Team Owner** and select a team. Skip this option to assign a user only.
    e. Click **OK**.



The Add Additional Owners dialogue box.

10. Click **Next**.

11. Click **Policy Review Recurrence** to specify how often the review must recur (or if it should not at all). Click **Notification Email Template to** select an email template to use to remind stakeholders.



The Recurrence page.

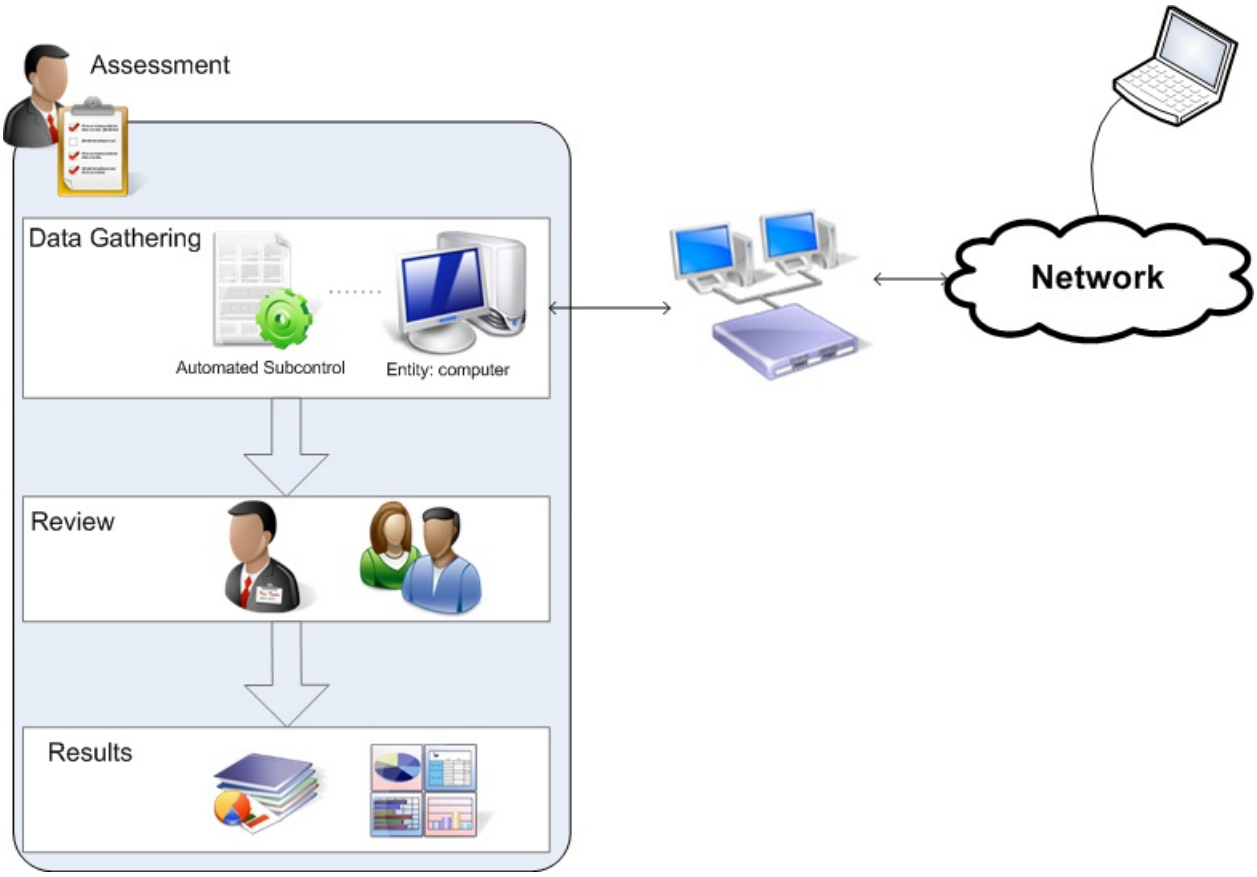
12. Click **Finish**.

The content pack workflow process will now launch and the stakeholders of the first stage will be notified. When the associated workflow is moved to the closed status, the content pack will be deployed and versioning will be applied.

Automated Controls

Automated controls use connectors to verify information on a remote system. An automated control performs a series of pass-fail tests and the results display automatically on the questionnaire results page of the assessment.

You must install and configure the connector on the RiskVision solution and then configure the connector - entity relationship



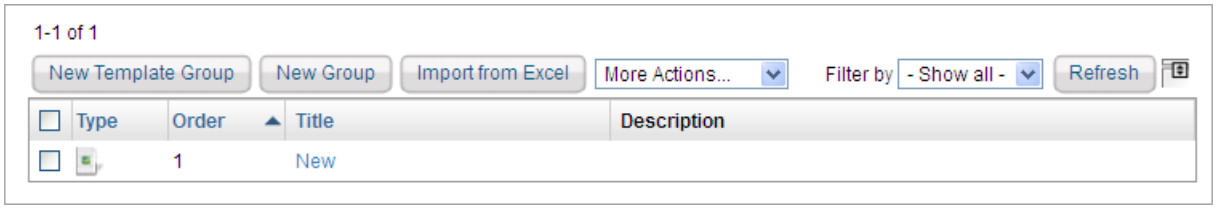
Create an Automated Control

Automated controls are considered groups of subcontrols. You can only create automated controls in the **Check Templates** folder when you have Control View and Control Author permissions.

You cannot directly assign a subcontrol in an assessment. Therefore, if there is a single check, you must still create a group.

To create a template group:

1. Go to the **Content** menu > **Controls and Questionnaires**.
2. Expand **Organization Content**. Click **Check Templates**.
3. **Optional**: Structure your content in a new root folder by Creating a New Group.



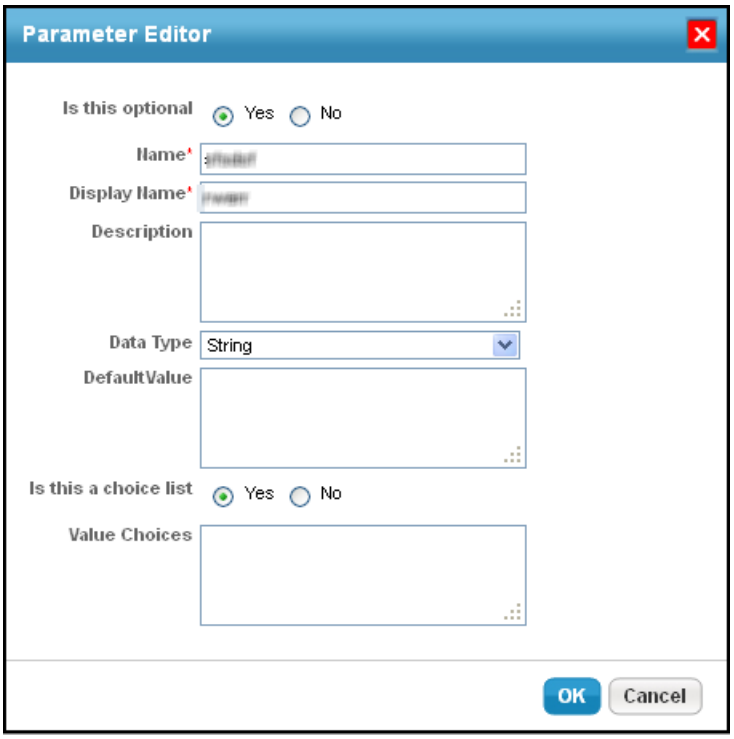
The Check Template Group details.

4. Click **New Template Group**.
5. Enter the following fields:
    - **Title**: The label that identifies the group.
    - **Control Statement**: Enter an optional statement to be associated with the new control. Click the field to open the rich text editor. The control statement specifies the actions or checks that must be provided by supporting subcontrols.
    - **Identifier**: Enter an optional identifier for the new control.
    - **Control Type**: Choose a control type.
    - **Status**: Lets you specify the stage of associated control development or completion. You can use this information to identify and track progress at various stages of completion.
    - **Key Control**: Click **Yes** if this is a key control. This field indicates whether the control must be included when a user selects **control options only** to implement or use key controls in measuring risk and compliance.
    - **Version**: Enter the new automated control's version in any consistent format.
    - **Target Entity's Preferred Ownership**: Choose users, teams, and roles to be preferred owners of the new control.
    - **Objective**: The Objective statement specifies the purpose of supporting controls that enforce, check, or verify risk measurement and compliance with organization policies and goals.
    - **Weight**: Indicates the weight assigned to this group when paired with other groups in an assessment. When compliance and risk scores are rolled up, values are calculated based on the percentage. This control objective's weight contributes to the total weight of objectives at the same level in a hierarchy.
    - **Reference Numbers**: Lets you specify information corresponding to related control framework or regulation reference numbers such as ISO-17799 1.4.1. To enter multiple reference numbers, you can include the reference numbers in a comma-separated list.
6. Click **Save**.

Setting the Input Parameters

The RiskVision solution populates the available arguments based on the Check Template parameters that you selected. Each argument may have different input parameters.

To specify the value:



1. Select an argument.
2. Click **Edit**. The **Parameter Editor** dialog appears.
3. Choose whether you want the argument to be optional, specify Name, Display Name, and Description, choose a Data Type, specify the default value for the selected string, choose whether the argument is a choice list and specify the value for choices, if you wish to make the argument a part of choice list.
4. Click **OK**.

Setting the General Information

Enter the general information for the automated subcontrol:

Setting	Description
Title	Enter the name of the check template that identifies the template to users.
Description	Enter a summary that describes the purpose of the check.
Reference Numbers	Enter a string or number that uniquely identifies this check or that identifies another related control or subcontrol to which you want to map the check results.
Weight	Enter a number used to normalize the importance of this subcontrol as compared to other subcontrols when evaluating results.
Author	Select the user who is the primary owner of this subcontrol. Any user with Policy privileges can access, view, and author, the automated controls.

Selecting a Check Template

Extends the automated subcontrol by defining which parameters and corresponding input values that the automated control must match to pass or fail the check.

By default, there are two root level groups that can contain check templates:

- **Check Templates**. Contains Resolver defined templates associated with particular checks.
- **Organization Check Templates**. Contains customized templates created by your organization.

Selecting the Check Parameters

The RiskVision solution populates the available selections on this page from the Check Template that you selected.

Check parameters are output values from the automated control.

Setting	Description
Optional	Yes or no
Name	Internal name
Display Name	Visible name
Description	Text describing the check parameter
Data Type	String, Integer, Float, Boolean, Date, Timestamp, list.application, list.patch, list.vulnerability, list.port, list.service, list.vulnSoftware
Default Value	Value if none entered
Choice List	Yes or no
Value Choices	List of potential choices

About the Common Control Framework

The RiskVision solution provides a common control framework out of the box, allowing your organization to test once and comply with many different standards.

Managing compliance and risk analysis one regulation at a time can be cumbersome, redundant, complex, and expensive. Standard frameworks such as CoBIT, NIST, and ISO 17799/27001 aid organizations by reducing the overhead required to develop and maintain custom controls. Recognizing that a significant number of specific control requirements are common across several frameworks -- for example, CoBIT-4, NIST 800-53, and FFIEC share a number of controls -- recommends employing a common control framework to reduce cost and complexity and improvement risk management effectiveness.

Using a common control framework, one assessment, rather than many will suffice to certify against any number of regulations.

A common control framework supports:

- Mapping of controls from 17799/27001, CoBIT, CoSo, NIST, FFIEC, and GAISP, among others, as well as custom-built controls to one common set of controls.
- Maintenance of the relationship between a common control and the corresponding regulation-specific control in the standard, simplifying change management.

The common control framework simplifies the process because there are fewer controls to test and independent assessments are unnecessary. Cost is lower as more work gets done faster with potentially fewer people. Now, the business can test once and certify against many regulations.

Common Control Framework

The RiskVision solution provides a common control framework out of the box, allowing you to test once and comply with many different standards. Using the Common Control Framework, one assessment rather than many will suffice to certify against any number of regulations. The Common Control Framework supports:

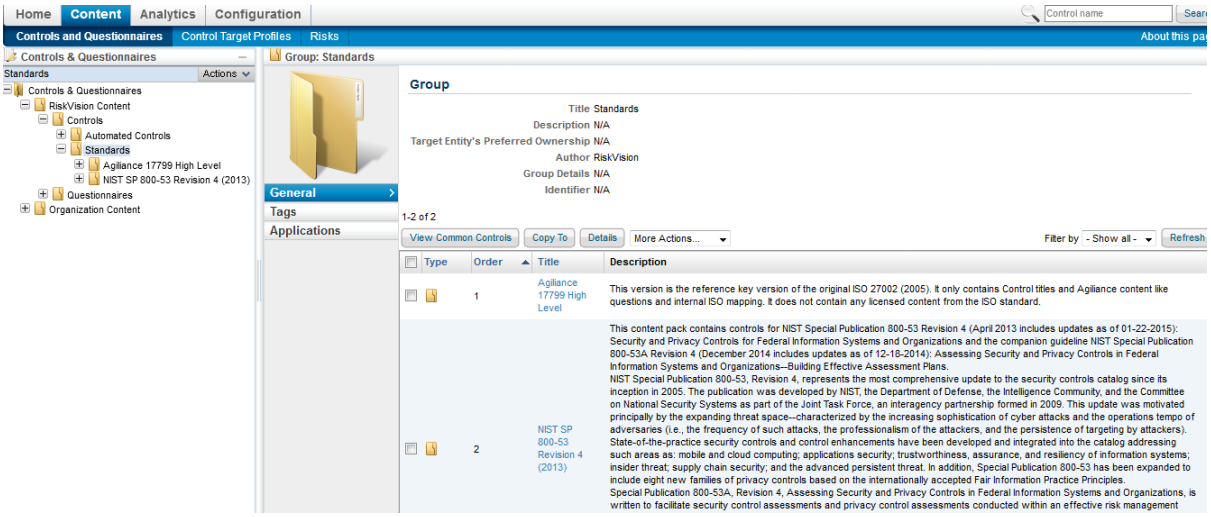
- Mapping of controls from 17799/27001, CoBIT, CoSo, NIST, FFIEC, and GAISP, among others, as well as custom-built controls to one common set of controls based on the ISO standard.
- Utilizing the relationship between the common controls based on the ISO standard and the corresponding regulation-specific controls to share control results for mapped controls, reducing the resources required to comply with, and track compliance with multiple regulations.

The Common Control Framework simplifies the process because controls only need to be tested once, and not once for each framework. This will increase operational efficiency and reduce expenses.

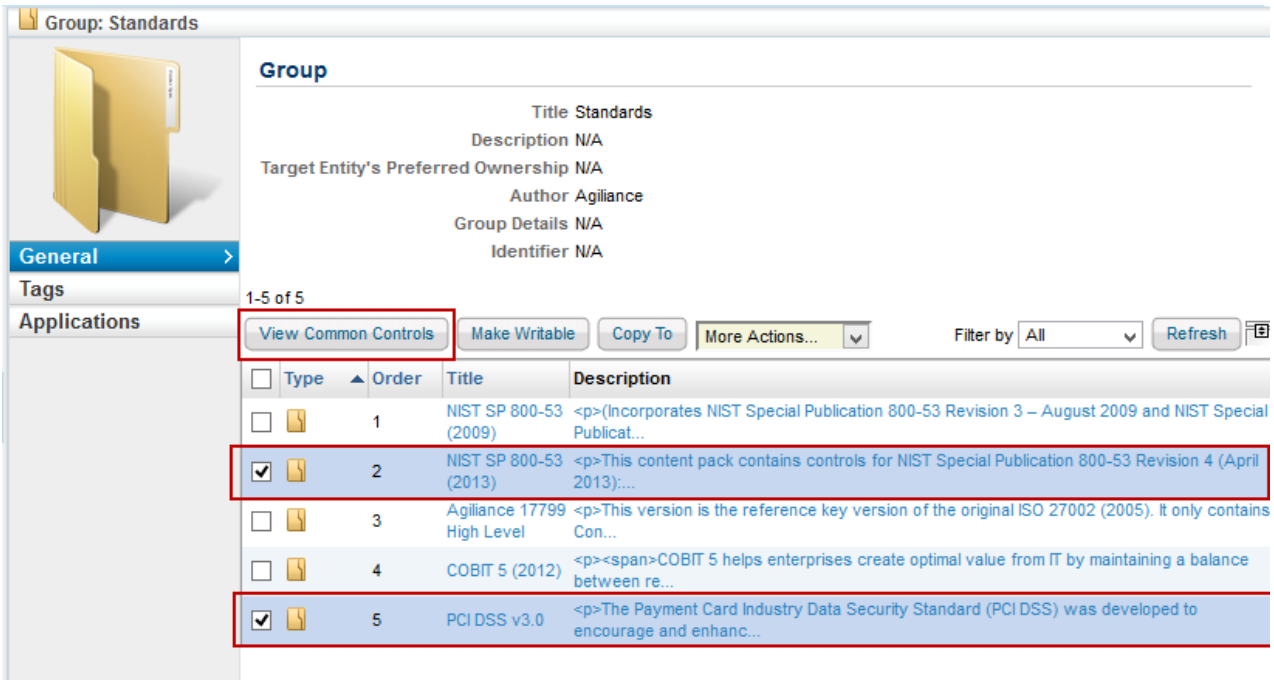
The Common Controls report lets you see a visual comparison of the controls employed in two or more standards.

To compare controls from two or more standards:

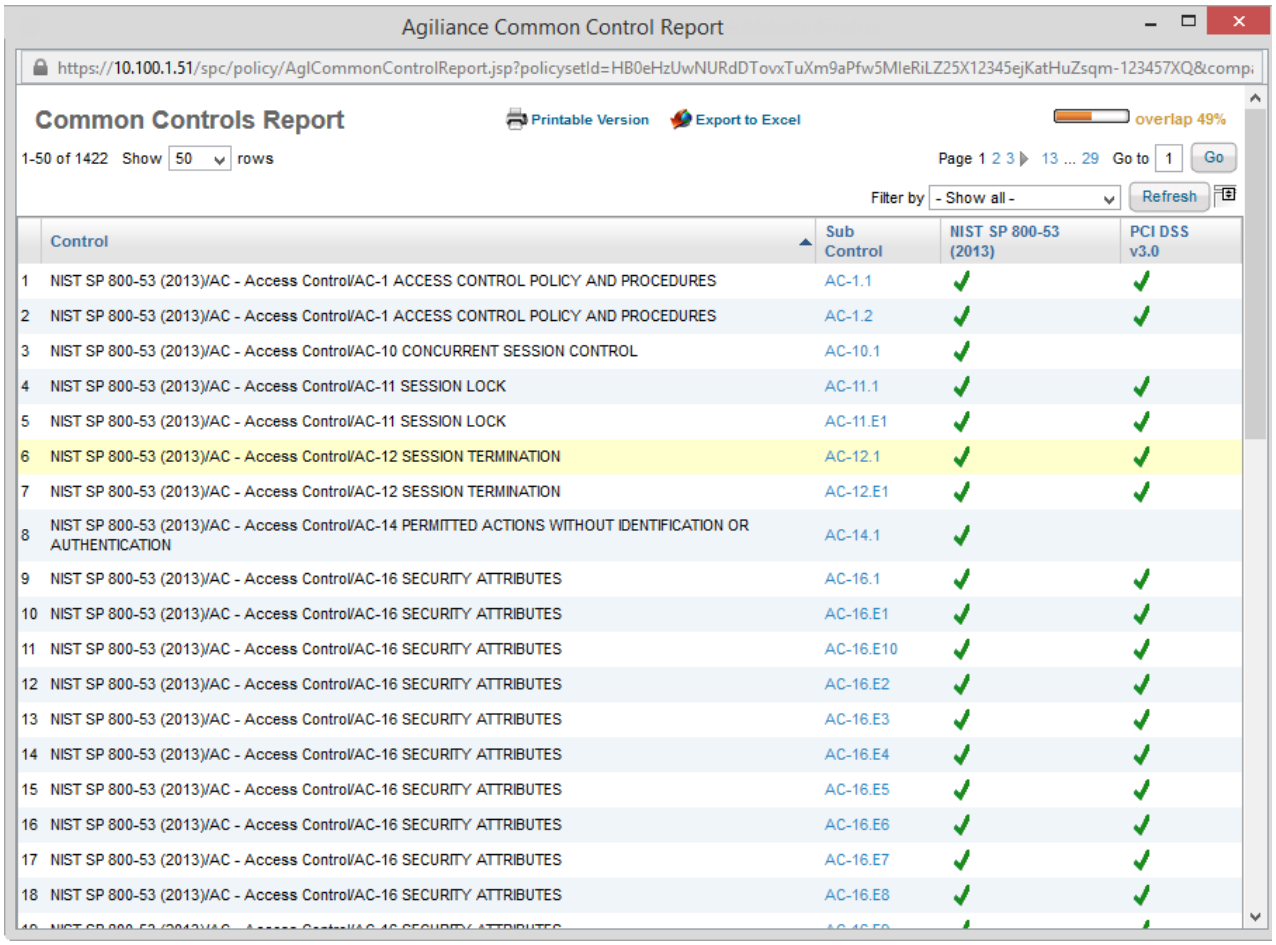
1. In Resolver RiskVision, go to **Content** > **Controls and Questionnaires**.
2. Expand the **Controls and Questionnaires** tree and navigate to **Controls and Questionnaires** > **Content** > **Controls** > **Standards**. A grid view of the available standards appears in the right pane.



3. Select two standards, and click on **View Common Controls**.



4. A **Common Control Report** appears in a pop-up window.



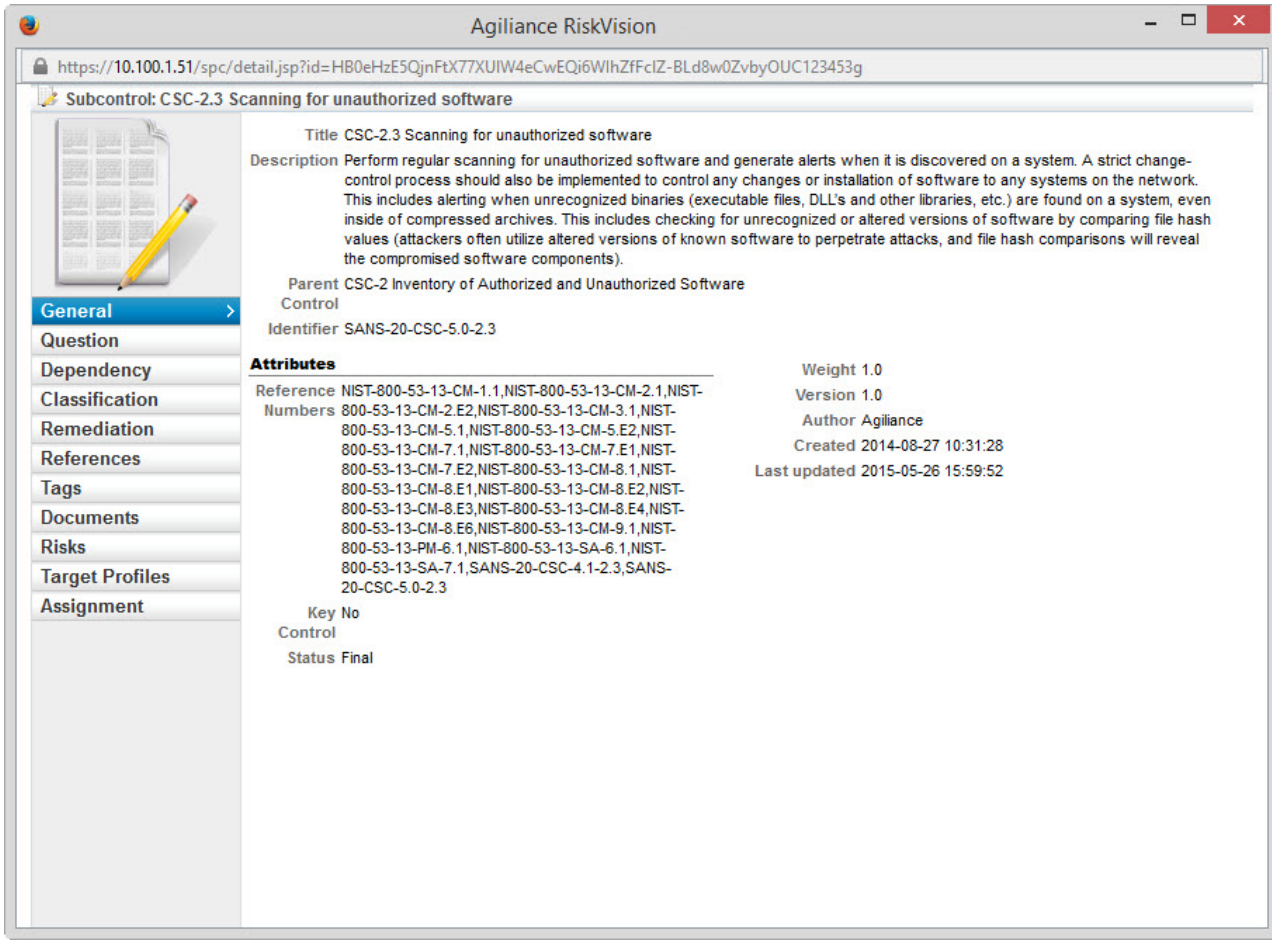
	Control	Sub Control	NIST SP 800-53 (2013)	PCI DSS v3.0
1	NIST SP 800-53 (2013)/AC - Access Control/AC-1 ACCESS CONTROL POLICY AND PROCEDURES	AC-1.1	✓	✓
2	NIST SP 800-53 (2013)/AC - Access Control/AC-1 ACCESS CONTROL POLICY AND PROCEDURES	AC-1.2	✓	✓
3	NIST SP 800-53 (2013)/AC - Access Control/AC-10 CONCURRENT SESSION CONTROL	AC-10.1	✓	
4	NIST SP 800-53 (2013)/AC - Access Control/AC-11 SESSION LOCK	AC-11.1	✓	✓
5	NIST SP 800-53 (2013)/AC - Access Control/AC-11 SESSION LOCK	AC-11.E1	✓	✓
6	NIST SP 800-53 (2013)/AC - Access Control/AC-12 SESSION TERMINATION	AC-12.1	✓	✓
7	NIST SP 800-53 (2013)/AC - Access Control/AC-12 SESSION TERMINATION	AC-12.E1	✓	✓
8	NIST SP 800-53 (2013)/AC - Access Control/AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14.1	✓	
9	NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES	AC-16.1	✓	✓
10	NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES	AC-16.E1	✓	✓
11	NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES	AC-16.E10	✓	✓
12	NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES	AC-16.E2	✓	✓
13	NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES	AC-16.E3	✓	✓
14	NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES	AC-16.E4	✓	✓
15	NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES	AC-16.E5	✓	✓
16	NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES	AC-16.E6	✓	✓
17	NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES	AC-16.E7	✓	✓
18	NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES	AC-16.E8	✓	✓

This Common Control Report shows a visual comparison of the sub-controls common to the selected standards.

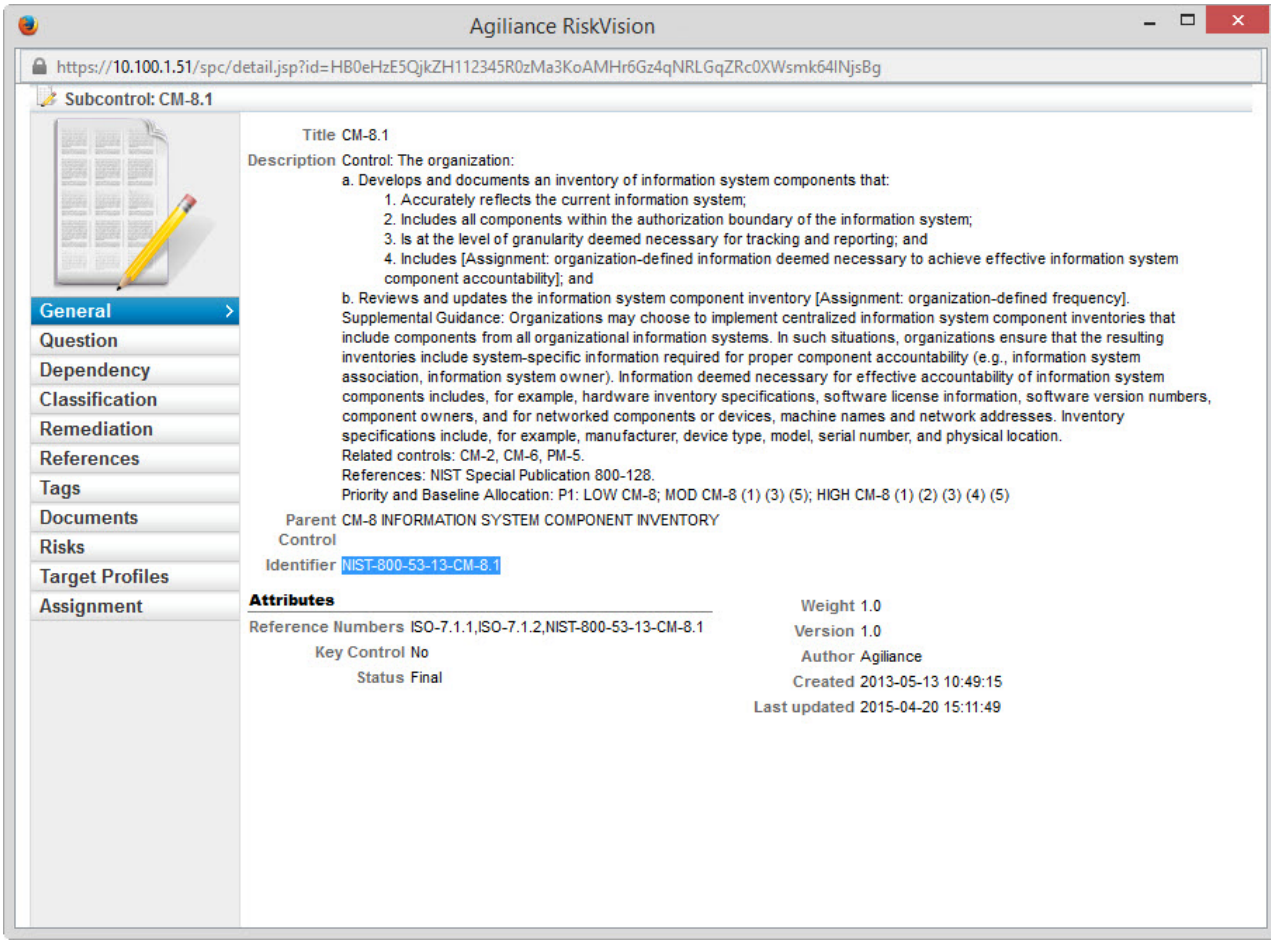
For example: 'CSC-5.1 Automated tools to continuously monitor' has sub-controls common in both NIST SP 800-53 (2013) and SANS 20 Critical Security Controls V5.0.

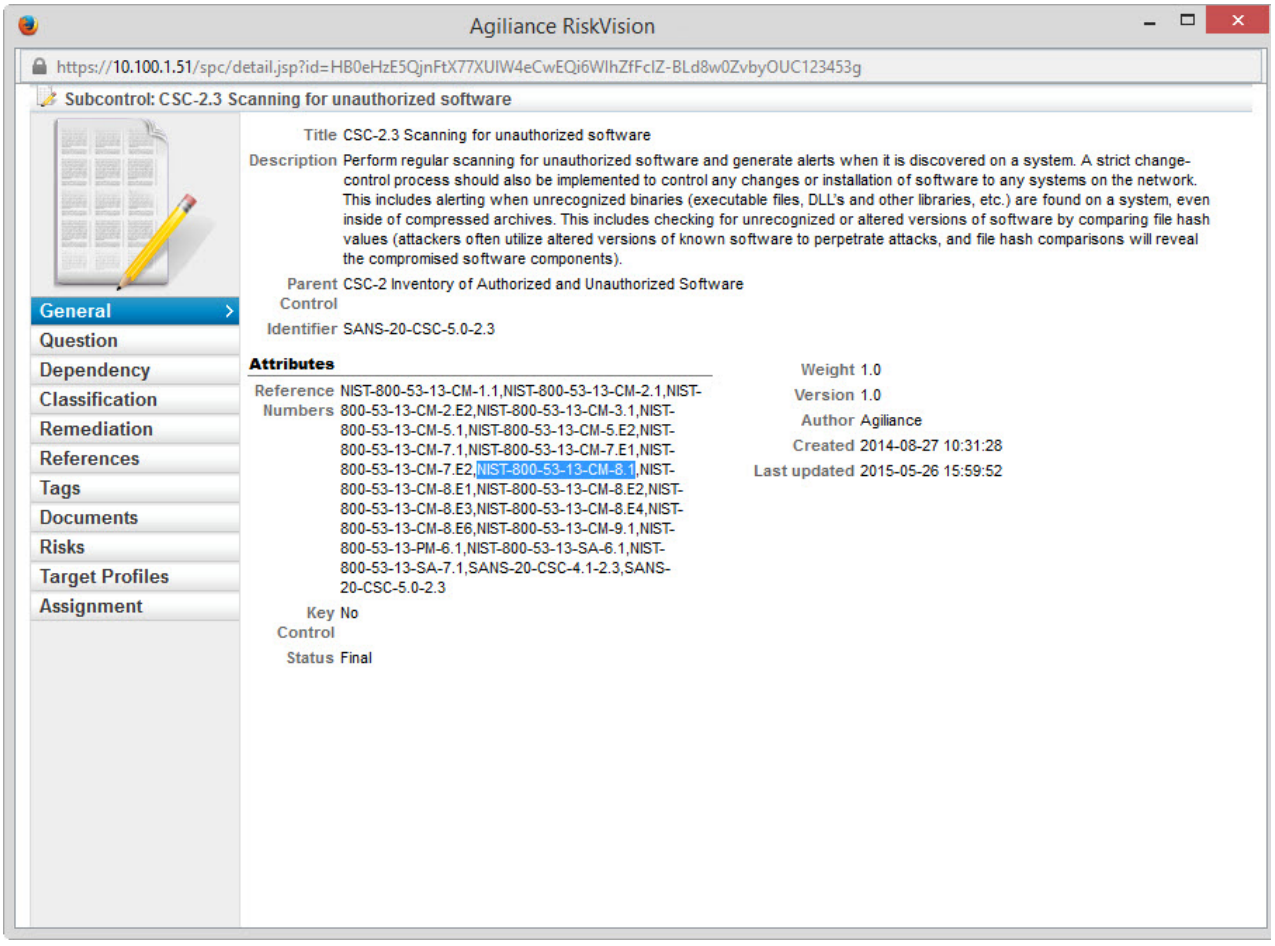
Click on tick mark in the standard column to see details of the common sub-controls.

Clicking on the sub-control displays a pop-up with information related to the sub-control.



If the sub-control identifier of the first sub-control is used as a reference number in the second sub-control or vice versa, then those two sub-controls are common controls.


Agiliance RiskVision
https://10.100.1.51/spc/detail.jsp?id=HB0eHzE5QjkZH112345R0zMa3KoAMHr6Gz4qNRLGqZRc0XWsmk64lNjsBg
Subcontrol: CM-8.1
General
Question
Dependency
Classification
Remediation
References
Tags
Documents
Risks
Target Profiles
Assignment
Title CM-8.1
Description Control: The organization:
a. Develops and documents an inventory of information system components that:
1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].
Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.
Related controls: CM-2, CM-6, PM-5.
References: NIST Special Publication 800-128.
Priority and Baseline Allocation: P1: LOW CM-8; MOD CM-8 (1) (3) (5); HIGH CM-8 (1) (2) (3) (4) (5)
Parent Control CM-8 INFORMATION SYSTEM COMPONENT INVENTORY
Identifier NIST-800-53-13-CM-8.1
Attributes
Reference Numbers ISO-7.1.1,ISO-7.1.2,NIST-800-53-13-CM-8.1
Key Control No
Status Final
Weight 1.0
Version 1.0
Author Agiliance
Created 2013-05-13 10:49:15
Last updated 2015-04-20 15:11:49


Agiliance RiskVision
https://10.100.1.51/spc/detail.jsp?id=HB0eHzE5QjnFtX77XUlW4eCwEQi6WIhZfFcIZ-BLd8w0ZvbyOUC123453g
Subcontrol: CSC-2.3 Scanning for unauthorized software
General
Question
Dependency
Classification
Remediation
References
Tags
Documents
Risks
Target Profiles
Assignment
Title CSC-2.3 Scanning for unauthorized software
Description Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network. This includes alerting when unrecognized binaries (executable files, DLL's and other libraries, etc.) are found on a system, even inside of compressed archives. This includes checking for unrecognized or altered versions of software by comparing file hash values (attackers often utilize altered versions of known software to perpetrate attacks, and file hash comparisons will reveal the compromised software components).
Parent Control CSC-2 Inventory of Authorized and Unauthorized Software
Identifier SANS-20-CSC-5.0-2.3
Attributes
Reference Numbers NIST-800-53-13-CM-1.1,NIST-800-53-13-CM-2.1,NIST-800-53-13-CM-2.E2,NIST-800-53-13-CM-3.1,NIST-800-53-13-CM-5.1,NIST-800-53-13-CM-5.E2,NIST-800-53-13-CM-7.1,NIST-800-53-13-CM-7.E1,NIST-800-53-13-CM-7.E2,NIST-800-53-13-CM-8.1,NIST-800-53-13-CM-8.E1,NIST-800-53-13-CM-8.E2,NIST-800-53-13-CM-8.E3,NIST-800-53-13-CM-8.E4,NIST-800-53-13-CM-8.E6,NIST-800-53-13-CM-9.1,NIST-800-53-13-PM-6.1,NIST-800-53-13-SA-6.1,NIST-800-53-13-SA-7.1,SANS-20-CSC-4.1-2.3,SANS-20-CSC-5.0-2.3
Key Control No
Status Final
Weight 1.0
Version 1.0
Author Agiliance
Created 2014-08-27 10:31:28
Last updated 2015-05-26 15:59:52

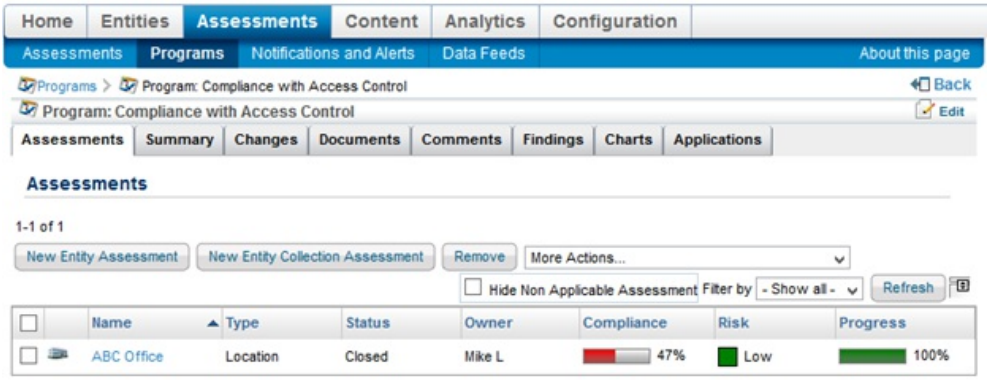
You can now compare the degree of overlap between the controls and sub-controls of the various frameworks and regulations that you need to comply with. You can also see the controls and sub-controls from which answers can be copied.

Example

To demonstrate the use of the Common Control framework, we will consider an assessment with the following details:

Program Name	Compliance with Access Control
Entity	ABC Office
Entity Owner	Mike L
Security Owner	John J
Controls in use	NIST SP 800-53 (2013) - AC-1 ACCESS CONTROL POLICY AND PROCEDURES - AC-11 SESSION LOCK - AC-12 SESSION TERMINATION

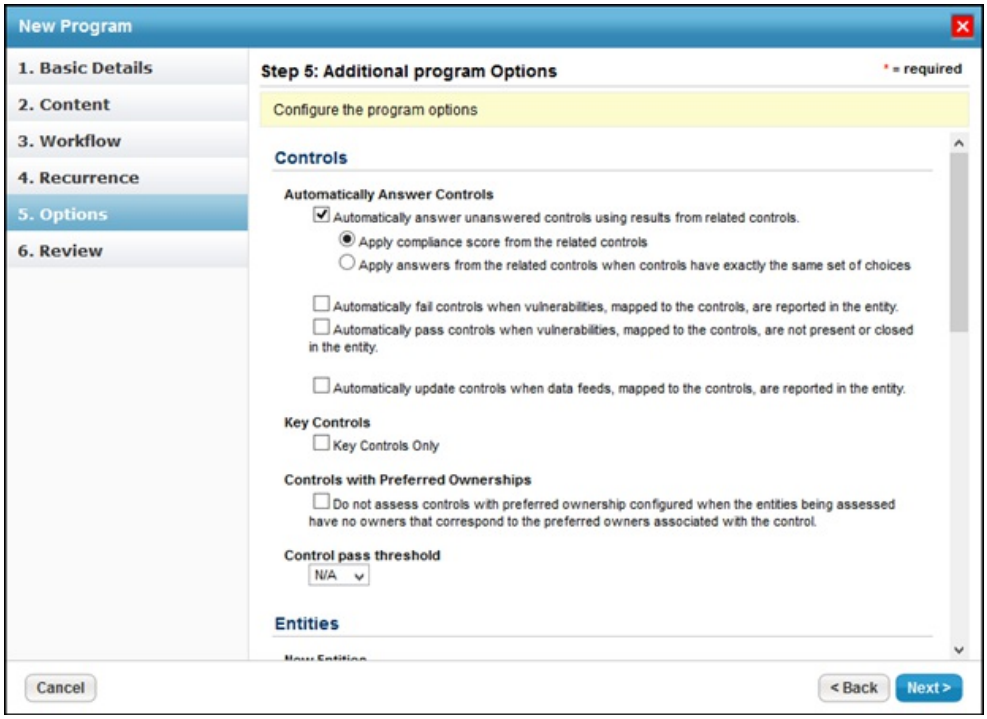
As an entity owner, Mike answers the questions from the above control. As the Security Owner, John approves the responses and sign's off the assessment. As a result, the compliance scores are calculated and the risk is determined.



Now we will create a new program with the following details:

Program Name	Access Control practices
Entity	ABC Office
Entity Owner	Mike L
Security Owner	John J

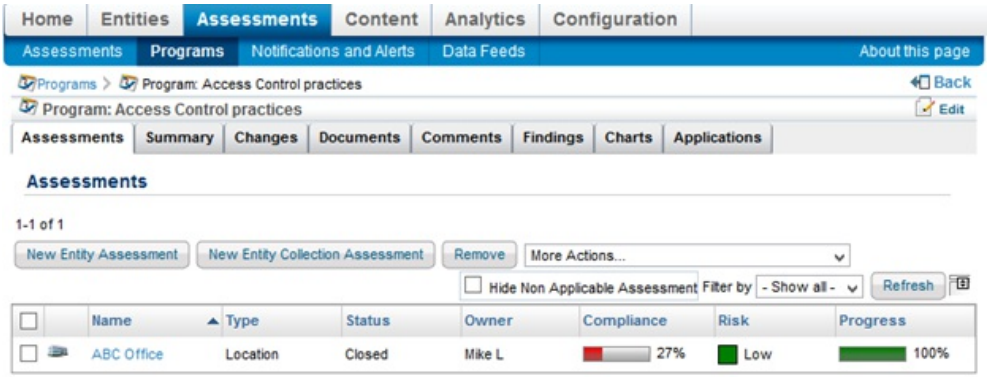
While creating the program, in the **Option's** tab of the **New Program** wizard, we will select **Automatically answer unanswered controls using results from related controls.**



This will ensure that if the questionnaire in the current program is not answered, the unanswered controls will use results from related controls that were answered in a different assessment. This is where the Common Controls Framework comes into use. If the controls overlap, then the responses used to answer controls in one assessment will be automatically re-used to answer controls in a different assessment.

- Selecting **Apply compliance score from the related controls** will make sure that responses from a related control are used to calculate the compliance scores.
- Selecting **Apply answers from the related controls when controls have exactly the same set of choices** will first validate if the same set of answer choices are used in the related controls and if yes, then they will be used as responses to the questionnaire.

Now, when the assessment using the control 'Access Control practices', moves through the workflow, and if it does not have responses to all the controls, responses from 'Compliance with Access Control' program will be used (since the controls are common and overlapping), to populate the compliance scores.



The option Apply answers from the related controls when controls work only when the controls have the same question text and the same set of choices. Common Control Framework works only with the combination of same question text and the same set of choices.

Importing Data

The first step after installing the RiskVision server is making the system aware of your organization's assets, users, vendors, and other entities. Importing the details of these system objects is a fast way to jump-start the system.

RiskVision provides a consistent mechanism for importing data from Microsoft Excel spreadsheets. The same mechanism is used to import:

- Users
- Assets or Entities (including Vendors)
- Questionnaires or Controls
- Findings
- Incidents
- Risks
- Entity Relationship

Working With Excel

An Excel file is called a workbook. Each workbook contains one or more worksheets. Each worksheet is represented by a tab along the bottom edge of the Excel spreadsheet window. To switch to another worksheet, click on its tab.

As with any spreadsheet, each worksheet represents a tabular grid — rows are numbered and columns are identified by letter. The upper left cell is referred to as A1.

RiskVision uses worksheets to separate the data to import from information about the data. A special worksheet, called a 'Map' worksheet describes the data to import. The actual data is on a different worksheet that can be called anything you'd like. A third sheet, Name Space, is a guide to available attributes, and is described later in this section.

The 'Map' worksheet has a specific format. On the first few rows, the Map describes the name of the data sheet, an optional Tag, and start and end row numbers for the data to be imported. The remainder of the Map worksheet lists attributes of the data being imported. For example, attributes of a User include firstName, lastName, and e-mail Address. For each attribute named in column A, a letter in column B identifies the column on the data worksheet that corresponds to the attribute. Column C provides an optional default value (to be used if the data for this attribute is missing), and column D is reserved for notes.

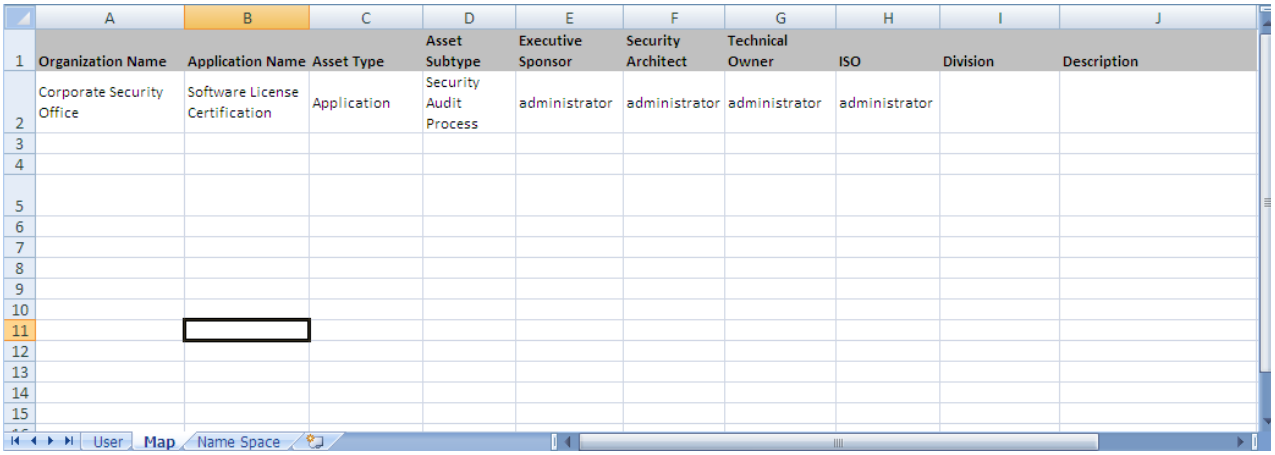
Some attributes are required, such as an entity's name, type, and primary owner (the user importing the data). Optional attributes for entities such as additional owners, location, classification, and organizational information, are useful for reporting and workflow-based assessment.

For example, assume that your data table is on a worksheet called 'User' and looks like this:

	A	B	C	D
1	**Asset Import Configuration**			
2	Data Sheet	Entity		
3	Object type	Vendor		
4	Start Row	2		
5	End Row	2		
6	**Attribute Name**	**Column**	**Default Value**	**Notes**
7	caption	B		
8	description	J		
9	name	B		
10	stage		1	The asset will be imported as "managed" asset
11	assetType	C	Vendor	
12	assetSubtype	D		
13	assetTag			
14	serialNumber			
15	model			
16	manufacturer			
17	version			
18	organization	A		
19	division	I		
20	subDivision			
21	classification.integrityImpact		5	
22	assetInformation.dataIntegrityCost		10	
23	ownerships.1.ownershipType.name		Primary Owner	
24	ownerships.1.ownerId	G		
25	ownerships.2.ownershipType.name		Security Owner	

User | Map | Name Space

In this case, your Map would look like this:



	A	B	C	D	E	F	G	H	I	J
1	Organization Name	Application Name	Asset Type	Asset Subtype	Executive Sponsor	Security Architect	Technical Owner	ISO	Division	Description
2	Corporate Security Office	Software License Certification	Application	Security Audit Process	administrator	administrator	administrator	administrator		
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										

Notice that the data worksheet can include columns that are not imported (because the column is not specified in the Map). Conversely, not all attributes listed in the Map must be provided by the data worksheet.

Boolean values must be either "true" or "false." Other values, such as "Yes" "No", "1", or "0" will evaluate to false.

Multi-Valued Attributes

The attributes in the Map can have multiple values, although the example fields (such as 'firstName') refer to only zero or one column in the data worksheet. More complex values, such as `classification.integrityImpact`, are possible. Custom attributes are handled this way, for example: customAttributes.long1, customAttributes.string1, and so on.

When an object can have multiple values for a specific attribute, a similar notation is used. The object is said to have a one-to-many or many-to-many relationship with another object. A User object, for example, can have a relationship with more than one Role object. The user's 'roles' attribute can be multi-valued. While importing, roles are referenced by their name attribute. So, to specify more than one role for a User, the map file might include:

Attribute	Column	Default Value
roles.1.name	C	Analyst
roles.2.name	D	Administrator

This describes the situation where a User has two named attributes, both called 'roles'. This mechanism can be extended to multiple attributes, for example, `vendorServices.1.ownerships.1.ownershipType.name`. This example (from `EntityImportTemplate.xls`) refers to the first vendorServices associated with the asset. In this case, vendorServices can have multiple ownerships so we are assigning a value to the ownershipType.name of the first ownership of the first vendor service.

Provided Excel Spreadsheets

Several Excel files are provided for your use as examples or templates:

- EntityImportTemplate.xls – Use for importing entities
- UserImportTemplate.xls – Use for importing users
- ControlImportTemplate.xls – Use for importing controls
- RiskAssessmentImportTemplate.xls- Use for importing risks
- EntityRelationshipImportTemplate.xls - Use for importing entity relationships

To import data using Excel:

1. In the Administration application, go to Administration > Server Administration > Documentation.
2. Select the correct file for your data:

RiskVision object	Excel spreadsheet
Entity, Asset, Vendor	EntityImportTemplate.xls
User	UserImportTemplate.xls
Incident	IncidentImportTemplate.xls
Controls, Questionnaires	ControlImportTemplate.xls
Risk Assessment	RiskAssessmentImportTemplate.xls
Entity Relationship	EntityRelationshipImportTemplate.xls

   Click the file, such as UserImportTemplate.xls, to download.
3. Rename the downloaded file based on the type and scope of data.
4. Open the file in Excel.
5. Load the data to import into the data worksheet (e.g., 'User'). Overwrite the sample data provided.
6. Edit the map worksheet to indicate the data columns that represent each attribute. Make sure that the Data Sheet name matches the name of your data worksheet, and enter the startRow and endRow.
7. Save the Excel file.
8. In RiskVision, navigate to the appropriate page and select the Import action. Browse to the Excel file in your local directory and click **OK**.

If new data needs to be imported, or initial data arrives asynchronously, you can import the same type of data again.

Overview of Attributes

The import system requires a basic knowledge of RiskVision solution objects. Some object types, such as Assets describe generic objects. Base object types are specialized by new, derived types that have additional attributes. For example, the Device object type is derived from the Asset object type (a Device is a kind of Asset). A Device object has all the attributes of an Asset object with the addition of the firmwareVersion attribute.

The more complicated import templates (for example, `EntityImportTemplate.xls`) include a Name Space worksheet. In EntityImportTemplate.xls, the Asset type is shown, followed by the objects that derive from the Asset--Account, ApplicationSystem, and so on. Every attribute of Asset is listed with attribute name, attribute type, and cardinality for each. Additional attributes are similarly listed under each derived type. The available attributes for a derived type (such as Vendor) is an aggregation of the attributes for Asset (the base class) and the additional attributes of the derived type.

Attribute Name

On the Map worksheet, you can refer to attribute names in column A in order to define data columns and default values for each. Every attribute name on the Map worksheet must match the attribute name on the Name Space worksheet for the Object type declared at the top of the Map worksheet. To continue the example, to import Devices, you would specify an Object type of 'Device' and add a row for 'firmwareVersion' that maps that attribute to a particular data column and optionally provides a default value.

Note that there is no distinction between base object and derived object attribute names on the Map worksheet.

Attribute Types

Simple attributes types, like 'string,' 'timestamp,' boolean,' or 'number,' are easy to understand, (in their details, the simple types tend to follow Java examples and data ranges). Some attributes, however, are RiskVision objects by themselves. For example, the Asset type has an attribute named 'address' that has a type of 'Address.' The available attribute object types are also described on the Name Space worksheet. Attribute objects do not derive from the base object, as a general rule meaning an Address object is not a kind of Asset.

The Address object, in this example, has the attributes name, address, city, state, and so on. Therefore, to refer to the address's city on the Map worksheet, you would enter address and city. It is not possible to represent a RiskVision object in an Excel cell, so the subordinate object's attributes (name, address, city, etc., in this example) must be explicitly referenced. That is, you cannot map column 'B' on your data worksheet to simply 'address.' RiskVision would not know what to do with the data in column B.

Cardinality

Certain attributes can be multi-valued, as described above. This information is also documented on the Name Space worksheet. Cardinality refers to the number of each attribute for a given object. The cardinality of most attributes is 1, meaning each asset, for example, has one name, one description, and so on. When an attribute's cardinality is listed on the Name Space worksheet as 'n,' it means that the object can have any number of values, zero to 'n' in math terms.

When you refer to an attribute with a cardinality of 'n,' you must specify the attribute's index number, even if there is only one. To add one named tag to each imported Asset, for example, you would add assetTags.1.name on the Map worksheet, because the assetTags attribute has a cardinality of 'n.' You could refer to a second value, assetTags.2.name, or not. Because the attribute's cardinality is not 1, the index number is required or else assetTags.name would generate an error.

Import Content from Excel

While it is possible to create a content pack within RiskVision through the user interface, this can be a time-consuming process depending on the quantity of controls and subcontrols. To save time, users can import their own content packs into RiskVision using the Excel Content Pack Import Template.

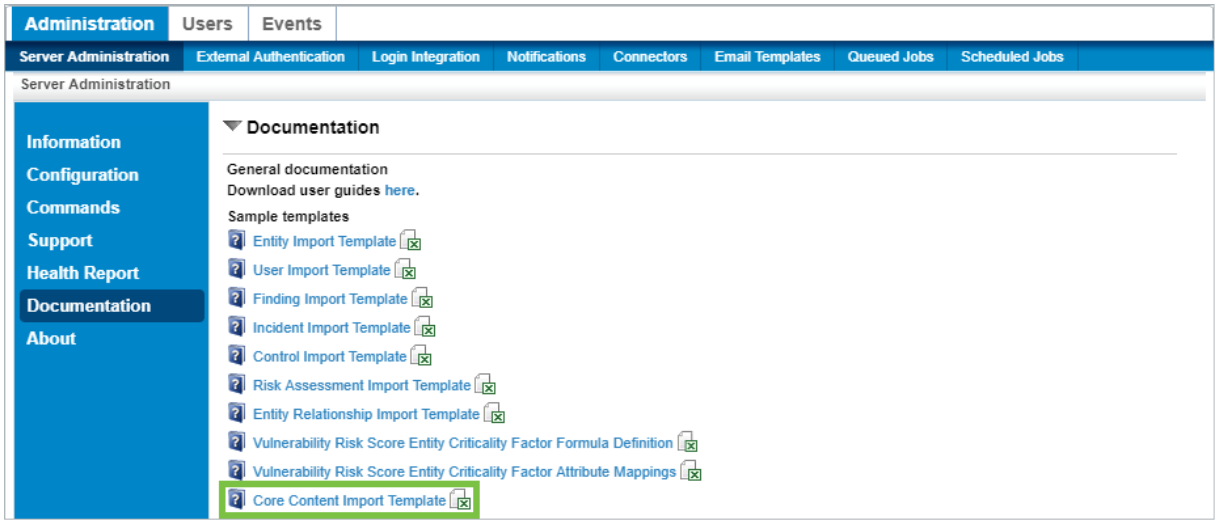
It is important to note that the content imported using this template must conform to the following structure:

- Content Pack
- Control Objective
- Control
- Subcontrol

If the imported content has a different structure, you may be able to change the content's structure after importing it. For example, control objectives can be changed to control groups by selecting the control objective in RiskVision and clicking the **Promote to Group** button.

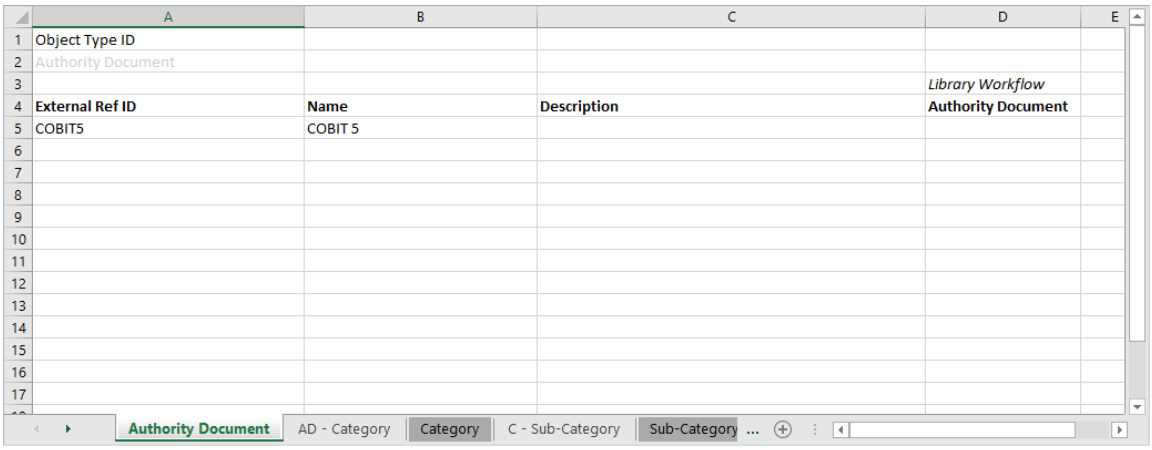
To import a content pack:

1. Navigate to the **Administration** application.
2. Click **Documentation** on the left side of the screen.
3. Click **Core Content Import Template** to download the import template.



The Core Content Import Template on the Documentation page.

4. Open the import template.
5. To create the content pack:
    a. Navigate to the **Authority Document** tab of the workbook.
    b. Enter the content pack's identifying code under **External Ref ID**. Users can enter an alphanumeric string including spaces and capitals with no character limit.
    c. Enter the content pack's name under **Name**.
    d. **Optional:** Enter a description for the content pack under **Description**.
    e. Leave the space under **Library Workflow** blank.



	A	B	C	D	E
1	Object Type ID				
2	Authority Document				
3				*Library Workflow*	
4	**External Ref ID**	**Name**	**Description**	**Authority Document**	
5	COBIT5	COBIT 5			

The Authority Document spreadsheet.

6. To create the control objectives:

    a. Navigate to the **Category** tab of the workbook.

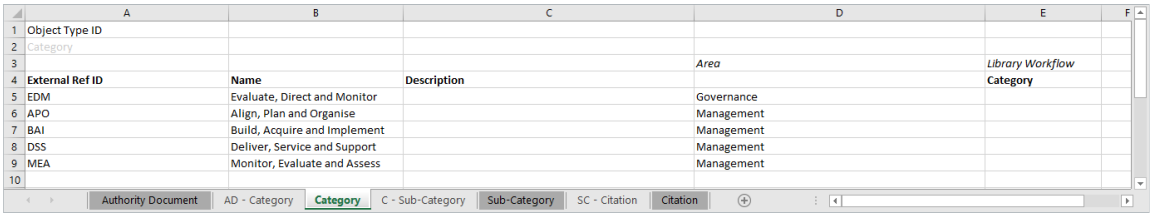
    b. Enter each control objective's identifying code under **External Ref ID**. Users can enter an alphanumeric string including spaces and capitals with no character limit.

    c. Enter the name of each control group under **Name**.

    d. **Optional:** Enter a description for each control group under **Description**.

    e. **Optional:** Enter the area each control group pertains to under **Area**.

    f. Leave the space under **Library Workflow** blank.



	A	B	C	D	E	F
1	Object Type ID					
2	Category					
3				*Area*	*Library Workflow*	
4	**External Ref ID**	**Name**	**Description**		**Category**	
5	EDM	Evaluate, Direct and Monitor		Governance		
6	APO	Align, Plan and Organise		Management		
7	BAI	Build, Acquire and Implement		Management		
8	DSS	Deliver, Service and Support		Management		
9	MEA	Monitor, Evaluate and Assess		Management		
10						

The Category spreadsheet.

7. To map control objectives to the content pack:

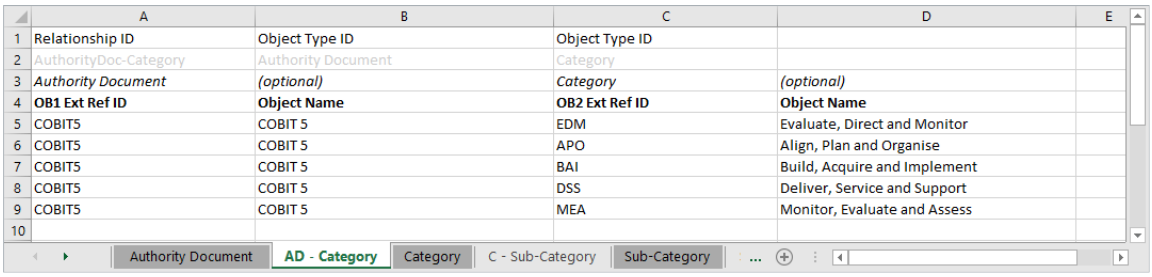
    a. Navigate to the **AD - Category** tab of the workbook.

    b. Enter the content pack's identifying code from step 5b under **OB1 Ext Ref ID**. Repeat this step as many times as there are control objectives to be mapped to the content pack. For example, if the content pack has five control objectives, enter the ref ID five times.

    c. **Optional:** Enter the name of the content pack under **Object Name** in column B. This is for user reference only.

    d. Enter the identifying code for each control objective from step 6b under **OB2 Ext Ref ID**.

    e. **Optional:** Enter the name of each control objective under **Object Name** in column D. This is for user reference only.



	A	B	C	D	E
1	Relationship ID	Object Type ID	Object Type ID		
2	AuthorityDoc-Category	Authority Document	Category		
3	*Authority Document*	*(optional)*	*Category*	*(optional)*	
4	**OB1 Ext Ref ID**	**Object Name**	**OB2 Ext Ref ID**	**Object Name**	
5	COBIT5	COBIT 5	EDM	Evaluate, Direct and Monitor	
6	COBIT5	COBIT 5	APO	Align, Plan and Organise	
7	COBIT5	COBIT 5	BAI	Build, Acquire and Implement	
8	COBIT5	COBIT 5	DSS	Deliver, Service and Support	
9	COBIT5	COBIT 5	MEA	Monitor, Evaluate and Assess	
10					

The AD - Category spreadsheet.

8. To create controls:

    a. Navigate to the **Sub-Category** tab of the workbook.

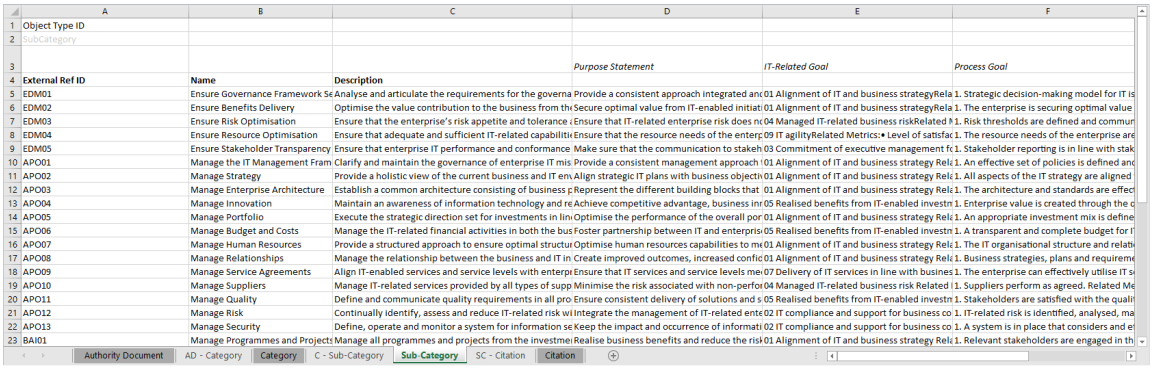
    b. Enter each control's identifying code under **External Ref ID**. Users can enter an alphanumeric string including spaces and capitals with no character limit.

    c. Enter the name of each control under **Name**.

    d. **Optional:** Enter a description of each control under **Description**.

    e. **Optional:** Enter the **Purpose Statement**, **IT-Related Goal**, and **Process Goal** of each control under the appropriate column. The content of these fields will appear under the Sub-Category's description field in RiskVision.

    f. Leave the remaining columns blank.



	A	B	C	D	E	F
1	Object Type ID					
2	SubCategory					
3				*Purpose Statement*	*IT-Related Goal*	*Process Goal*
4	**External Ref ID**	**Name**	**Description**			
5	EDM01	Ensure Governance Framework Se	Analyse and articulate the requirements for the governa	Provide a consistent approach integrated anc	01 Alignment of IT and business strategyRela	1. Strategic decision-making model for IT is
6	EDM02	Ensure Benefits Delivery	Optimise the value contribution to the business from th	Secure optimal value from IT-enabled initiati	01 Alignment of IT and business strategyRela	1. The enterprise is securing optimal value
7	EDM03	Ensure Risk Optimisation	Ensure that the enterprise's risk appetite and tolerance	Ensure that IT-related enterprise risk does nc	04 Managed IT-related business riskRelated M	1. Risk thresholds are defined and commun
8	EDM04	Ensure Resource Optimisation	Ensure that adequate and sufficient IT-related capabiliti	Ensure that the resource needs of the enterp	09 IT agilityRelated Metrics:• Level of satisfac	1. The resource needs of the enterprise are
9	EDM05	Ensure Stakeholder Transparency	Ensure that enterprise IT performance and conformance	Make sure that the communication to stakeh	03 Commitment of executive management fc	1. Stakeholder reporting is in line with stak
10	APO01	Manage the IT Management Fram	Clarify and maintain the governance of enterprise IT mis	Provide a consistent management approach	01 Alignment of IT and business strategy Rela	1. An effective set of policies is defined and
11	APO02	Manage Strategy	Provide a holistic view of the current business and IT en	Align strategic IT plans with business objecti	01 Alignment of IT and business strategy Rela	1. All aspects of the IT strategy are aligned
12	APO03	Manage Enterprise Architecture	Establish a common architecture consisting of business p	Represent the different building blocks that	01 Alignment of IT and business strategy Rela	1. The architecture and standards are effect
13	APO04	Manage Innovation	Maintain an awareness of information technology and re	Achieve competitive advantage, business inr	05 Realised benefits from IT-enabled investm	1. Enterprise value is created through the c
14	APO05	Manage Portfolio	Execute the strategic direction set for investments in lin	Optimise the performance of the overall por	01 Alignment of IT and business strategy Rela	1. An appropriate investment mix is define
15	APO06	Manage Budget and Costs	Manage the IT-related financial activities in both the bus	Foster partnership between IT and enterpris	05 Realised benefits from IT-enabled investm	1. A transparent and complete budget for I
16	APO07	Manage Human Resources	Provide a structured approach to ensure optimal structu	Optimise human resources capabilities to me	01 Alignment of IT and business strategy Rela	1. The IT organisational structure and relati
17	APO08	Manage Relationships	Manage the relationship between the business and IT in	Create improved outcomes, increased confic	01 Alignment of IT and business strategy Rela	1. Business strategies, plans and requireme
18	APO09	Manage Service Agreements	Align IT-enabled services and service levels with enterpr	Ensure that IT services and service levels me	07 Delivery of IT services in line with busines	1. The enterprise can effectively utilise IT s
19	APO10	Manage Suppliers	Manage IT-related services provided by all types of supp	Minimise the risk associated with non-perfor	04 Managed IT-related business risk Related I	1. Suppliers perform as agreed. Related Me
20	APO11	Manage Quality	Define and communicate quality requirements in all pro	Ensure consistent delivery of solutions and s	05 Realised benefits from IT-enabled investm	1. Stakeholders are satisfied with the qualit
21	APO12	Manage Risk	Continually identify, assess and reduce IT-related risk wi	Integrate the management of IT-related ente	02 IT compliance and support for business co	1. IT-related risk is identified, analysed, ma
22	APO13	Manage Security	Define, operate and monitor a system for information se	Keep the impact and occurrence of informati	02 IT compliance and support for business co	1. A system is in place that considers and e
23	BAI01	Manage Programmes and Projects	Manage all programmes and projects from the investmer	Realise business benefits and reduce the risk	01 Alignment of IT and business strategy Rela	1. Relevant stakeholders are engaged in th

The Sub-Category spreadsheet.

9. To map controls to control objectives:

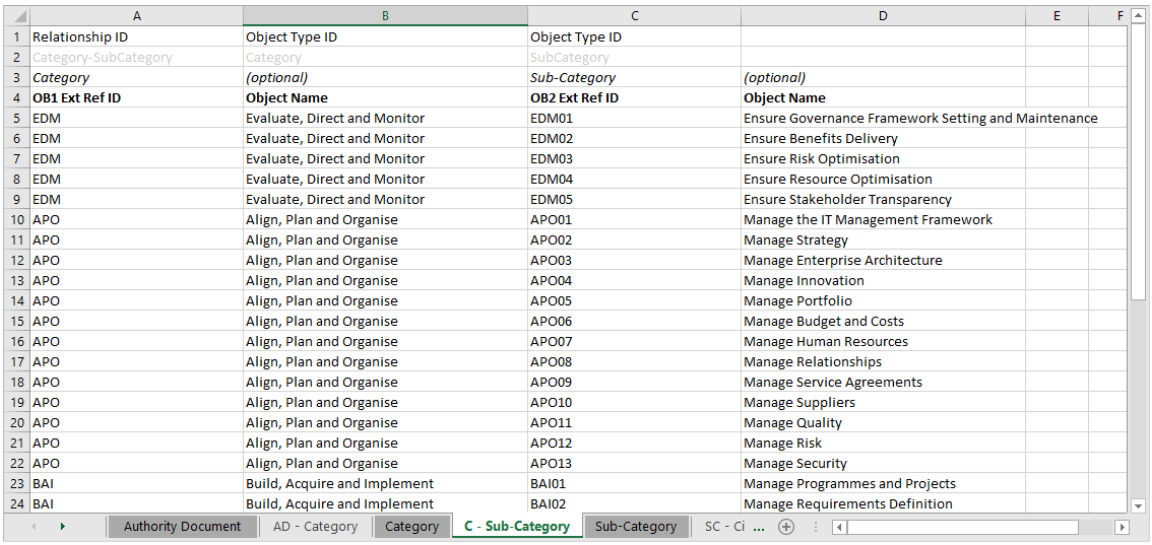
    a. Navigate to the **C - Sub-Category** tab of the workbook.

    b. Enter the identifying code for each control objective from step 6b under **OB1 Ext Ref ID**. Make a copy of each ID for every control being mapped to the control objective. For example, if the EDM objective contains five controls, enter EDM five times in the column.

    c. **Optional:** Enter the name of the control objective under **Object Name** in column B. This is for user reference only.

    d. Enter the identifying code for each control from step 8b under **OB2 Ext Ref ID**. Ensure each control is in the same row as its corresponding control objective.

    e. **Optional:** Enter the name of the control under **Object Name** in column D. This is for user reference only.



	A	B	C	D	E	F
1	Relationship ID	Object Type ID	Object Type ID			
2	Category-SubCategory	Category	SubCategory			
3	*Category*	*(optional)*	*Sub-Category*	*(optional)*		
4	**OB1 Ext Ref ID**	**Object Name**	**OB2 Ext Ref ID**	**Object Name**		
5	EDM	Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance		
6	EDM	Evaluate, Direct and Monitor	EDM02	Ensure Benefits Delivery		
7	EDM	Evaluate, Direct and Monitor	EDM03	Ensure Risk Optimisation		
8	EDM	Evaluate, Direct and Monitor	EDM04	Ensure Resource Optimisation		
9	EDM	Evaluate, Direct and Monitor	EDM05	Ensure Stakeholder Transparency		
10	APO	Align, Plan and Organise	APO01	Manage the IT Management Framework		
11	APO	Align, Plan and Organise	APO02	Manage Strategy		
12	APO	Align, Plan and Organise	APO03	Manage Enterprise Architecture		
13	APO	Align, Plan and Organise	APO04	Manage Innovation		
14	APO	Align, Plan and Organise	APO05	Manage Portfolio		
15	APO	Align, Plan and Organise	APO06	Manage Budget and Costs		
16	APO	Align, Plan and Organise	APO07	Manage Human Resources		
17	APO	Align, Plan and Organise	APO08	Manage Relationships		
18	APO	Align, Plan and Organise	APO09	Manage Service Agreements		
19	APO	Align, Plan and Organise	APO10	Manage Suppliers		
20	APO	Align, Plan and Organise	APO11	Manage Quality		
21	APO	Align, Plan and Organise	APO12	Manage Risk		
22	APO	Align, Plan and Organise	APO13	Manage Security		
23	BAI	Build, Acquire and Implement	BAI01	Manage Programmes and Projects		
24	BAI	Build, Acquire and Implement	BAI02	Manage Requirements Definition		

Authority Document | AD - Category | Category | C - Sub-Category | Sub-Category | SC - Ci ...

The C - Sub-Category spreadsheet.

10. To create subcontrols:

    a. Navigate to the **Citation** tab of the workbook.

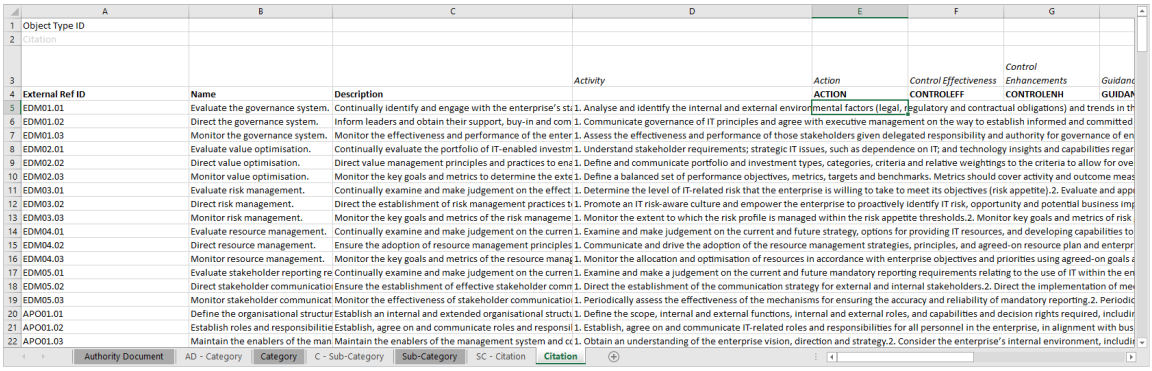
    b. Enter each subcontrol's identifying code under **External Ref ID**. Users can enter an alphanumeric string including spaces and capitals with no character limit.

    c. Enter the name of each subcontrol under **Name**.

    d. **Optional:** Enter the description of each subcontrol under **Description**.

    e. **Optional:** Enter the activities to be performed by each subcontrol under **Activity**. The content of these fields will appear under the subcontrol's description field in RiskVision.

    f. Leave the remaining columns blank.



	A	B	C	D	E	F	G
1	Object Type ID						
2	Citation						
3				*Activity*	*Action*	*Control Effectiveness*	*Control Enhancements*
4	**External Ref ID**	**Name**	**Description**		**ACTION**	**CONTROLEFF**	**CONTROLENH**
5	EDM01.01	Evaluate the governance system.	Continually identify and engage with the enterprise's sta	1. Analyse and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in th			
6	EDM01.02	Direct the governance system.	Inform leaders and obtain their support, buy-in and com	1. Communicate governance of IT principles and agree with executive management on the way to establish informed and committed			
7	EDM01.03	Monitor the governance system.	Monitor the effectiveness and performance of the enter	1. Assess the effectiveness and performance of those stakeholders given delegated responsibility and authority for governance of en			
8	EDM02.01	Evaluate value optimisation.	Continually evaluate the portfolio of IT-enabled investm	1. Understand stakeholder requirements; strategic IT issues, such as dependence on IT; and technology insights and capabilities regar			
9	EDM02.02	Direct value optimisation.	Direct value management principles and practices to ena	1. Define and communicate portfolio and investment types, categories, criteria and relative weightings to the criteria to allow for ove			
10	EDM02.03	Monitor value optimisation.	Monitor the key goals and metrics to determine the exte	1. Define a balanced set of performance objectives, metrics, targets and benchmarks. Metrics should cover activity and outcome meas			
11	EDM03.01	Evaluate risk management.	Continually examine and make judgement on the effect	1. Determine the level of IT-related risk that the enterprise is willing to take to meet its objectives (risk appetite).2. Evaluate and appl			
12	EDM03.02	Direct risk management.	Direct the establishment of risk management practices t	1. Promote an IT risk-aware culture and empower the enterprise to proactively identify IT risk, opportunity and potential business imp			
13	EDM03.03	Monitor risk management.	Monitor the key goals and metrics of the risk manageme	1. Monitor the extent to which the risk profile is managed within the risk appetite thresholds.2. Monitor key goals and metrics of risk			
14	EDM04.01	Evaluate resource management.	Continually examine and make judgement on the curren	1. Examine and make judgement on the current and future strategy, options for providing IT resources, and developing capabilities to			
15	EDM04.02	Direct resource management.	Ensure the adoption of resource management principles	1. Communicate and drive the adoption of the resource management strategies, principles, and agreed-on resource plan and enterpr			
16	EDM04.03	Monitor resource management.	Monitor the key goals and metrics of the resource manag	1. Monitor the allocation and optimisation of resources in accordance with enterprise objectives and priorities using agreed-on goals a			
17	EDM05.01	Evaluate stakeholder reporting re	Continually examine and make judgement on the curren	1. Examine and make a judgement on the current and future mandatory reporting requirements relating to the use of IT within the en			
18	EDM05.02	Direct stakeholder communicatio	Ensure the establishment of effective stakeholder comm	1. Direct the establishment of the communication strategy for external and internal stakeholders.2. Direct the implementation of me			
19	EDM05.03	Monitor stakeholder communicat	Monitor the effectiveness of stakeholder communicatio	1. Periodically assess the effectiveness of the mechanisms for ensuring the accuracy and reliability of mandatory reporting.2. Periodic			
20	APO01.01	Define the organisational structur	Establish an internal and extended organisational struct	1. Define the scope, internal and external functions, internal and external roles, and capabilities and decision rights required, includir			
21	APO01.02	Establish roles and responsibilitie	Establish, agree on and communicate roles and responsi	1. Establish, agree on and communicate IT-related roles and responsibilities for all personnel in the enterprise, in alignment with bus			
22	APO01.03	Maintain the enablers of the man	Maintain the enablers of the management system and c	1. Obtain an understanding of the enterprise vision, direction and strategy.2. Consider the enterprise's internal environment, includi			

Authority Document | AD - Category | Category | C - Sub-Category | Sub-Category | SC - Citation | Citation

The Citation spreadsheet.

11. To map subcontrols to controls:

    a. Navigate to the **SC - Citation** tab of the workbook.

    b. Enter the identifying code for each control from step 8b under **OB1 Ext Ref ID**. Make a copy of each ID for every sub-control being mapped to the control. For example, if EDM01 has three sub-controls, enter EDM01 three times in the column.

    c. **Optional:** Enter the name of the control under **Object Name** in column B. This is for user reference only.

    d. Enter the identifying code for each subcontrol from step 10b under **OB2 Ext Ref ID**. Ensure each subcontrol is in the same row as its corresponding control.

    e. **Optional:** Enter the name of each subcontrol under **Object Name** in column D. This is for user reference only.

	A	B	C	D	E
1	Relationship ID	Object Type ID	Object Type ID		
2	SubCategory-Citation	SubCategory	Citation		
3	*Sub-Category*	*(optional)*	*Citation*	*(optional)*	
4	**OB1 Ext Ref ID**	**Object Name**	**OB2 Ext Ref ID**	**Object Name**	
5	EDM01	Ensure Governance Framework Setting and M	EDM01.01	Evaluate the governance system.	
6	EDM01	Ensure Governance Framework Setting and M	EDM01.02	Direct the governance system.	
7	EDM01	Ensure Governance Framework Setting and M	EDM01.03	Monitor the governance system.	
8	EDM02	Ensure Benefits Delivery	EDM02.01	Evaluate value optimisation.	
9	EDM02	Ensure Benefits Delivery	EDM02.02	Direct value optimisation.	
10	EDM02	Ensure Benefits Delivery	EDM02.03	Monitor value optimisation.	
11	EDM03	Ensure Risk Optimisation	EDM03.01	Evaluate risk management.	
12	EDM03	Ensure Risk Optimisation	EDM03.02	Direct risk management.	
13	EDM03	Ensure Risk Optimisation	EDM03.03	Monitor risk management.	
14	EDM04	Ensure Resource Optimisation	EDM04.01	Evaluate resource management.	
15	EDM04	Ensure Resource Optimisation	EDM04.02	Direct resource management.	
16	EDM04	Ensure Resource Optimisation	EDM04.03	Monitor resource management.	
17	EDM05	Ensure Stakeholder Transparency	EDM05.01	Evaluate stakeholder reporting requirements.	
18	EDM05	Ensure Stakeholder Transparency	EDM05.02	Direct stakeholder communication and reporting.	
19	EDM05	Ensure Stakeholder Transparency	EDM05.03	Monitor stakeholder communication.	
20	APO01	Manage the IT Management Framework	APO01.01	Define the organisational structure.	
21	APO01	Manage the IT Management Framework	APO01.02	Establish roles and responsibilities.	
22	APO01	Manage the IT Management Framework	APO01.03	Maintain the enablers of the management system.	
23	APO01	Manage the IT Management Framework	APO01.04	Communicate management objectives and direction.	
24	APO01	Manage the IT Management Framework	APO01.05	Optimise the placement of the IT function.	

... | AD - Category | Category | C - Sub-Category | Sub-Category | SC - Citation | Citation

The SC - Citation spreadsheet.

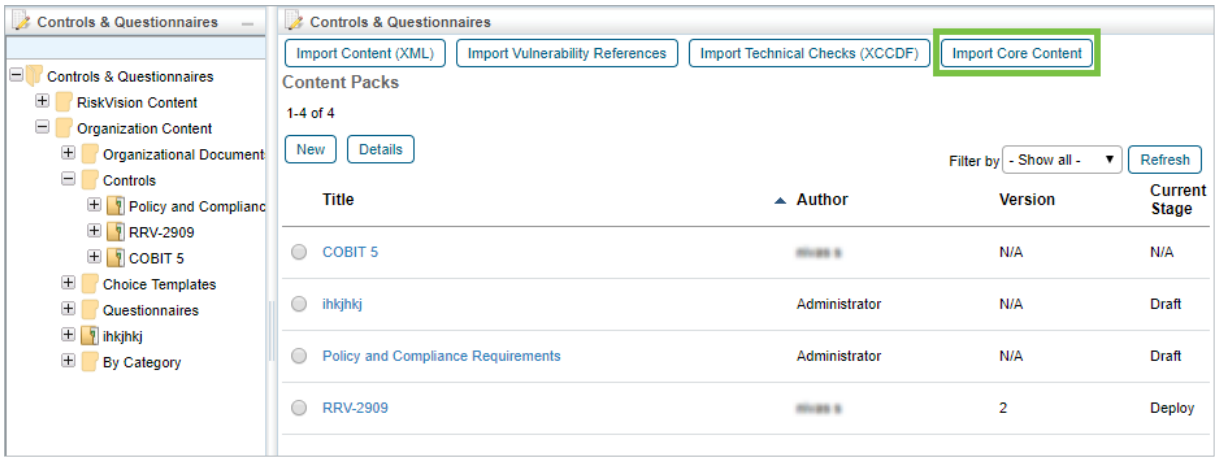
12. Navigate to the **server\config\agiliance.properties** file and place the following property:

```
ui.import.coreContent=true
```

> Skip step 12 if the property has already been placed in the file.

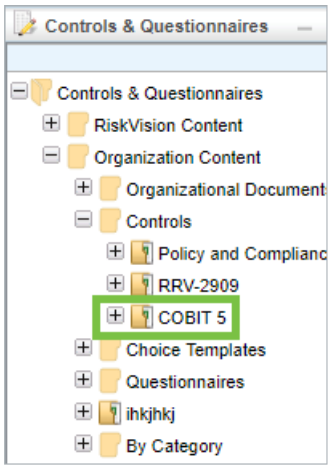
13. In RiskVision, navigate to **Content** > **Controls and Questionnaires**.

14. Click **Import Core Content**.



The Import Core Content button.

15. The imported content pack can be accessed under **Organization Content** > **Controls** in the tree view.



The newly imported content pack.

Entity Import Template

The table below lists the attributes available for importing entities and entity collections:

Attribute	Description
*caption	Enter the name of an entity.
description	Any additional information that helps understand the purpose of creating an entity.
*name	Specify the name of an entity.
stage	Enter '1' to import an entity as managed.
*assetType	Specify the type of an entity.
assetSubtype	The entity subtype.
assetTag	Specify a label for an entity.
serialNumber	Specify the serial number of an entity. Not all entity types contain the Serial Number attribute.
model	Specify the model number of an entity. Not all entity types contain the Model attribute.
manufacturer	Specify the manufacturer of an entity. Not all entity types contain the Manufacturer attribute.
version	Specify the version number of an entity. Not all entity types contain the Version attribute.
organization	Specify the name of an organization that owns an entity.
division	Specify the name of a division that owns an entity.
subDivision	Specify the name of a sub division if a particular division is composed of separate parts.
classification.integrityImpact	Specify the impact affecting the integrity.
assetInformation.dataIntegrityCost	Specify the cost involved in maintaining the data integrity.
ownerships.1.ownershipType.name	Specify the owner's name for the ownership type.
ownerships.1.ownerId	Specify the owner ID for an entity owner.

Attribute	Description
ownerships.1.teamownerId	Specify the team owner ID for an entity owner .
addressLinks.1.addressType.name	Specify the name of the address type, such as permanent address and billing address, to help indicate the preferred mode of communication.
addressLinks.1.address.name	Specify the name of the address to help locate an entity.
addressLinks.1.address.country	Specify the name of the country.
tags.1.name	Enter the name of the tag.
tags.1.category	The name of the category with which you will group common entities.
tags.1.description	Any additional information that will help demonstrate the purpose of creating a tag.
hierarchies.1.hierarchyType	Specify the organization hierarchy type.
hierarchies.1.description	Specify any additional information that will help understand the purpose of creating an organization hierarchy.
hierarchies.1.level1	Specify the first level of organization hierarchy.
hierarchies.1.level2	Specify the second level of organization hierarchy.
hierarchies.1.level3	Specify the third level of organization hierarchy.
vendorServices.1.name	Specify the name of the vendor service.
vendorServices.1.defaultFlag	Enter '1' to import vendor service as Default.
vendorServices.1.serviceType	Specify the type of the vendor service.
vendorServices.1.ownerships.1.ownershipType.name	Specify the owner for the ownership type of a vendor service.
vendorServices.1.ownerships.1.ownerId	The owner ID of the vendor service owner.

1. Organization hierarchy must be available in the Vendor Risk Manager prior to importing of Vendor Contact.
2. Enter '1' in the vendorServices.1.stage attribute field to import as managed vendor services.

User Import Template

The table below lists the attributes available for importing users:

Attribute	Description
address	Specify the user's address
city	Specify the user's city.
country	Specify the user's country.
*emailAddress	Specify the user's email address.
externalAuthenticationFlag	Specify '0' to import the users as internal.
fax	Specify the user's fax number.
*firstName	Specify the user's first name.
*lastName	Specify the user's last name.
localeCountry	Specify the user's country of origin.
localeLanguage	Specify the user's native language.
managerUserId	Specify the manager's user ID to whom a user is reporting.
middleinitial	Specify the initial letter of the user's middle name.
mobile	Specify the mobile number of the user.
passwordFromClear	Specify '1' to force the user to change the password when logging in for the first time.
phone	Specify the alternate contact number.
role.1.name	Specify the role so that the user(s) can access the RiskVision application based on that role.
state	Specify the user's state.
timezone	Specify the time zone in which the user will access the RiskVision application.
userAgreementAcceptedFlag	Enter '1' to automatically accept the user agreement on behalf of user.
userGroups.1.name	Assign the user to the team specified here.
*userid	Specify the user ID that will be used for login purposes.
vendor.name	Specify the vendor's name.

Attribute	Description
zip	Specify the user's zip code.

Finding Import Template

The table below lists the attributes available for importing findings:

Attribute	Description
*Name	Specify the name of the finding.
Control	Enter the title of the control to which you will associate a finding. When controls become non-compliant, you can specify for which controls the findings should be created.
Status	Enter the status of the finding when imported into the RiskVision application. Leaving this field blank will set the status to 'Open.'
Description	Any additional information that helps understand the purpose of creating a finding.
*Likelihood	Specify a value between 0 and 10 to provide an opinion as to how often the finding occurs. The value you specify here fetches a likelihood rating based on the threshold range configured on the Findings Configuration page.
*Impact	Specify a value between 0 and 10 to provide an opinion as to how the finding affects your organization. The value you specify here fetches an impact rating based on the threshold range configured on the Findings Configuration page.
Residual Likelihood	Specify a value between 0 and 10 to provide an opinion that after following certain procedures the chances of occurrence will subside. The value you specify here fetches an impact rating based on the threshold range configured on the Findings Configuration page.
Residual Impact	Specify a value between 0 and 10 to provide an opinion that if certain remediation procedures are followed the chances of occurrence will subside. The value you specify here fetches an impact rating based on the threshold range configured on the Findings Configuration page.
Owner	The owner is the user importing the findings into RiskVision application.
Team	Enter the team so that the finding can be worked on by a group of stakeholders.
Response Title	Enter the title for the response if you want to mitigate a finding using a response.
Response Action	Enter an action for the response. For example, if you are going to mitigate a finding's effect, the response action is usually set as 'Mitigate.'
Response Comment	Any additional information that helps understand the purpose of creating a response.
Response Owner	The user importing the findings into RiskVision application is the response owner.
Response	Enter the status of the response. Note that the status 'Implemented/Completed' mitigates the risk score of a finding.

Attribute	Description
Status	

Control Import Template

The table below lists the attributes available for importing controls:

Attribute	Description
ControlDescription	Any additional information that helps understand the purpose of creating a control.
ControlDescriptor	Enter the identifier of a control.
ControlGuidance	Provide detail information for the efficient use of a control.
ControlOtherInfo	Enter other details of a control. This information appears in the Other field of Additional Details tab, on the control details page.
ControlReference	Enter the reference numbers for organization or industry defined content. To enter multiple reference numbers, include the reference numbers in a comma-separated list.
ControlSubType	The specific characteristic that fall under the control type. The possible values are subcontrolSet, singleSubcontrol, and eGRC. By default, the value is 'subcontrolSet.' • Set 'subcontrolSet' if you want to import the 'Predefined Subcontrols' control type. • Set 'singleSubcontrol' if you want to import the 'Predefined Single Subcontrol' control type. • Set 'eGRC' if you want to import the 'Flexible Tests and Documentation' control type.
*ControlTitle	Enter the title for the control.
ControlType	The characteristic of the subcontrol that differs from a group of other controls. By default, the value is 'ControlPolicy.' The different types that can be specified are: Predefined Subcontrols, Predefined Single Subcontrol, and Flexible Tests and Documentation.
SubcontrolCheckType	Enter KRI if the controls to be imported are KRIs.
SubcontrolDescription	Any additional information that helps understand the purpose of creating a subcontrol.
SubcontrolDescriptor	Enter the identifier of the subcontrol.
SubcontrolFixText	Enter the remediation steps for the subcontrol.
SubcontrolFixType	Add the custom field 'Remediation Type' to view the type specified here.
SubcontrolMandatory	Enter '1' to import as key control.
SubcontrolPrimaryFlag	Enter '1' to import as key subcontrol.
SubcontrolQuestion	Enter the question for the subcontrol.
SubcontrolQuestionChoices	Enter the answer choices for the question.
SubcontrolQuestionHelp	Enter any information that will help the questionnaire responders to answer a question.

Attribute	Description
SubcontrolQuestionProcedure	Enter the assessment procedure for the question.
SubcontrolQuestionType	Specify the type to allow the stakeholders to input their answers. The type of questions that you can author are: Check Boxes, Text Box, Radio buttons, Table, and Time Series.
SubcontrolReference	Enter the reference numbers for organization or industry defined content.
SubcontrolTagCategory	Enter the name of the category using which you will group common subcontrols.
SubcontrolTagName	Enter the label to be assigned for the subcontrol.
*SubcontrolTitle	Enter the title for the subcontrol.
SubcontrolWeight	Enter a value between 0 and 1 to indicate the weight assigned to a control. When compliance and risk scores are rolled up, the values are calculated based on the percentage of a control's weight which contributes to the total weight of controls at the same level in a hierarchy.
KRAlpha	Specify the alpha value for the KRI.
KRBeta	Specify the beta value for the KRI.
KRCompositionMethod	Specify the method, such as Multiplication and Maximization.
KRICollectionFrequency	Specify the collection frequency, such as daily, weekly, and monthly for the KRI.
KRIMeasurementRules	Specify the measurement rules for the KRI.
KRINature	Specify the KRI nature.
KRIThresholdH0	Specify the threshold value for normal to medium risk (H0).
KRIThresholdH1	Specify the threshold value for medium to high risk (H1).
KRIType	Specify the KRI type.
KRIUnitOfMeasurement	Specify the unit of measurement, such as count, seconds, yen, dollars, and more.
KRIValueFormat	Specify the KRI format.
ControlWeight	Enter a value between 0 and 1 to indicate the weight assigned to a control. When compliance and risk scores are rolled up, values are calculated based on the percentage of a control's weight which contributes to the total weight of controls at the same level in a hierarchy.
Tags	Enter the label to be assigned for the control.

Risk Assessment Import Template

The table below lists the attributes available for importing risks:

Attribute	Description
*Permanent Id	Enter the unique ID for the risk.
Risk Category	Enter the category to group the risk.
Risk Description	Any additional information that helps understand the purpose of creating a risk.
Inherent Likelihood	Specify a value between 0 and 10 to provide an opinion as to how often a risk occurs.
Inherent Impact	Specify a value between 0 and 10 to provide an opinion as to how a risk will affect your organization.
Inherent Risk Score	The inherent risk score is calculated as inherent likelihood multiplied by inherent impact.
*Residual Likelihood	Specify a value between 0 and 10 to provide an opinion of whether after following certain remediation procedures the chances of risk occurrence in the future will subside or not.
*Residual Impact	Specify a value between 0 and 10 to provide your opinion of whetherafter following certain remediation procedures the risk's effect will subside or not..
Residual Risk Score	The residual risk score is calculated as residual likelihood multiplied by residual impact.
Risk Response1	Enter comments for the risk response.
Response1 Title	Enter the title for the response if you want to mitigate a finding using the response.
Response1 Startdate	Enter the date to begin remediating a risk.
Response1 Enddate	Enter the date by which you will complete the remediation process.
Response1 Status	The status of the response. Note that the status 'Implemented/Completed' mitigates the finding's risk score.

Entity Relationship Import Template

The table below lists the attributes available for importing relationships:

Attribute	Description
*Source Entity Name	Enter the name of an entity that needs a relationship.
*Source Entity Type	Enter the source entity type, such as computer, application, and entity collection.
*Target Entity Name	Enter the name of the entity to which the source entity is related.
*Target Entity Type	Enter the target entity type, such as computer, application, and entity collection.
*RelationshipType Name	The relationship that you will create between source and target entities.

The asterisk (*) symbol preceding the attributes are the required fields in the import templates.

Alternatives to Excel

You can create Users, Entities, and other objects manually in the RiskVision solution. In addition, connectors and third-party tools can import data into the system.

The Authentication connector, for example, can be used to import Users. Vulnerability scanners can be used to discover entities which RiskVision imports from the scan report. These entities are initially 'unmanaged,' meaning that they cannot be used in assessments.

Importing Entity Collections

Using the `EntityImportTemplate.xls` file, you can also import entity collections into RiskVision application.

Guidelines:

The following guidelines should be followed strictly when using the `EntityImportTemplate.xls` file to import entity collections.

1. Open the `EntityImportTemplate.xls` file, ensure that you are in the **Entity Map** sheet, and specify "EntityCollection" in the **Object type** and **assetType** fields. There can be no space between "Entity" and "Collection."
2. Go to the **Entity** sheet and enter "Entity Collection" in the **Asset Type**of each corresponding row. There must be a space between "Entity" and "Collection."

Importing entity collections will just import the entity collections and not its members. To import entities as members, you will once again need the `EntityImportTemplate.xls` file. Afterwards, you use the `EntityRelationshipImportTemplate.xls` file to import the Member of Entity Collection relationship type. For more information, see Importing Relationships. This procedure helps complete the process of importing entity collections and its members. You may want to visit the **Entities** tab of **Entity Collection** details page to ensure that entities you imported are available.

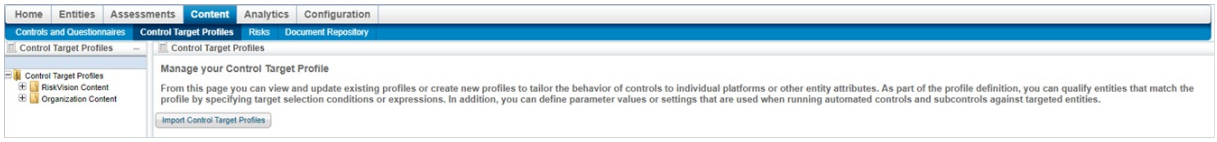
Creating a Control Target Profile

Control target profiles are sets of instructions that match up applicable controls and questions with entities based on their attributes. Users with **Profile View** and **Profile Author** permissions can create control target profiles and set which entities are targeted by introducing target conditions. Once created, the profile will be available for attachment.

Target conditions are not added at the creation phase of control target profiles. This means that newly created control target profiles will match all entities. To match profiles to specific entities, you must add target conditions as described in Configuring Target Selection Options.

To create a new control target profile:

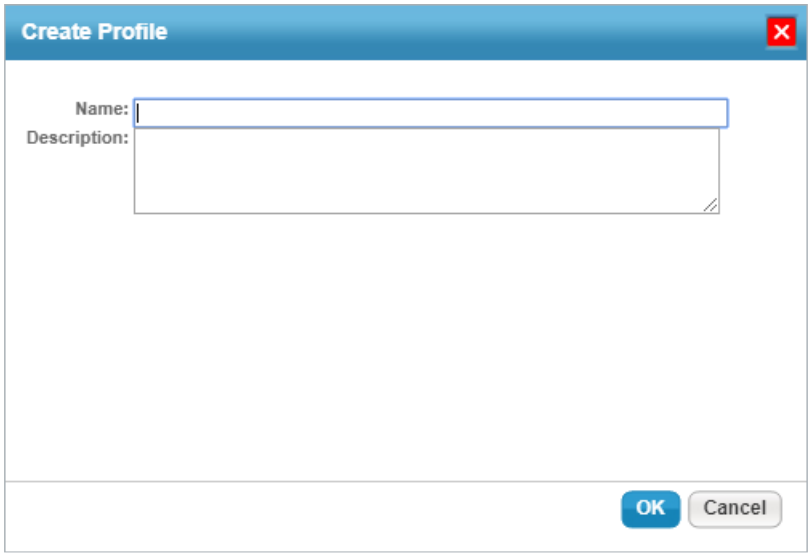
1. On the **Content** menu, click **Control Target Profiles**.



The Control Target Profiles screen.

2. Expand the **Organization Content** tree in the **Control Target Profiles** pane on the left hand side of the screen and select the group you wish to add the new profile to.

3. Click **New Profile** to display the **Create Profile** window.



The Create Profile window.

4. Enter a name for the control target profile in the **Name** field.

5. **Optional:** Enter a description of the control target profile in the **Description** field. Descriptions will appear next to the profile on the group's details page.

6. Click **OK**.

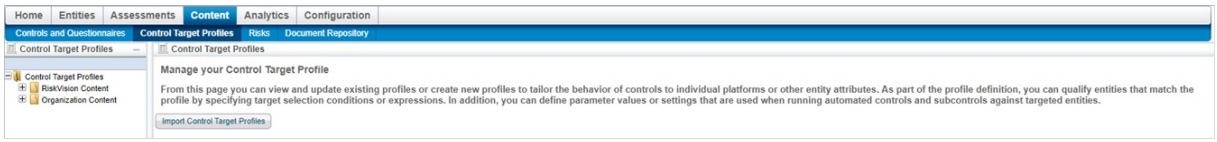
> ⚠ Control target profiles must be applied at the subcontrol level, rather than the control level. They will only apply at the control level if they have been applied to all of that level's subcontrols. Attaching a profile directly to the control level will result in the profile being lost at the control and subcontrols level. This means that only the subcontrols that were available before the creation of a control target profile will retain the profile.

Deleting Profile Control Target Profiles

Control target profiles can only be deleted by users with **Control Author** permissions if the user owns the profile and **Manage** permissions if the user does not own the profile. Furthermore, profiles can be deleted only if they have not been attached to any content. If you try to delete a profile that is currently in use, an error listing the content to which it is attached will appear.

To delete a profile:

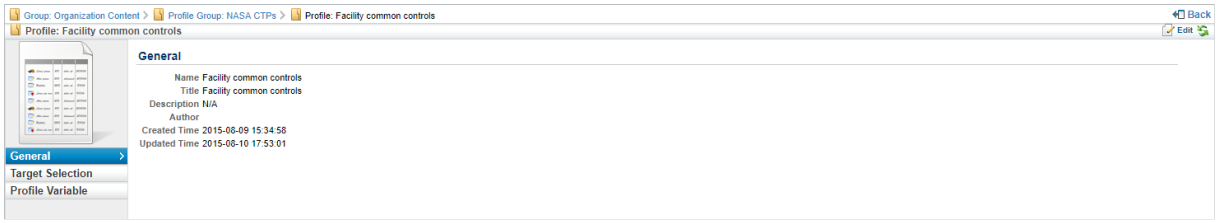
1. On the **Content** menu, click **Control Target Profiles**.



The Control Target Profiles screen.

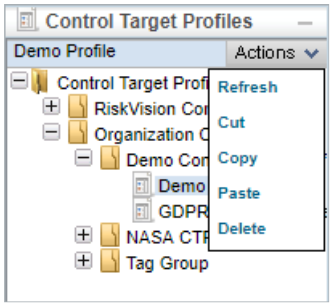
2. Expand the **Organization Content** tree in the **Control Target Profiles** pane on the left hand side of the screen and expand the group that contains the profile you wish to delete.

3. Select the profile to open its details page.



A control target profile's details page.

4. Click on the **Actions** dropdown menu at the top right of the **Control Target Profiles** pane and then click on **Delete**.



The Actions dropdown menu.

5. Click **OK**.

About Target Selection Options

The target set contains a set of conditions used by assessments to match content to entities. The following describes options on the target matching page:

- **Filter conditions.** Options for building operands.
- **Entity object.** Displays a list of entity types, entity (any type), Computer System (computer), and Account.
- **Field path.** Displays a list of available attributes for the type of entity object that you selected. The format is typically `tab_name.field_nam` where tab is the name of the tab on the entities detail page.
- **Comparison Op (operator)** Displays a list of logical operators that you can select to build a filter condition. SeeAbout Comparison Operators.
- **Value.** The string, number, or selection that you want to match.

About Comparison Operators

The following table describes the operators that you can use to match entity fields that contain any data type:

Operators	Description
==	Entity field exactly matches the value.
!=	Matches any entity field that does not exactly match the value.
contains	Entity field contains the exact phrase that you entered, for example: 'al' matchesalright and **minimal,**but not .
not-contains	Entity field does **NOT** contain the exact phrase that you entered. For example: 'al' matches,but not alright and minimal.
starts with	Entity field begins with the exact phrase that you entered. For example: 'al' matchesalright, but not minimal.
ends with	Entity field ends with the exact phrase that you entered, For example: 'al' matchesminimal, but not alright and minimal.
is-null	Matches entity field which has no value.
not null	Matches entity field which has any value that you entered.

The following table describes the operators that you can use to match entity fields that contain timestamps, integers, and short/long numbers:

Operators	Description
Greater than (>)	Entity field is higher than the number that you entered.
Greater than or equal (>=)	Entity field is the same or higher than the number that you entered.
Less than (<)	Entity field is lower than the number that you entered.
Less than or equal (<=)	Entity field is the same or lower than the number that you entered.

About Conjunctions

Join operands to create truth table as follows:

Conjunction	Description
AND	Returns true if all conditions are true, and false if any condition is false.
OR	Returns true if any condition is true, and false if all conditions are false.

RiskVision solution does not support mixing conjunction types in the same table.

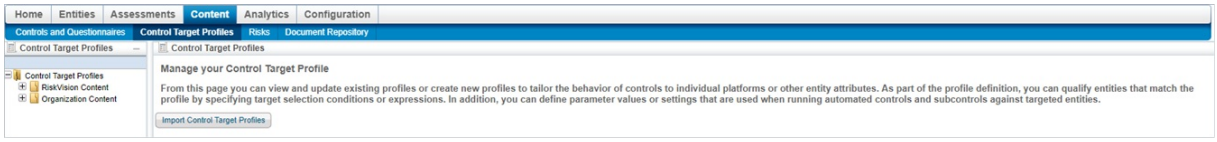
Configuring Target Selection Options

By setting a control target profile's target selection options, users can determine which entities the profile applies to. These changes are applied the next time the content completes a policy revision cycle. For existing programs, the change is applied after the content revision is completed and the program is manually synchronized.

Users with **Profile View** and **Profile Author** permissions can add, modify, or remove a target selection criteria associated with a profile.

To add a condition:

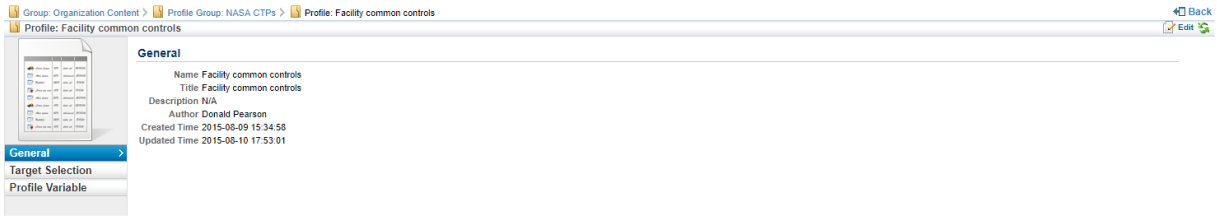
1. On the **Content** menu, click **Control Target Profiles**.



The Control Target Profiles screen.

2. Expand the **Organization Content** tree in the **Control Target Profiles** pane on the left hand side of the screen and select the group that contains the profile you wish to add the new target selection options to.

3. Select the profile to open its details page.



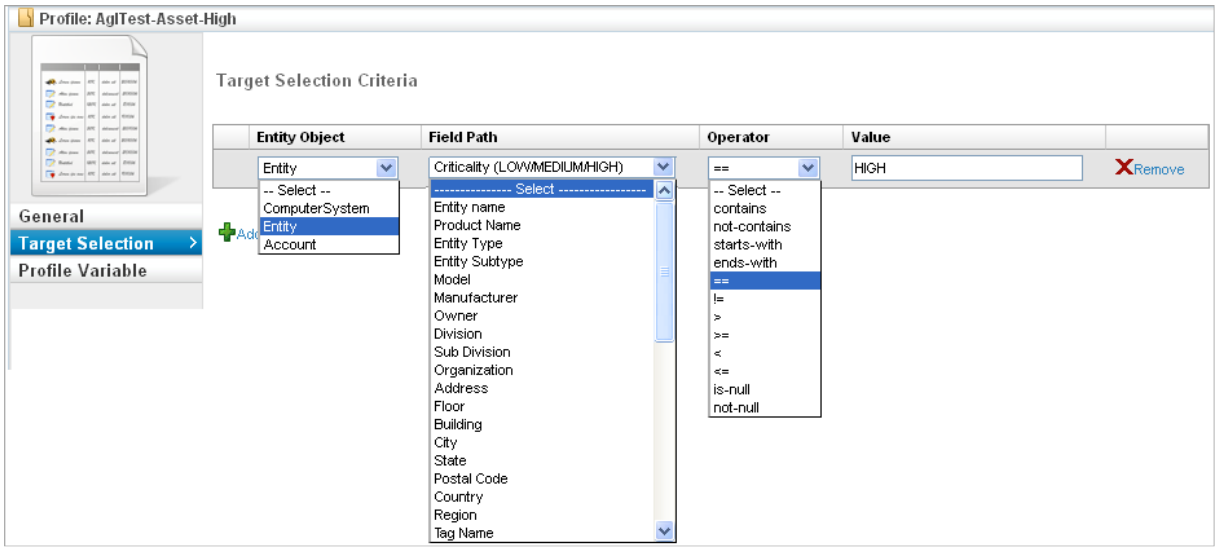
A control target profile's Details page.

4. Click the **Target Selection** tab, then click **Edit**.

5. Click **Add Condition**.

> If this is your first time adding any target selection criteria to a profile, you will not need to click **Add Condition**.

6. Enter the target conditions as follows:



The Edit Target Selection Criteria screen.

a. **Entity object**: Select the type of entity that you want to match.

b. **Field Path**: Select the entity field that you want to match.

c. **Operator**: Select an operator for the formula.

d. **Value**: Enter the value you wish to target.

e. **Conjunctions**: Joins conditions to build a joint expression that will help to narrow the target criteria. Select the same type for all conditions in filter.

   Use the attribute Matches filter to combine AND and OR expressions.

   If custom attributes have been added to an entity and a control target profile is in place, the content matches the entity in an assessment only when the selection criteria in that control target profile uses a combination of the following fields: custom strings, custom text, custom number, and custom dates.

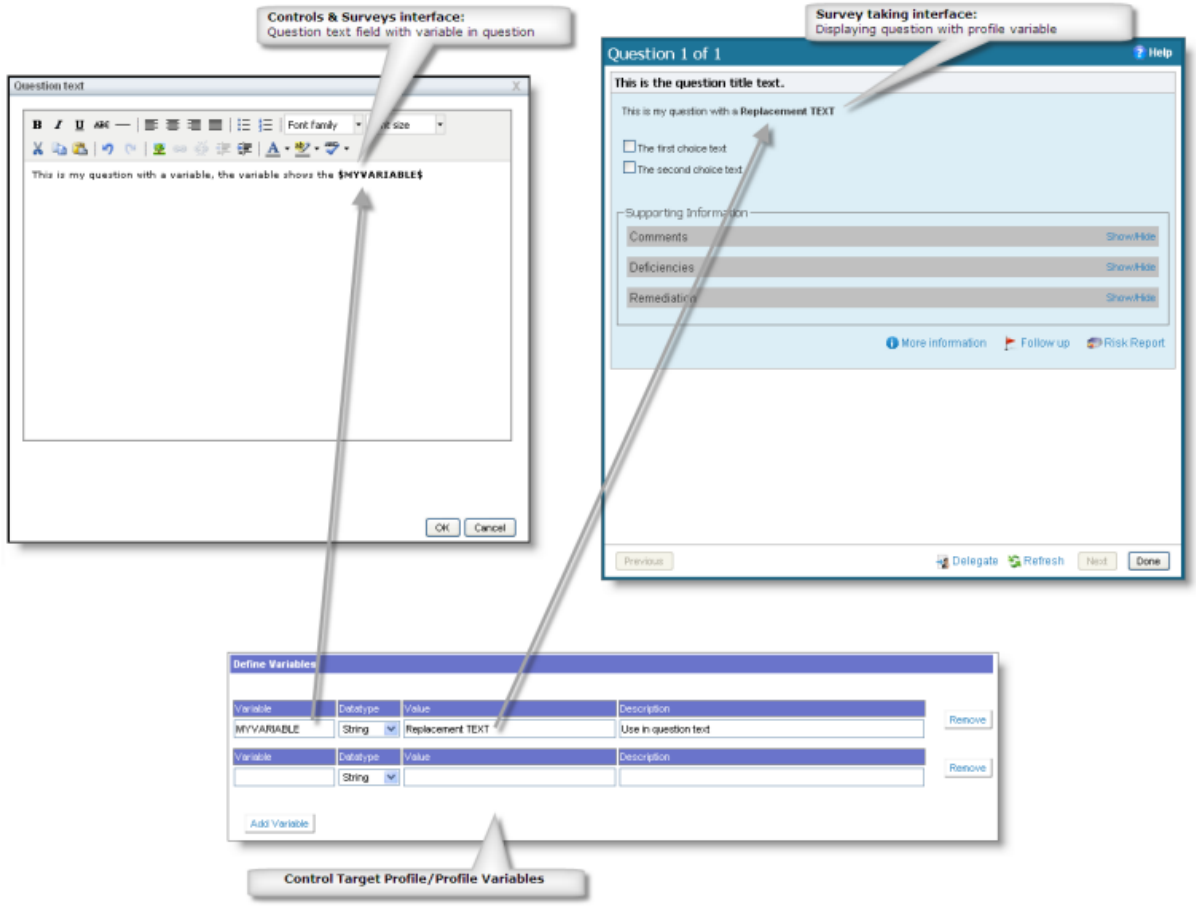
7. Click **Save**.

To remove a condition:

1. On the **Content** menu, click **Control Target Profiles**.
2. Expand the **Organization Content** tree in the **Control Target Profiles** pane on the left hand side of the screen and select the group that contains the profile you wish to remove a target selection option from.
3. Select the profile to open its details page.
4. Click the **Target Selection** tab, then click **Edit.**
5. Click **Remove** next to the condition(s) you wish to remove**.**
6. Click **Save**.

Configuring Profile Variables

Profile variables allow you to use a variable in the question text field. The questionnaire displays the defined variable value in place of the variable name. You must surround the variable name with '$', as shown in this example.

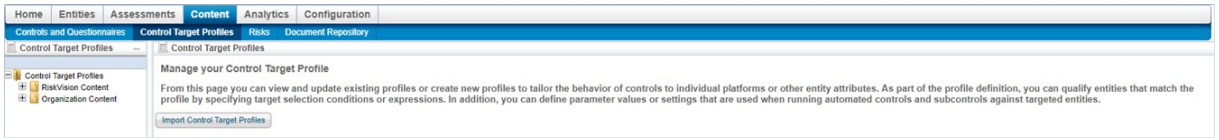


How variables work in questionnaires.

Users with **Profile View** and **Profile Author** permissions can add, modify, or remove a profile variable associated with a control target profile.

To add a variable:

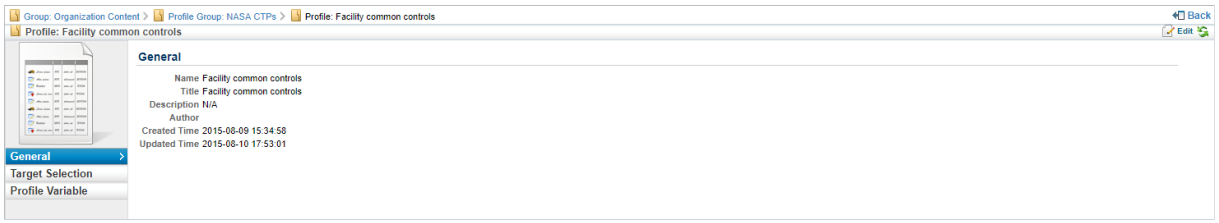
1. On the **Content** menu, click **Control Target Profiles**.



The Control Target Profiles screen.

2. Expand the **Organization Content** tree in the **Control Target Profiles** pane on the left hand side of the screen and expand the group that contains the profile you wish to add a variable to.

3. Select the profile to open its details page.



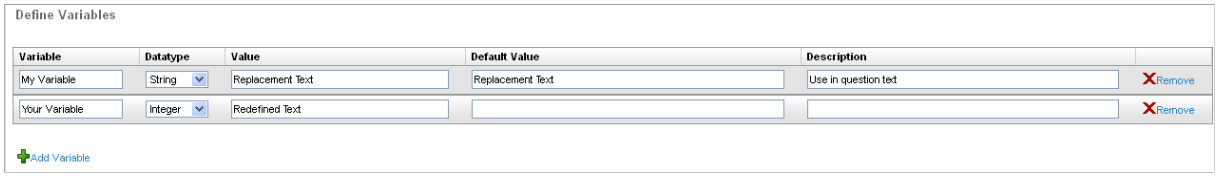
A control target profile's details page.

4. Click the **Profile Variables** tab, then click **Edit.**

5. Click **Add Variable**.

> If this is your first time adding any variables to a profile, you will not need to click **Add Variable**.

6. Enter the variable definition as follows:



The Define Variables screen.

1. **Variable**: Enter the name of the variable as it appears in the question text.
2. **Data type**: Select the type of data of the value.
3. **Value**: Enter the replacement information.
4. **Description**: Enter a summary.

7. Click **Save**.

To remove a variable:

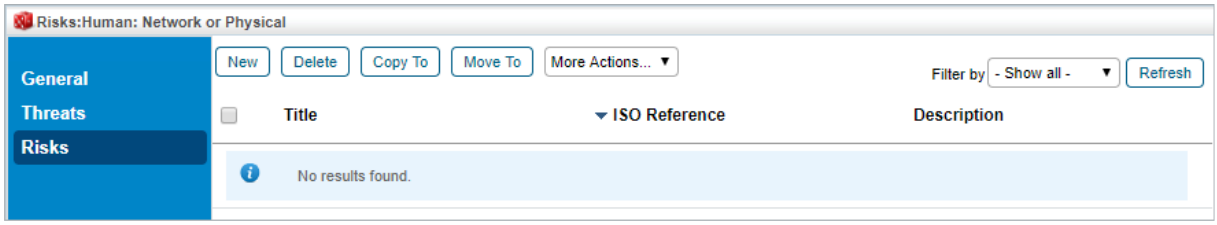
1. On the **Content** menu, click **Control Target Profiles**.
2. Expand the **Organization Content** tree in the **Control Target Profiles** pane on the left hand side of the screen and select the group that contains the profile you wish to remove a variable from.
3. Select the profile to open its details page.
4. Click the **Profile Variables** tab, then click **Edit.**
5. Click **Remove** next to the variable(s) you wish to remove.
6. Click **Save**.

Creating a New Risk

You can create a new risk if your user role has Risk View and Risk Author permissions.

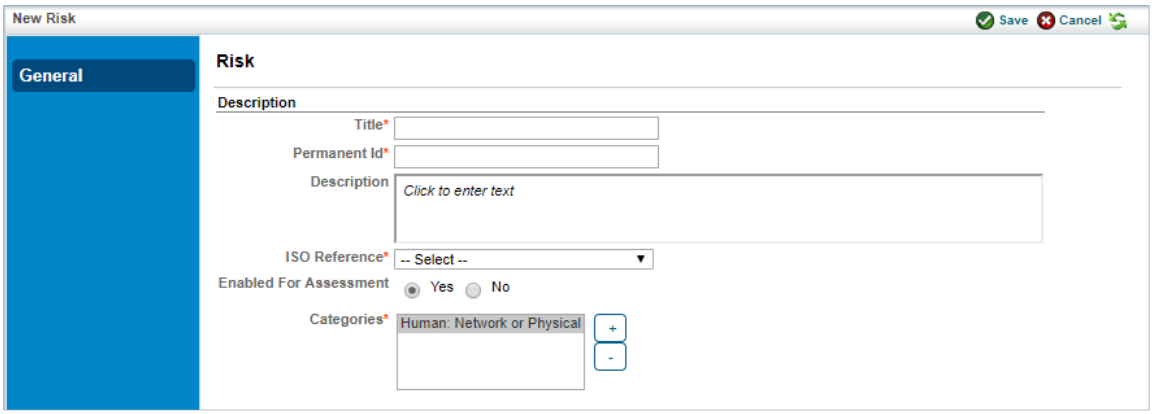
To create a new risk:

1. In the RiskVision Application application, go to **Content** > **Risks**.
2. Use the tree on the left to find **Risks & Threats** and under that, the risk category or ISO domain for the new risk. In the right-hand panel, click the **Risks** tab and then click **New**.



The Risks page.

3. Enter the following parameters and click **Save** (on the top bar):
   - **Title:** The risk's title, such as "Computer crime", or "Incomplete background checks".
   - **Permanent ID:** A unique identifier, such as "BR0031".
   - **Description:** A general description of the risk which can include styled text.
   - **ISO Reference:** Choose from one of the available options or define a new entry.
   - **Enabled for Assessment:** Choose **Yes** or **No**.
   - **Categories:** Select one or more categories from the category tree.



The New Risk screen.

Risk categories can be created or deleted using the **New Category**, **New Sub Category**, and **Delete Category** actions in the drop-down list associated with the **Risk Configuration** tree. The availability of these actions depends on the currently selected node in the **Risk Configuration** tree.

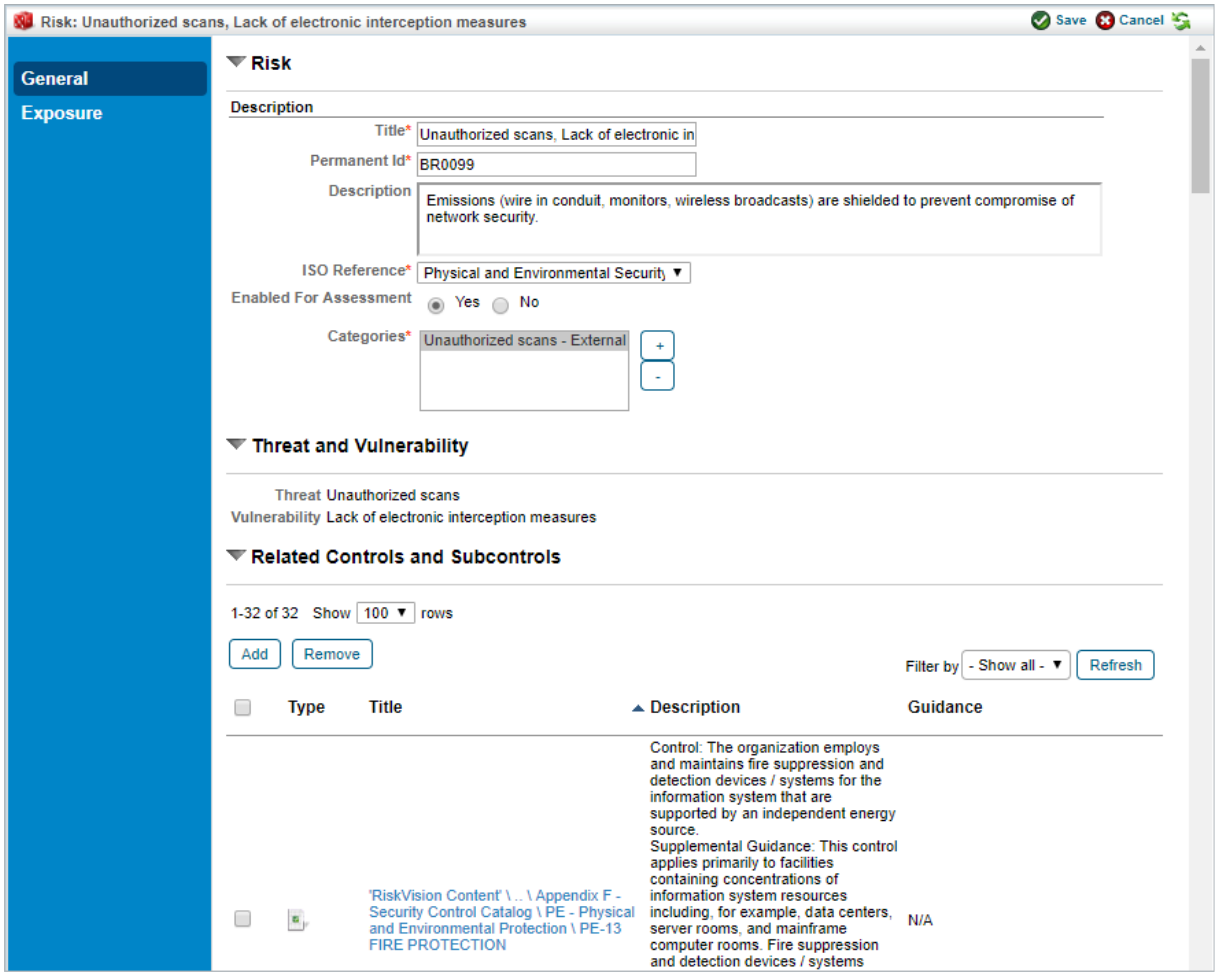
Despite the possibility of importing a risk with the Enabled For Assessment option set to 'No,' the risk will be applicable in risk assessment. When risks are imported using this setting, you must delete the risk or mark the risk as not applicable to drop them from assessments. For information about how to delete a risk or mark a risk as not applicable, see Understanding Risk Actions.

Associating Threats, Vulnerabilities And Controls With Risks

New risks are more meaningful if they are associated with threats, vulnerabilities, and controls. When your user role has Risk View and Risk Author permissions, you automatically obtain the access rights to update a risk so that threats and vulnerabilities can be associated, related controls can be added or removed, and fields in the Exposure tab can be updated.

To add threats or vulnerabilities to a risk:

1. In the RiskVision Application application, go to **Content** > **Risks**.
2. Find the desired risk in the tree on the left, open it, and click **Edit**.

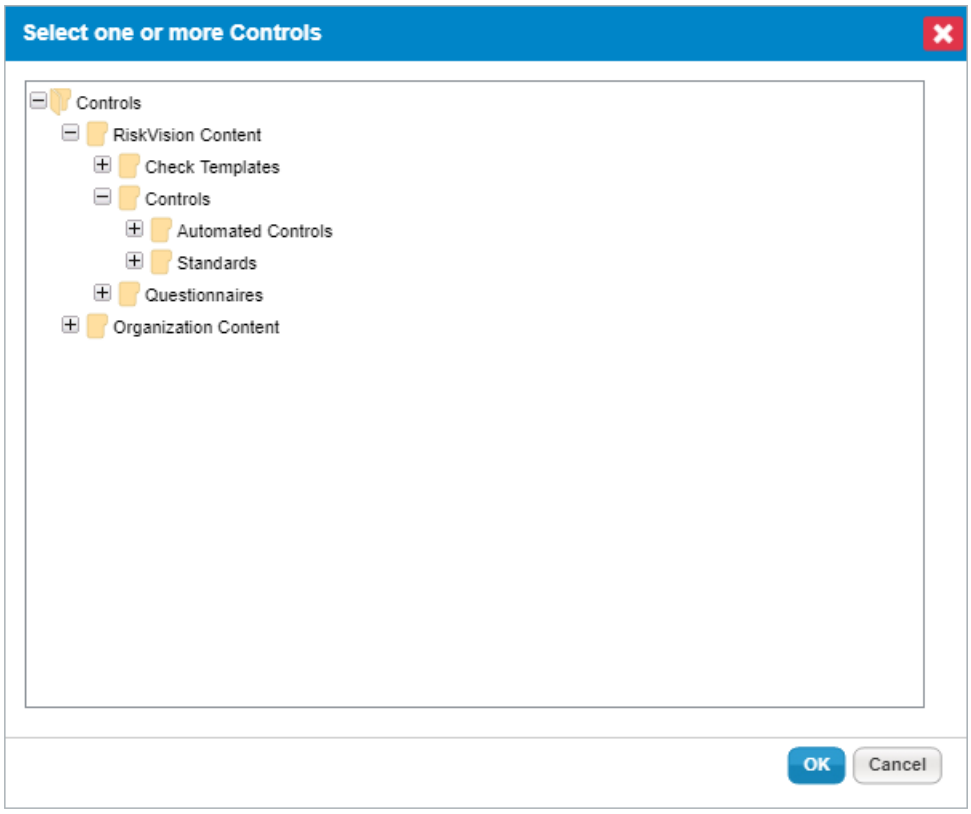


The Edit Risk Screen

3. To associate a threat with this risk, choose it from the **Threat** drop-down list. Likewise, to associate a vulnerability with this risk, make a selection from the **Vulnerability** drop-down list.
4. Click **Save**.

To relate controls and subcontrols to the new risk:

1. In the RiskVision Application application, go to **Content** > **Risks**.
2. Find the desired risk in the tree on the left, open it, and click **Edit**.
3. Under **Related Controls and Subcontrols**, click **Add** to bring up the **Control Selection** dialogue box. Find the desired control or subcontrol, select it, and click **OK**.



The Control Selection dialogue box.

4. In the **Risk General** Tab, click **Save**.

Understanding Risk Exposure

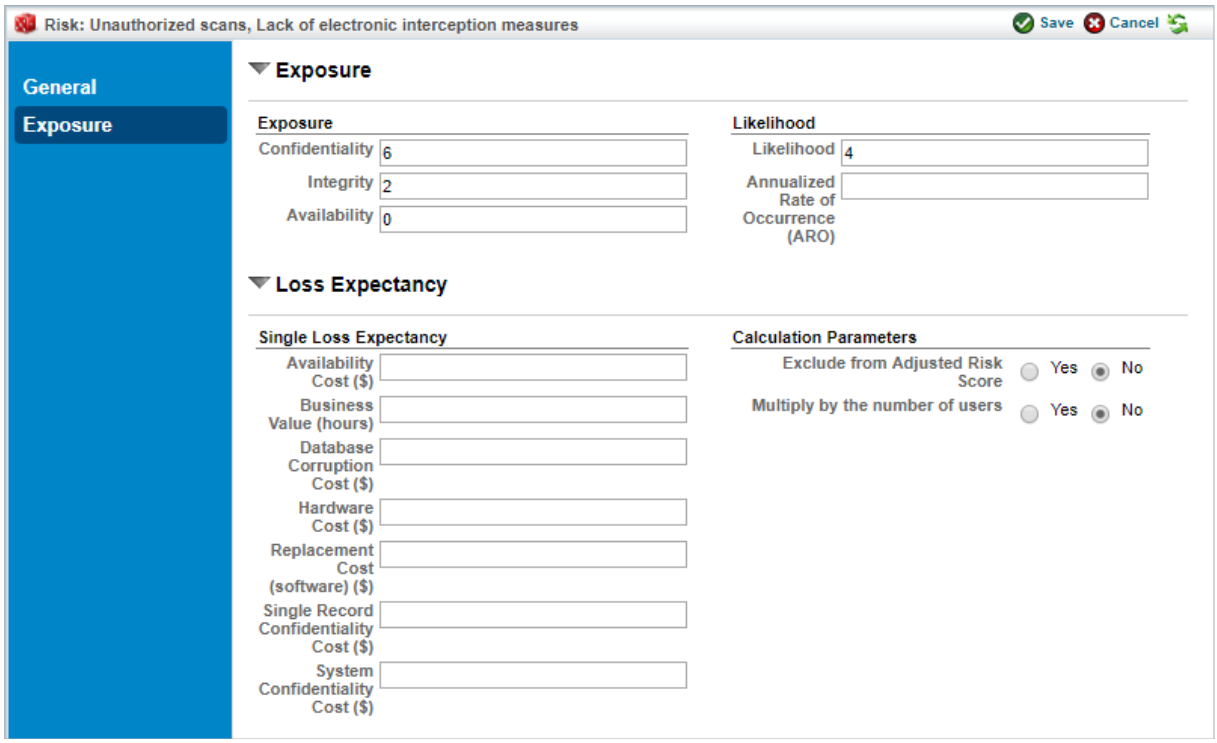
The organization's exposure to and loss expectancy from a single risk is important information.

Values specified in the likelihood and exposure fields drive the security risk scores in the application. RiskVision calculates overall risk based in part on single loss expectancy from a given risk. Risks can also be excluded from the Adjusted Risk Score.

Exposure values for Confidentiality, Integrity, and Availability (CIA) assess the impact of a risk. Likelihood specified the probability of a risk occurring. The overall risk score is calculated as likelihood x impact.

To specify a risk's exposure, likelihood, and loss expectancy:

1. In the RiskVision Application application, go to **Content** > **Risks**.
2. Open the desired risk in the tree on the left.
3. Click the **Exposure** tab, then click **Edit**.



The Edit Risk Exposure page.

4. Enter the following parameters:

Parameter	Description
Exposure	
Confidentiality	Risk of loss of confidentiality, 0 = no risk to 10 = maximum risk
Integrity	Risk of loss of data integrity, 0 = no risk to 10 = maximum risk
Availability	Risk of loss of availability of data, 0 =no risk to 10 = maximum risk
Likelihood	
Likelihood	Likelihood that this risk will affect the organization, 0 = extremely unlikely to 10 = certain
Annualized Rate of Occurrence (FRO)	How often is the vulnerability likely to be exploited in a year
Single Loss Expectancy	
Availability Cost	Cost in dollars, of not having the data available
Business Value	Affect in hours, on business operations

Database Corruption Cost	Cost, in dollars, of losing data integrity
Hardware Cost	Cost, in dollars, of new hardware and equipment
Replacement Cost	Cost, in dollars, of new software
Single Record Confidentiality Cost	Cost, in dollars, of loss of confidentiality for a single record (to be multiplied by the number of records)
System Confidentiality Cost	Cost, in dollars, of loss of confidentiality for the system as a whole
Calculation Parameters	
Exclude from Adjusted Risk Score	Yes to exclude this risk's exposure and likelihood from the overall risk score
Multiply by the number of users	Click yes to multiply loss expectancy number by the number of users affected

5. Click **Save**.

Creating a New Threat

If your user role contains the Risk View and Risk Author permissions, you can create, update, or delete a threat.

To create a new threat:

1. In the RiskVision application, go to **Risks** > **Risks**. In the RiskVision application, go to **Content** > **Risks**.
2. Use the tree on the left to find **Risks & Threats** and under that, the risk category or ISO domain for the new threat. In the right-hand panel, click the **Threats** tab, and then click **New**.
3. Enter the following fields:

Parameter	Description
Title	Title, such as 'Computer crime, Incomplete background checks'
Description	Can include styled text
Enabled for Assessment	Yes or No
Categories	Select one or more categories from the category tree

4. Click **Save**.

Risk categories can be created or deleted using the New Category, New Sub Category, and Delete Categoryactions in the drop-down list associated with the **Risk Configuration** tree. The availability of these actions depends on the currently selected node in the **Risk Configuration** tree.

Deleting a Risk

A user with sufficient privileges can delete a risk or threat.

To delete a risk:

1. In the RiskVision application, go to **Risks** > **Risks**. In the RiskVision application, go to **Content** > **Risks**.
2. Use the tree on the left to find the risk category or ISO domain containing the risk or threat to be deleted.
3. Click **Threats** or **Risks**and check the box next to the risk or threat to be deleted.
4. Click Delete.

Exporting Risks

An organization's risks, threats, and vulnerabilities can be exported as an XML file. This file can be edited and imported.

To export the Risk Configuration:

1. **In the RiskVision application, go to Risks > Risks. In the RiskVision application, go to Content > Risks.**
2. Choose the category of risks to be exported and click **Export in the Actions** drop-down list. Then select a local location for the XML file.

Importing Risks

An organization's risks, threats, and vulnerabilities can be imported from an XML file. To create an XML file in the correct format, start by exporting the Risk Configuration.

To import the Risk Configuration:

1. **In the RiskVision application, go to Risks > Risks.In the RiskVision application, go to Content > Risks.**
2. Click Import Risk Configuration. The **Import Risk Configuration** dialog appears.
3. Click **Browse**, select the file, and click **Open**.
4. Click **OK**. The risk configuration is imported.

Understanding Operational Vulnerabilities

An operational vulnerability is a potential risk that appears in the Risk Configuration > Operational Vulnerabilities tree. An operational vulnerability can be created only if your user role has Risk View and Risk Author permissions.

To create a Vulnerability:

1. In the RiskVision application, go to **Risks** > **Risks**. In the RiskVision application, go to **Content** > **Risks**.
2. Select **Operational Vulnerabilities** in the **Risk Configuration** tree.
3. Click **New**. Enter **Title**and **Description. Clicking to enter the text in the Description**field displays the **Description** dialog (rich-text editor). After entering the text, click **OK** to exit the **Description** dialog.
4. Click **Save**.

Understanding Risk Catalogs

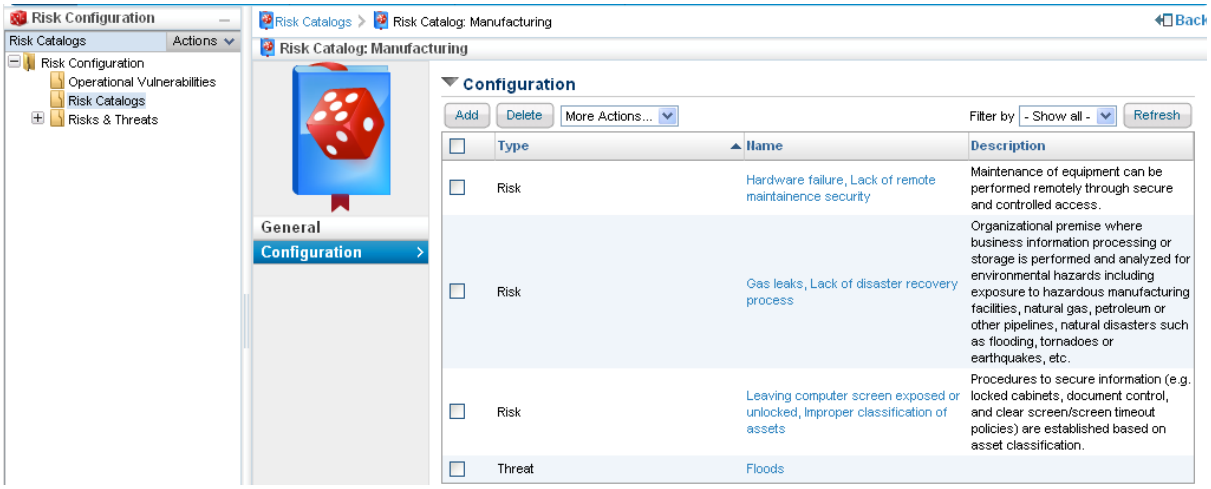
A Risk Catalog is a named group of threats and risks that appears in the Risk Configuration > Risk Catalogs tree, available on the . To create or update a risk catalog, you need to have the Risk View and Risk Author permissions.

To create a Risk Catalog:

1. In the RiskVision application, go to **Risks** > **Risks**. In the RiskVision application, go to **Content** > **Risks**.
2. Select **Risk Catalogs** in the **Risk Configuration** tree.
3. Click **New**. Enter **Name**and Description.
4. Click **Save**.

To associate risks and threats with a Risk Catalog:

1. **In the RiskVision application, go to Risks > Risks. In the RiskVision application, go to Content > Risks.**
2. Select **Risk Catalogs** in the **Risk Configuration** tree and select the risk catalog to open its details page.



3. Select the **Configuration** tab and click **Add**.
4. The **Select Risks/Threats** dialog appears. Expand the **Risks** tree, select the box next to threat(s) and/or risk(s) of interest, and then click **>>** to move the selected threat(s) and/or risk(s) to the **Risks/Threats** box.
5. Click **Apply**.

Risk Score Calculation Methods

When creating a risk program, there are three supported risk score calculation methods:

- Weighted Average
- High Water Mark
- Custom

Weighted Average:

Calculate the mean of a set of risk scores multiplied by pre-defined weights is the typical method for calculating a risk score. For example, imagine five entities, each with a weight of 1, except for one entity that has a weight of 0.5. The lower weight implies that the entity is less important than the others. A set of values might be { 6, 6, 5, 6, and 9 } and the last number is weighted 0.5. For this example, each value is multiplied by its weight:

6 * 1 = 6, 6 * 1 = 6, 5 * 1 = 5, 6 * 1 = 6, 9 * 0.5 = 4.5

6 + 6 + 5 + 6 + 4.5 = 27.5

The total (27.5) is divided by the number of values (5) to find the mean, so the weighted average is 27.5 / 5, or 5.5. Without weighting, the mean of the values would be 6.4. Weighting allows calculations to reflect the relative importance of different entities.

High Water Mark:

In some cases, the highest risk score is most important. The chain is no stronger than its weakest link. The high water mark method makes the risk score equal to the highest risk value in the set. Our example values {6, 6, 5, 6, and 9} would yield a risk score of 9. Because this method does not use weighting, it is most useful while aggregating risk scores for entities of similar importance.

Custom

Risk score calculation can be performed in an external script by specifying the script file in the .properties file, and by creating a script file that implements a specific Java interface in the Groovy language. (Groovy is syntactically similar to Java.)To get started, place the groovy script files in the *config / scripts* folder.

The default script used by the RiskVision system is a helpful reference for users who wants to customize the risk score:

`%AGILIANCE_HOME%\Tomcat\webapps\WEB-INF\classes\scripts\NgErmScriptupdater.groovy`

Treat this file as read-only; never modify files under the WEB-INF folder, because changes can be overwritten without warning.

To use a custom Groovy script for risk score calculations, add the following property to `%AGILIANCE_HOME%\config\agiliance.properties`:

ngerm.riskscore.update.groovy.source=file:%AGILIANCE_HOME%/server/config/NgErmScriptUpdater.groovy

To enable groovy ensure that the following property is configured as false

com.agiliance.web.risk.disableCustomRiskUpdaterGroovy=false

Provide the path to your script file (such as file : `D://main/config/scripts/MyRisk.groovy`). Implement the following methods:

- customLikelihoodValue(RAUserInput userInput)
- customImpactValue(RAUserInput userInput)
- customResidualLikelihoodValue(RAUserInput userInput)
- customResidualImpactValue(RAUserInput userInput)

You can also override these methods:

- calculateInherentRiskScore
- calculateCurrentRiskScore
- calculateResidualRiskScore

Your custom Groovy script must specify the following package and imports:

package com.agiliance.risk;

```
import java.util.Map;

import com.agiliance.common.ALException;

import com.agiliance.dal.model.LikelihoodDefinition;

import com.agiliance.dal.model.ImpactDefinition;

import com.agiliance.dal.model.RAUserInput;

import com.agiliance.risk.NgErmRiskUpdater;

import com.agiliance.risk.profile.BaseNgErmRiskUpdater;

import com.agiliance.risk.util.RAUtil;

import com.agiliance.common.log.AglLogger
```

Using the Document Repository

A document repository is used for storing critical documents, such as audit material, security plans and sensitive information pertaining to each domain in your organization. You can also refer stakeholders to useful information on the Internet or your intranet using web references. If your user role has sufficient permissions, you can upload files of any kind to share in the repository as well as you can refer to specific websites.

Typically, the document repository is available on the Content, Risks, or Administration menu in RiskVision application.

In addition to the shared document repository, documents and weblinks/ network paths can be uploaded and associated with various RiskVision objects, including entities, controls, programs, contracts, policy documents and so on. These objects have a **Documents** tab in their detail pages. The user permissions control the associated documents to view, upload, or perform any action.

Document Repository Structure

A document repository contains groups and document collections. Typically, a group represents a domain and a document collection is a container that can hold files, and web/ network path references. The document repository supports multiple file uploads of various file formats and image extensions. A user maintaining the document repository has to create at least one group or one document collection to upload documents. This enables you to store all the documents, web and network path references pertaining to your organization. However, creating a single group or document collection will grant other users unrestricted access to all documents, some of which are not relevant to their domain. Use groups to segregate documents based on specific domains, and then create separate groups and document collections within the top-level group with the ownership defined at the group or document collection level.

To support different file format extension, enable the following property `propertycom.agiliance.esapi.allowed.attachment.file.extensions=true.` Here the Default Value = true.

The lists of file formats supported by Document Repository are:

- PDF
- XLS
- XLSX
- DOC
- DOCX
- PPT
- PPTX
- TXT
- JPG
- JPEG
- PNG
- BMP
- MPP
- MPPX
- VSD
- VSDX
- MSG

Linkages for files attached directly to an object (e.g. to an assessment as evidence or to an entity, a finding, etc.) shall be maintained for files moved within the Document Repository. This consists of the following scenarios:

- When moving a file that is linked directly to an object from one Document Collection to another.
- When moving a Document Collection in which the file that was linked directly to an object resides from one Group to another.

Linkages for Document Collections attached directly to an object shall be maintained in the following scenarios:

- When moving a Document Collection into another Document Collection.
- When moving a Document Collection to a different group.

When a Document Collection is attached to an object and files are moved out of the Document Collection, these files shall no longer be linked to the objects they were previously linked to as a result of their membership in the Document Collection that they are no longer part of.

To create a group:

1. Open RiskVision Compliance Manager.
2. Go to **Content** > **Document Repository**.
3. Select the **Document Repository** node or locate a group, select to display its details, and then click **New Group**. The **New Group** dialog appears.
4. Enter **Name** and **Description.**
5. Click **OK**.

To create a Document Collection:

1. Open RiskVision Compliance Manager.
2. Go to **Content** > **Document Repository**.
3. Select the **Document Repository** node or locate a group, select to display its details and then click **New Document Collection**. The **New Document Collection** dialog appears.
4. Enter Name and Description.
5. Click **OK**.

Document Repository Ownership

The Reader and Writer document repository ownership roles control user access and limit the actions that can be performed by users in a document repository. Using a role, you can define an ownership at the group or document collection level.

Action	Ownership	Permission
Cut	Writer	View + Create + Update or Manage only
Paste	Writer	View + Create + Update or Manage only
Delete	Writer	View + Delete or Manage only
Move to	Writer	View + Create + Update or Manage only

Note: Users can attach and delete documents on entities as long as they have entity view, create, and update permissions. However, the Global Document Repository feature also requires document repository-related permissions and ownership to attach documents from the Document Repository to an entity.

Modifying Ownership

When you create a group or document collection, all RiskVision users are assigned Reader ownership by default.

To assign ownership to a group:

1. Open RiskVision Compliance Manager.
2. Go to **Content > Document Repository**.
3. Select a group in the **Document Repository** node to display its details.
4. Select **Assign ownership** in the **Group actions** dropdown list and then perform step 4 and step 5 for assigning the ownership to a document collection.

To assign ownership to a Document Collection:

1. Open RiskVision Compliance Manager.
5.
2. Go to **Content > Document Repository**.
6.
3. Locate the group in the **Document Repository** node and click the document collection of interest to display its details.
4. Click the **Ownership** tab.

   Click **Add Owners**. The **Add additional owners** dialog box appears.

   Select the ownership type from the *Owner Type* dropdown list. To assign the ownership, select a single user in the Individual Owner dropdown list or a team in the Team Owner dropdown list, and click **OK**. Optionally, click **+** to search a user based on role if the user that you intend to assign the ownership is not in the list.

A group can have nested groups, whereas a document collection can hold only the files and web links/network links. You cannot create a group in a document collection.

To delete ownership:

1. Open RiskVision Compliance Manager.
2. Go to **Content > Document Repository**.
3. To delete the group ownership, locate and select the group, select **Assign ownership** in the **Group actions** drop-down list. Select the owner(s) and then click **Delete**.
4. To delete the document collection ownership, locate and select the document collection, and click the **Ownership** tab. Select the owner(s) and click **Delete**.

Document Repository Actions

You can perform an action on a group or document collection using the actions drop-down list of document repository root node or using the **More Actions** drop-down list which appears when the details are displayed. To perform an action on a document, or web or network path reference, use the **More Actions** drop-down list from the document collection details page.

The linkage between a RiskVision object and Document Repository object (Document Collection, Document) will be preserved only when we add and move the same type of items, but not when we add one type of item and try moving the other type.

- The linkage is maintained, when you add Document Collection to an object and move document collection from one group to another group or when you add the document to an object and move document(s) from one Document Collection to another Document Collection.
- The linkage is not maintained when you add Document Collection to an object and move document out of it because linking to Document Collection means we documents will be shown at the current point of time in the Documents tab of the linked object.

Move

Documents can be moved to any group within the document repository node if you have the appropriate ownership and permission. You can use cut and paste to move a group or document collection. Use the move action to move an individual document or a web/ network path reference.

To move an object:

1. Open RiskVision Compliance Manager.
2. Go to **Content > Document Repository**.
3. Select the group or document collection in the Document Repository tree.
4. Click **Actions > Cut**.
5. Select the new location, then click **Actions > Paste**.

To move a document or web reference:

1. Open a document collection.
2. Select a document or web reference.
3. Click **More Actions > Move to**.
4. Select the document collection the item will be moved to.
5. Click OK.

Delete

To delete an object:

1. In the RiskVision application, go to **Content** > **Document Repository**. In RiskVision, go to **Risks** > **Document Repository**. In the Administration application, go to **Administration** > **Document Repository**.
2. To delete a group or document collection, select the object, and choose to **Delete** in the **Actions** drop-down list.
3. To delete a document or web reference, locate the document collection, and then select to display its details. Select the object and click **Delete**.

Documents that are linked to objects, such as entities and policies, cannot be deleted. Archive the linked documents by moving them to other groups.

About Data Feeds

Data Feeds are evidence from sources outside the RiskVision solution. Data Feeds include:

- Scanner reports
- Third-party tools
- Imported Excel/CSV documents

Data Feeds can be mapped to specific Controls and Subcontrols.

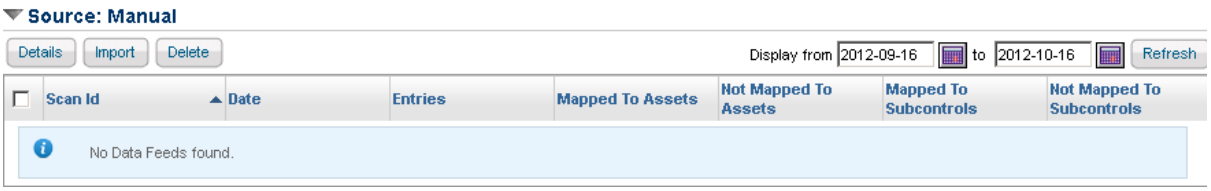
Data Feeds are either Manual or Questionnaire. A Manual Data Feed can be designated as the baseline against which to measure other Manual Data Feeds.

Importing Data Feeds

In RiskVision Compliance Manager, users with Data Feed View and Manage permissions can import CSV (Excel) documents, reports from scanners or other third-party software, and delete or update them.

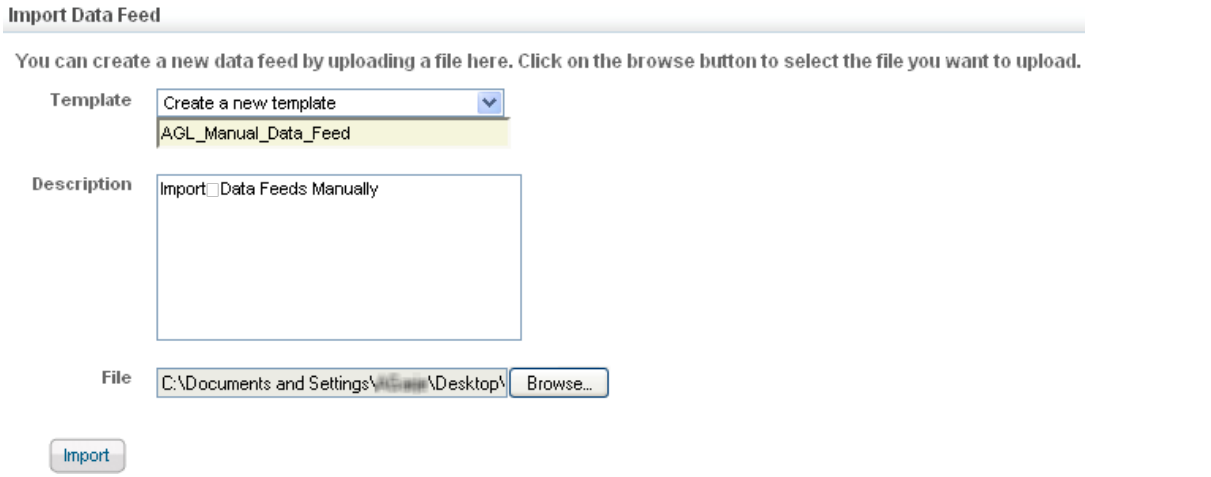
To import Data Feeds

1. Navigate to **Assessments > Data Feeds**. The **Data Feeds** page is displayed.



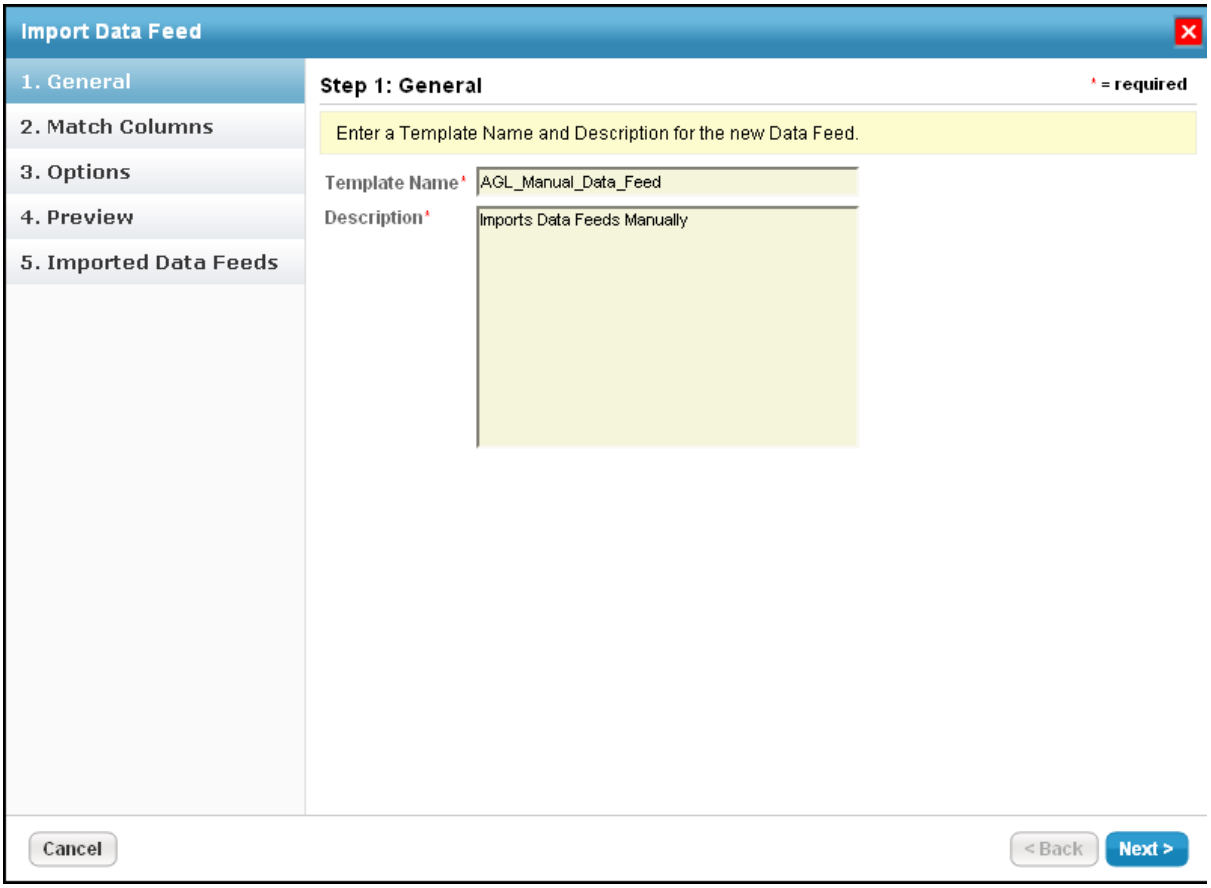
In the **Source: Manual** section, click **Import**.

2. The **Import Data Feed** page is displayed. Select an existing template for interpreting the document to upload, or create a new template. The template description is displayed. Click **Browse** to specify the local file to upload, and then click **Import** to upload the file.



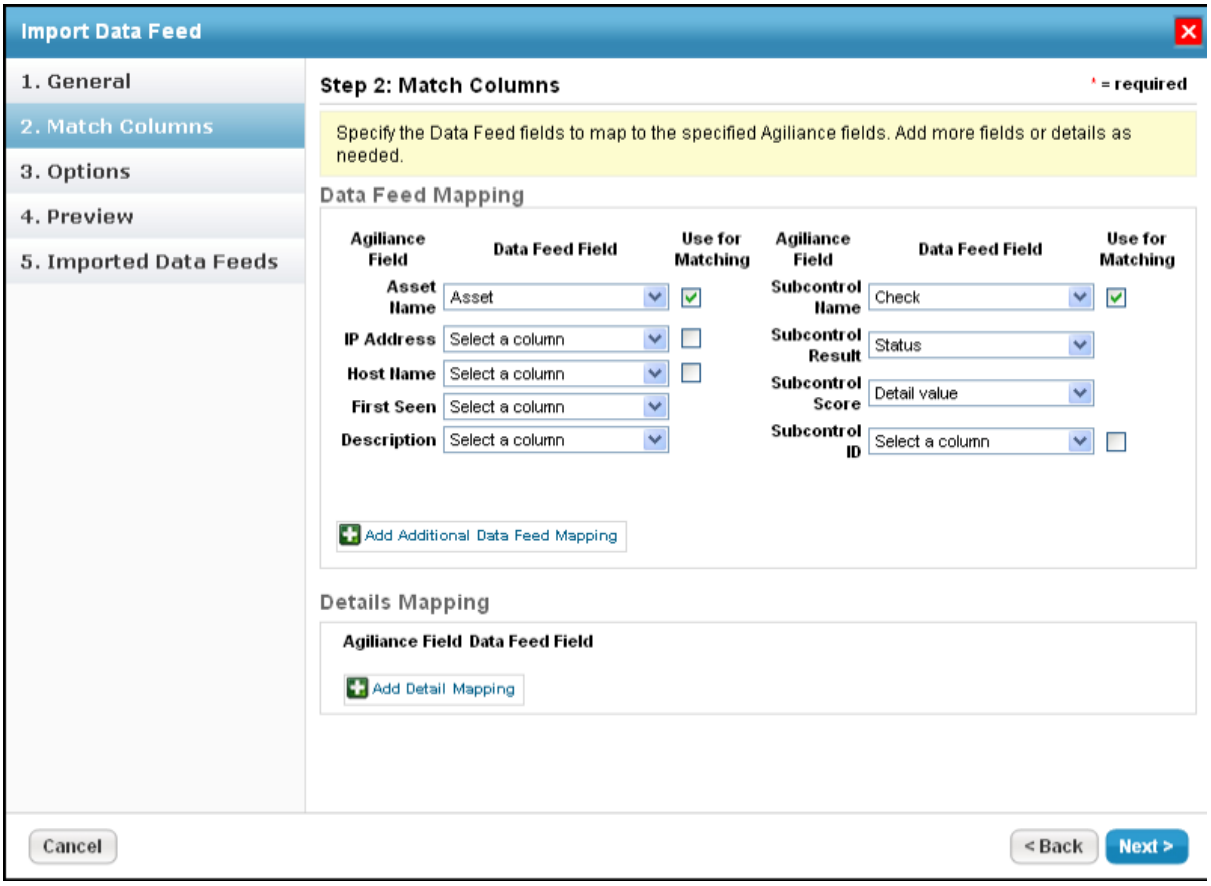
When the file is imported, the **Import Data Feed** page modifies. Click **Next** to continue.

3. The **Import Data Feed** wizard appears. In the **General** wizard page, enter **Template Name** and **Description.**



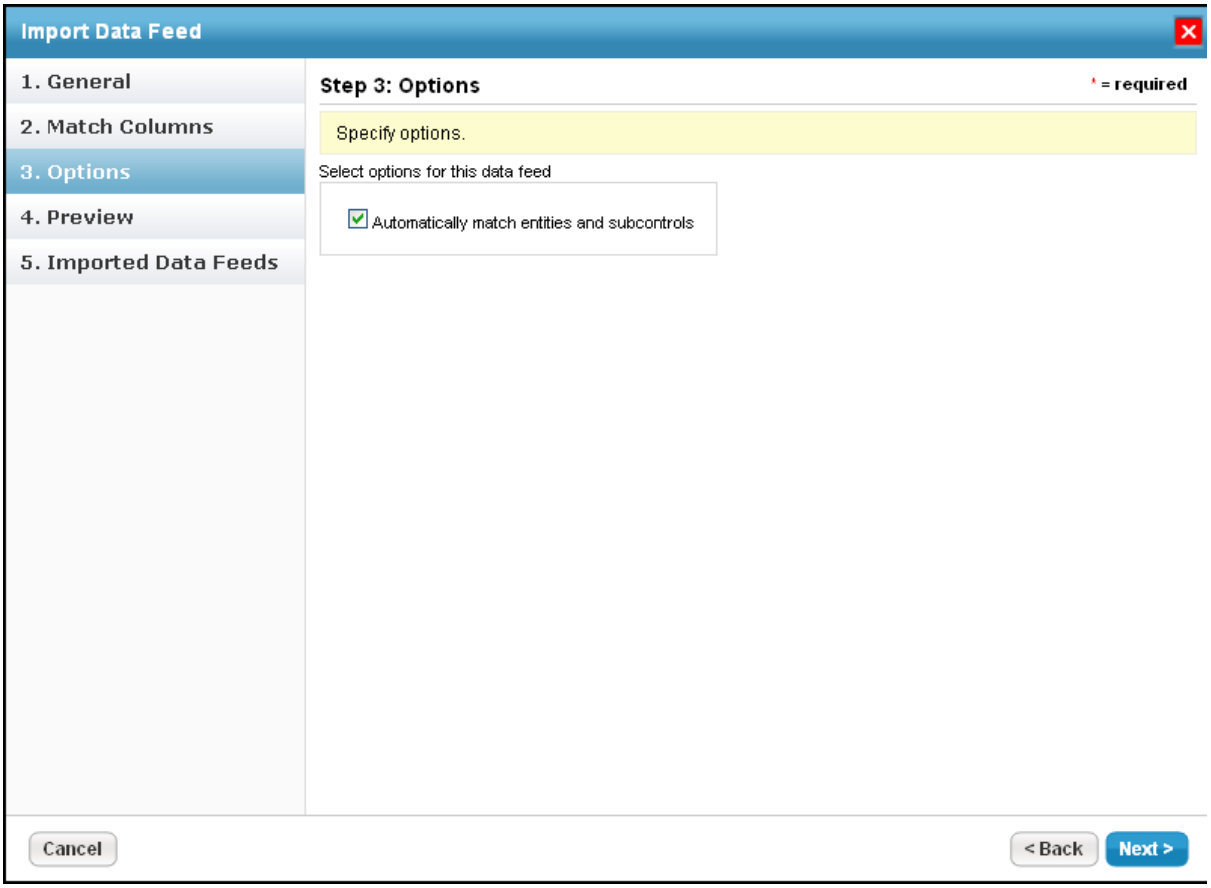
Click **Next** to continue.

4. The **Match Columns** wizard page is displayed. Select all data feed fields from your template that you want to map with the field. For example, if you are using a template for Asset mapping, then select 'Asset Name' for 'Asset', 'Subcontrol Name' for 'Check', 'Subcontrol Result' for 'Status', and 'Subcontrol Score' for 'Detail value'. Select the **Use for Matching** option to make the desired data feed field as a matching criteria. Optionally, you can create additional data feed and detail mappings.



Click **Next** to continue.

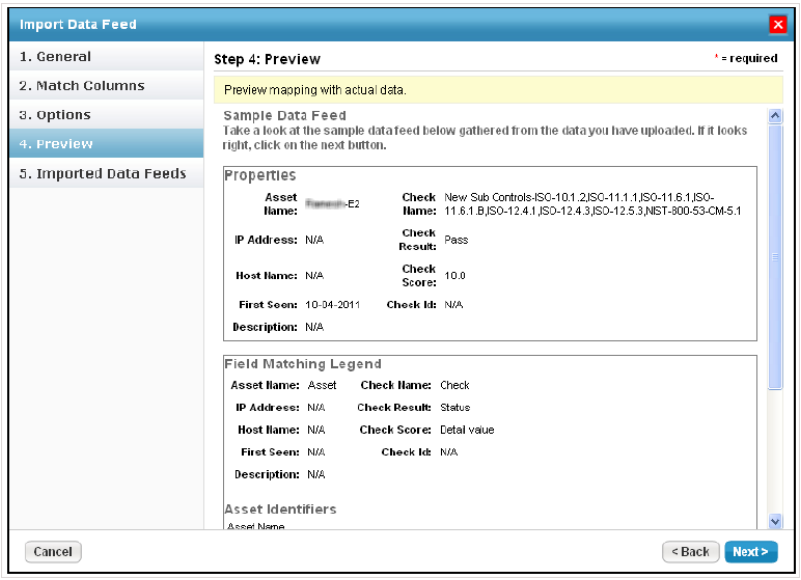
5. The **Options** wizard page is displayed. Select the box next to the Automatically match entities and subcontrols option to match entities with subcontrols. Leaving this option may not provide the compliance score for the entities imported through data feed in an assessment.



You may not be able to delete data feeds that are used in compliance programs. However, you can either create a new data feed template or contact Resolver Support to delete an existing data feed.

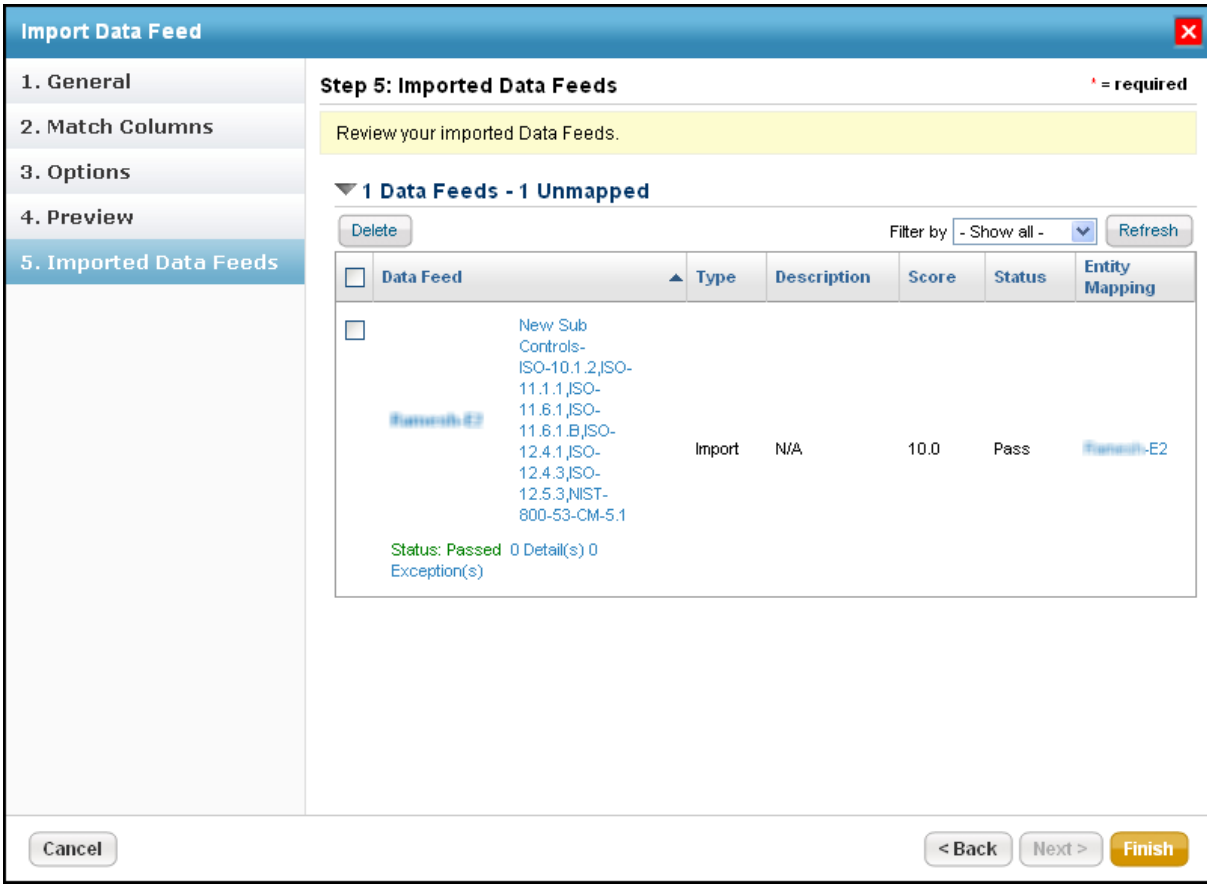
Click **Next** to continue.

6. The **Preview** wizard page is displayed. Make sure that the correctness of the data, such as properties, field matching legend, etc. is appropriate according to the data that you have uploaded from the template.



Click **Next** to continue.

7. The **Import Data Feeds** wizard page is displayed. You may delete the unwanted data feeds rather than importing all of them. Finally, review the data feeds to import, and then click **Finish** to import data feeds manually.



Each imported scan will show the number of assets and subcontrols that are not mapped with it.

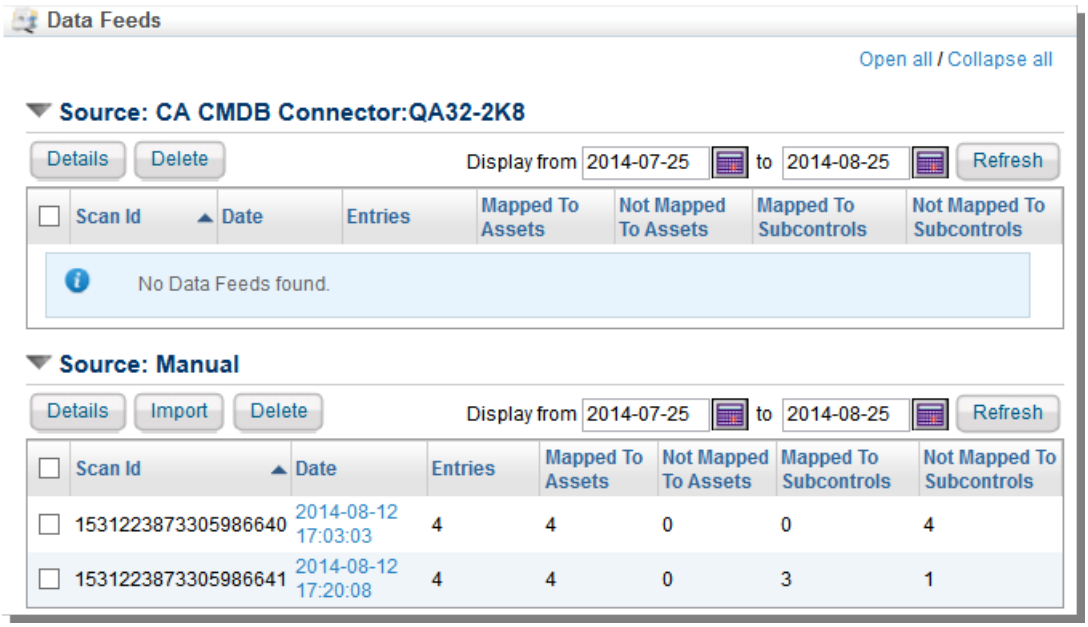
Resolver recommends running the **Scan Summary Update** system job before you include the data feeds in program assessments. To know the next execution time of **Scan Summary Update** job, in the Administration application, go to **Administration > Scheduled Jobs**.

Deleting Data Feeds

You can delete an unwanted data feed in the RiskVision application if your user role has Data Feed View and Data Feed Manage permissions.

To delete a data feed:

1. In the RiskVision application, go to **Assessments** > **Data Feeds**.



2. Expand the **Source** section in which the data feed you want to delete is available. If you cannot locate a scan, select a date range in the **Display from** and **to** fields, and click **Refresh**. To select a date, click the icon .
3. Check the box next to the data feed(s) and click **Delete**.
4. The **Delete Scans** prompt box appears in which you need to confirm the deletion of mappings to entities and controls. If you want to retain the mappings, clear the checkbox next to the **Remove mappings to entities and controls** option.
5. Click **OK**. The data feed is deleted.

Assessing Compliance

RiskVision applications help automate and streamline compliance assessments for today's highly-regulated industries. RiskVision encapsulates the compliance assessment within the notion of a program. Programs define a set of assessment options, including questionnaire selection and workflow that defines stakeholders for review and signoff of the assessment. For ongoing assessments, such as quarterly PCI assessment needs, the default duration and recurrence schedule can be set when a program is created. For more information about these topics, see:

- **Programs**
- **Controls and Questionnaires**
- **Questionnaire Presentation Options**
- **Workflow**

Understanding Programs

Programs provide reusable templates for assessments, including details of ownership, controls, and workflow. In addition to selecting a questionnaire, a program refers to a set of questionnaire presentation options that configure the questionnaire-taking interface with which the end-user will interact. Both Enterprise Risk Management (ERM) and Information Technology Risk Management (IT RM) assessments, and several other types are supported.

Predefined program types include:

- Classification Assessment
- Contract Awareness Campaign
- Control Assessment
- Key Risk Monitoring (KRI)
- Policy Awareness Campaign
- Risk Management
- Vendor Assessment

About the Program Wizard

The program wizard takes you through the program creation process and allows you to modify some program settings on the following tabs:

- Names and Owners - Provide basic information for an assessment program, such as name and description, program owner, and program type.
- Workflow - Select a workflow template. The RiskVision solution creates a workflow instance for each assessment. Assessments transition through the various stages on separate timelines. Modifications to an assessment instance, such as an additional stakeholder, affect the workflow instance only. The workflow instance specifies the process stages, stakeholders and participants, automatic run-time process controls, and stage transition requirements.
- Recurrence - Set the timeline and questionnaire options for reassessments.
- Options - Choose options controlling additional customizable behavior relevant to the current program type.
- Review - Examine the details of the program setup before saving and/or launching and starting assessments.

To create a program, your user role must have the Program View and Program Update permissions. When you have these permissions, you can create, update, and delete only the programs for which you are the owner. If your user role has the Program Manage permission, you can create, update, and delete any program no matter who owns it.

New Program Wizard Buttons

The wizard buttons allow you to navigate between pages (when it is appropriate) to cancel the wizard and, in some cases, to submit the wizard early by clicking the Finish button.

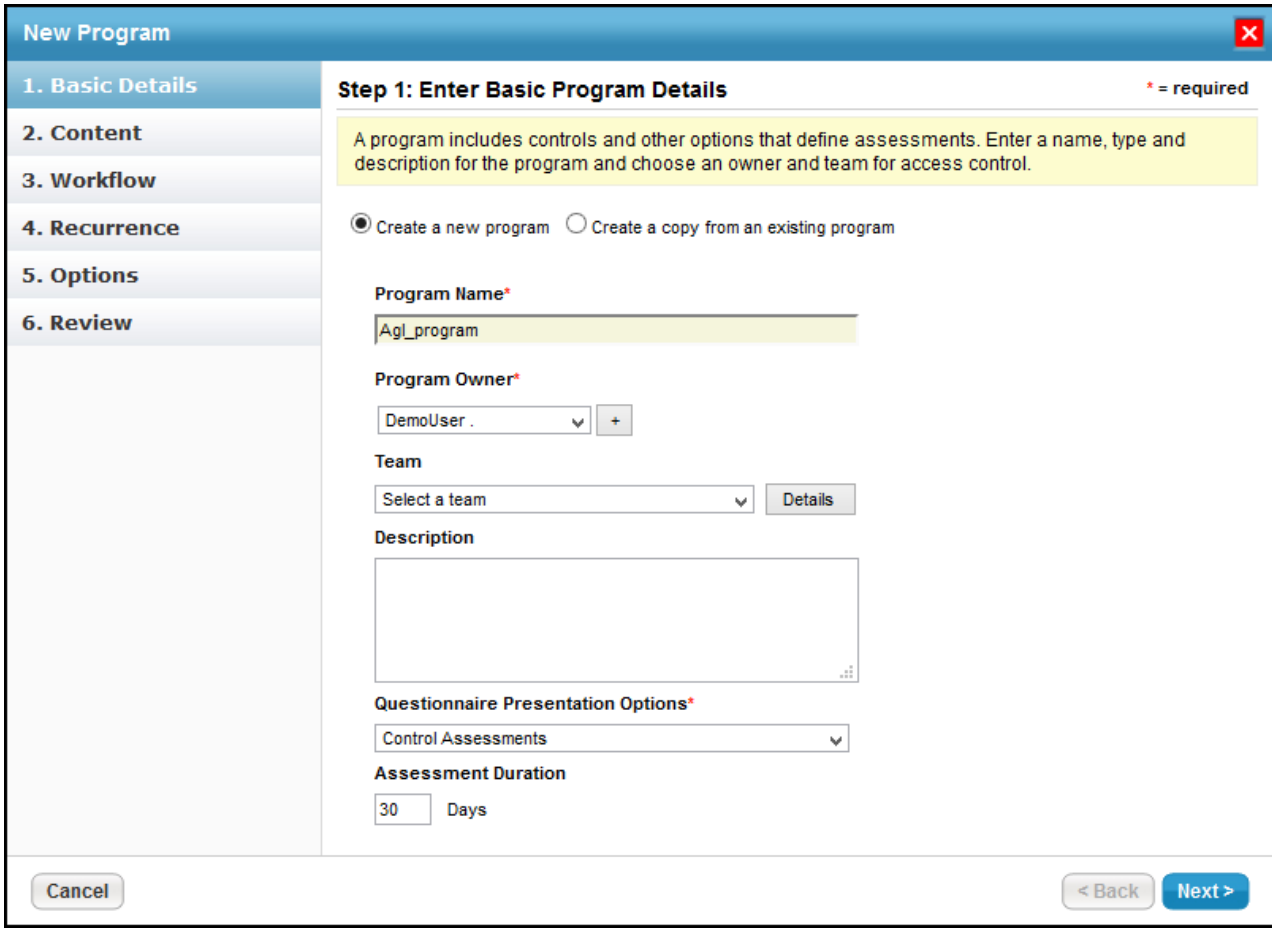
Checklist for Creating a Program

Assemble the following RiskVision objects before creating a program:

1. If an assessment needs a group of users to work on it, ensure that a team is available for you to select while creating a program.
2. Choose or create a Questionnaire Presentation Option that makes sense for your program's assessment. Consider your questionnaire responders and reviewers, what questions you will ask, and what evidence or other supporting information that you'll need from stakeholders.
3. Appropriate standard controls and questionnaires are available. Alternatively create your own content to assess entities. Contact Support to obtain additional content if the default content in the RiskVision application does not satisfy your assessment criteria.
4. Choose any default workflow template or design a workflow that suits your assessment. recommends that you test a user-designed workflow before an assessment is run in the production.
5. Determine which e-mail template that you need to use to notify users with when an assessment reaches a particular stage of a workflow, when a user takes an action on a questionnaire, or if you are planning to assess an entity periodically.
6. Must have Program View, and Program Update or Program Manage permissions. If you have Program View and Program Update permissions, you will be able to create new programs and modify only those for which you are the owner. Whereas, if you have Program View and Program Manage permissions, you will be able to create programs and assessments and manage actions, such as deleting programs, irrespective of the ownership.

Naming the Program and Assigning Owners

Enter the following information on the Basic Details page of the Program wizard.



Field	Type	Description
Program Name	String up to 255 characters	Identifies program.
Program Owner	Select user by name	Choose a user to manage the program settings, including launch. Requires Program and Assessments Manage permission. **Note:** Changing the owner disables the Launch button. Once you save the change, you only can see the program if you are a member of the program team.
Team	Select a team	Choose a team of users that you want to allow to view program details and manage settings. Requires that all team members have Program and Assessments Manage permission.
Description	Text	Optional description of the program.
Questionnaire Presentation Options	Named options	Select the questionnaire presentation options.
Assessment Duration	Number	Number of days to complete the assessment. Default is 30 days.

Program Type cannot be changed once the program is created. The type can affect the additional program options available for editing after the program is created.

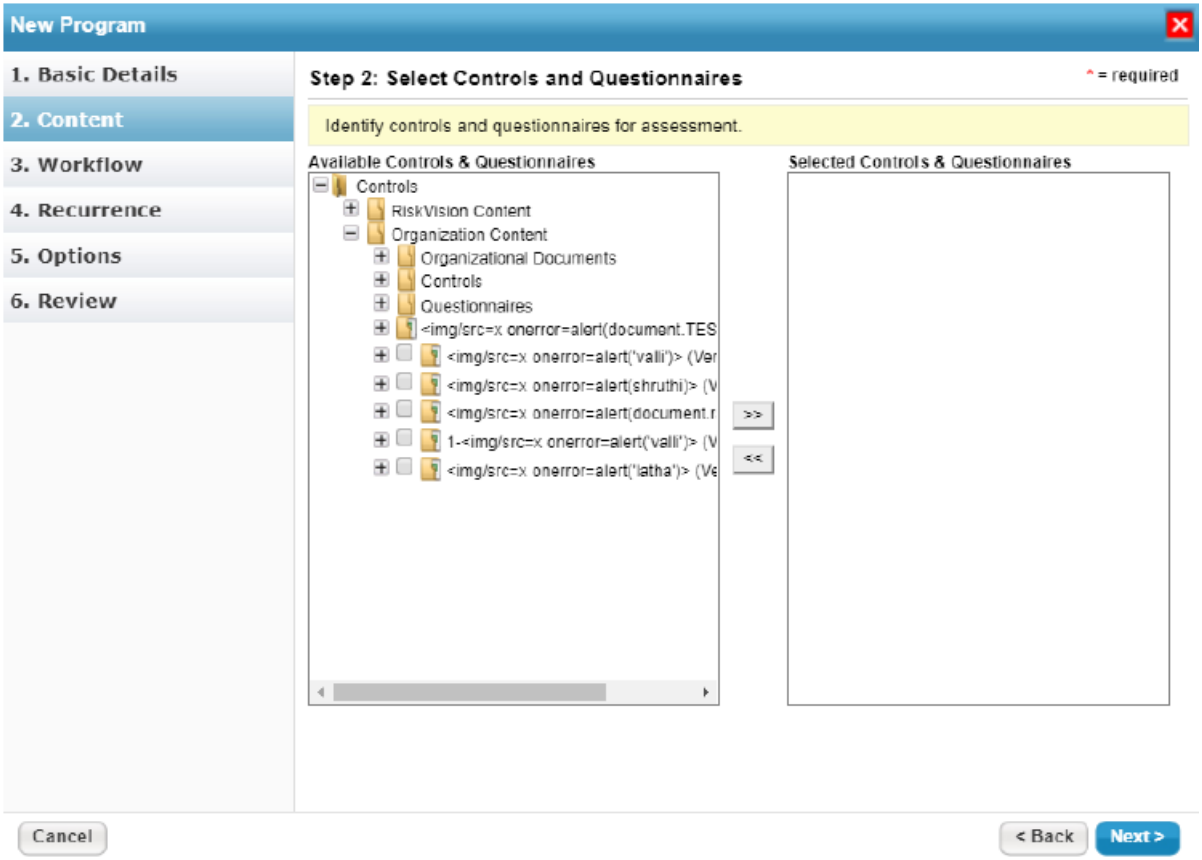
About Questionnaire Types

The following table describes the types of questionnaires sent to users:

Questionnaire Type	Description
Classification	Evaluate and classify
Compliance and Risk Assessment	Evaluate compliance and assess risk against a control
Contract Awareness Campaign	Gather attestations of awareness of the details of a specific contract
Enterprise Risk Assessment	Evaluate and classify Risk Opinion and Risk Identification survey
Policy Awareness Campaign	Evaluate awareness of a particular policy

Selecting Controls and Questionnaires

The Content page allows you to choose either RiskVision Content or your own organization's Controls and Questionnaires or Policy Documents. For additional information on content, see About Controls and Questionnaires.



- **Risk Management, Control Assessment, and Vendor Assessment** - Select the controls for which you want to evaluate compliance, including automated subcontrols and extended subcontrols.
- **Key Risk Monitoring (KRI)** - Select the Functional Risk Areas and KR controls for which you want to evaluate risk level.
- **Classification Assessment** - Select the questionnaire that contains the classification questions that you want to evaluate.
- **Enterprise Risk Assessment** - Select Risk Assessment and Risk Identification questionnaires.
- **Policy Awareness Campaign** - Select the questionnaire associated with documents that you want to ensure entity owners have received and read.
- **Contract Awareness Campaign** - Select the questionnaire associated with documents that you want to ensure entity owners have received and read.
- Users with sufficient privileges can also define their own assessment types.

Assigning Content

You can only assign groups, control objectives, controls, and questionnaires. The control list displays all Resolver and organization content.

Resolver recommends assigning the same control types.

To select content, you must know its name and location in the **Controls and Questionnaires** tree. Select all the controls and questionnaires that you want to assign to target entities. You can assign the content to all entities in the project or specify an entity or group on the next page.

Select a group or control by checking the box next to the item and moving it to the selected column using the arrows. The items are grouped into a single assignable unit.

The following table explains the content labels:

Icon	Object type	Description
	Group	Indicates a group of policy packs, controls, subcontrols, questionnaires, and/or automated controls.
	Control Objective	Indicates a control objective and assigns all the controls and subcontrols it contains to a single questionnaire for each entity.
	Control	Indicates a control. Assigns all subcontrols.
	Automated control	Indicates a check template that automatically verifies the settings with a pass/fail score.
	Questionnaire	Indicates a manual questionnaire.
	Policy Pack	Indicates a set of organization controls, subcontrols, or questionnaires.

Selecting Workflow

The RiskVision solution creates a workflow instance for each assessment. The workflow instance specifies the process stages, the stakeholders and participants, automatic run-time controls, and stage transition requirements.

Each assessment in the program transitions through the various stages on independent timelines. The program is considered complete when all assessments reach the terminal stage. Modifications to the assessment process affect that workflow instance only.

The workflow template notification dates, and program recurrence and assessment duration settings determine the milestones.

Select an existing workflow template or click **Create a new template**. For more information about workflows, see About Workflows.

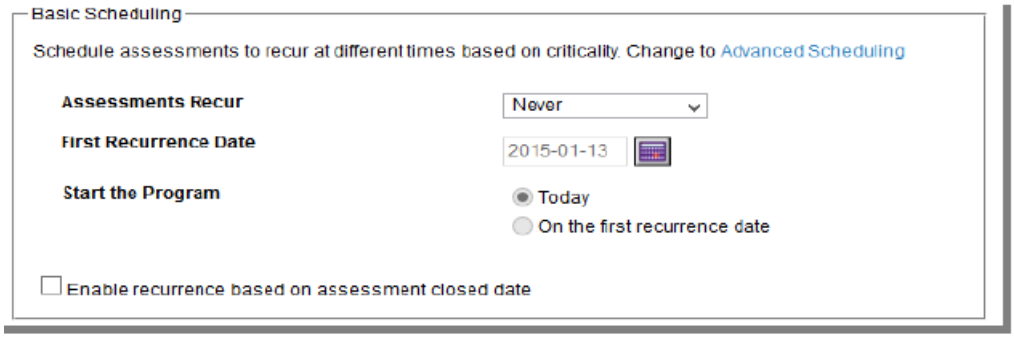
The workflow template preview pane displays the stage numbers and stakeholders. Stakeholders shown in **bold** receive notifications.

Understanding Recurrence

The recurrence settings allow you to automatically reassess the entities against the selected controls and questionnaires at regular intervals. Please be careful while selecting various combinations of options to ensure that the settings produce the desired effect.

Reassessing All Entities On the Same Schedule

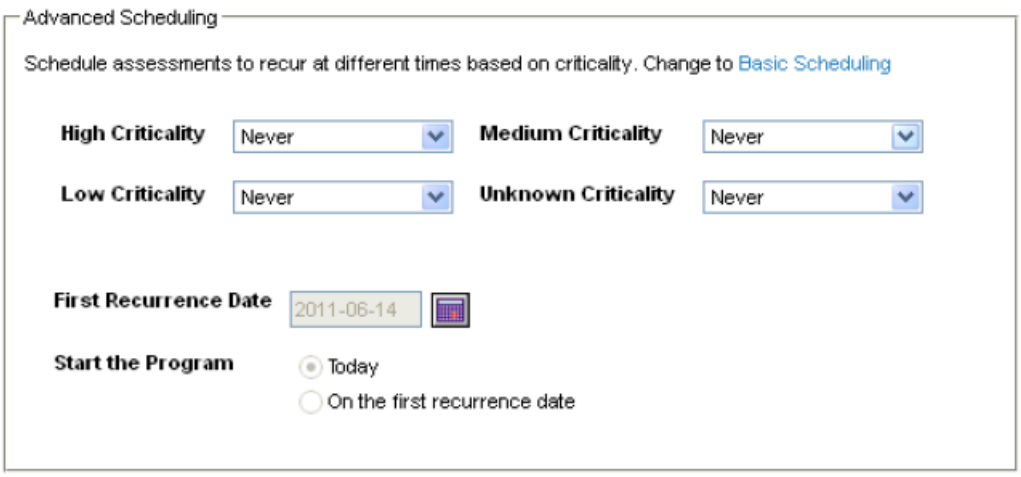
The basic scheduling options allow you to set the date and time to re-launch all assessments in the project as follows:



Setting	Option	Description
Assessments Recur	Never	One-time assessment. First and only assessment occurs when the project launches. Selecting 'Never' disables other recurrence options.
	Weekly, Every two weeks, Monthly, Quarterly, Semi-Annual, Annual, Every two years, Every three years, Every four years	Recurs on the date indicated by first recurrence.
First Recurrence Date	Long date	Select the date and time that you want to launch the project for the first time.
Start the Program	Today	On launching the project, the assessments process begins.
	On the first recurrence date	Assessment process begins on first recurrence date, but not when the project is launched.
Enable recurrence based on assessment closed date	-	Select whether to recur assessments based on the closed date.

Reassessing Entities Based On Criticality

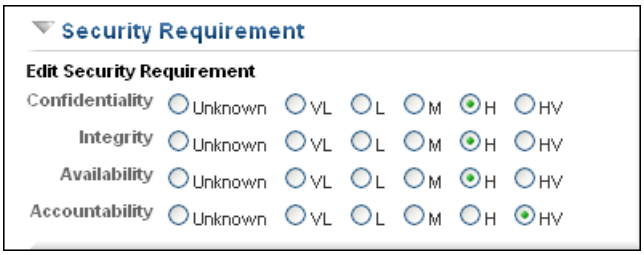
The Advanced Scheduling options allow you to set the date and time to relaunch all assessments in the project as follows:



Setting	Option	Description
High/Medium/Low/Unknown Criticality	Never	One time assessment for the entities with the criticality setting. First and only assessment occurs when the project launches. *Note: Selecting 'Never' disables other recurrence options.*
	Monthly, Quarterly, Semi-Annual, Annual, Every 2 years, Every 3 years	Entities with the criticality setting are reassessed on the date indicated by first recurrence.
First Recurrence Date	Long Date	Select the date and time you want to launch the project for the first time and for every recurrence thereafter.
Start the Program	Today	On launching the project, the assessments process begins.
	On the first recurrence date	Assessment process begins on first recurrence date, not when the project is launched.

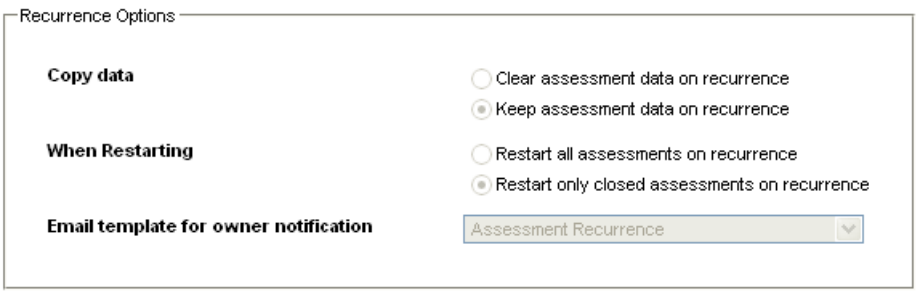
Security Requirement

To map High/Medium/Low criticality to systems that use VL (very low), L (low), M (medium), H (high), and VH (very high) labels, assume that H or VH are high, M is medium, and L or VL are low.



Selecting the Questionnaire Option For Reassessment

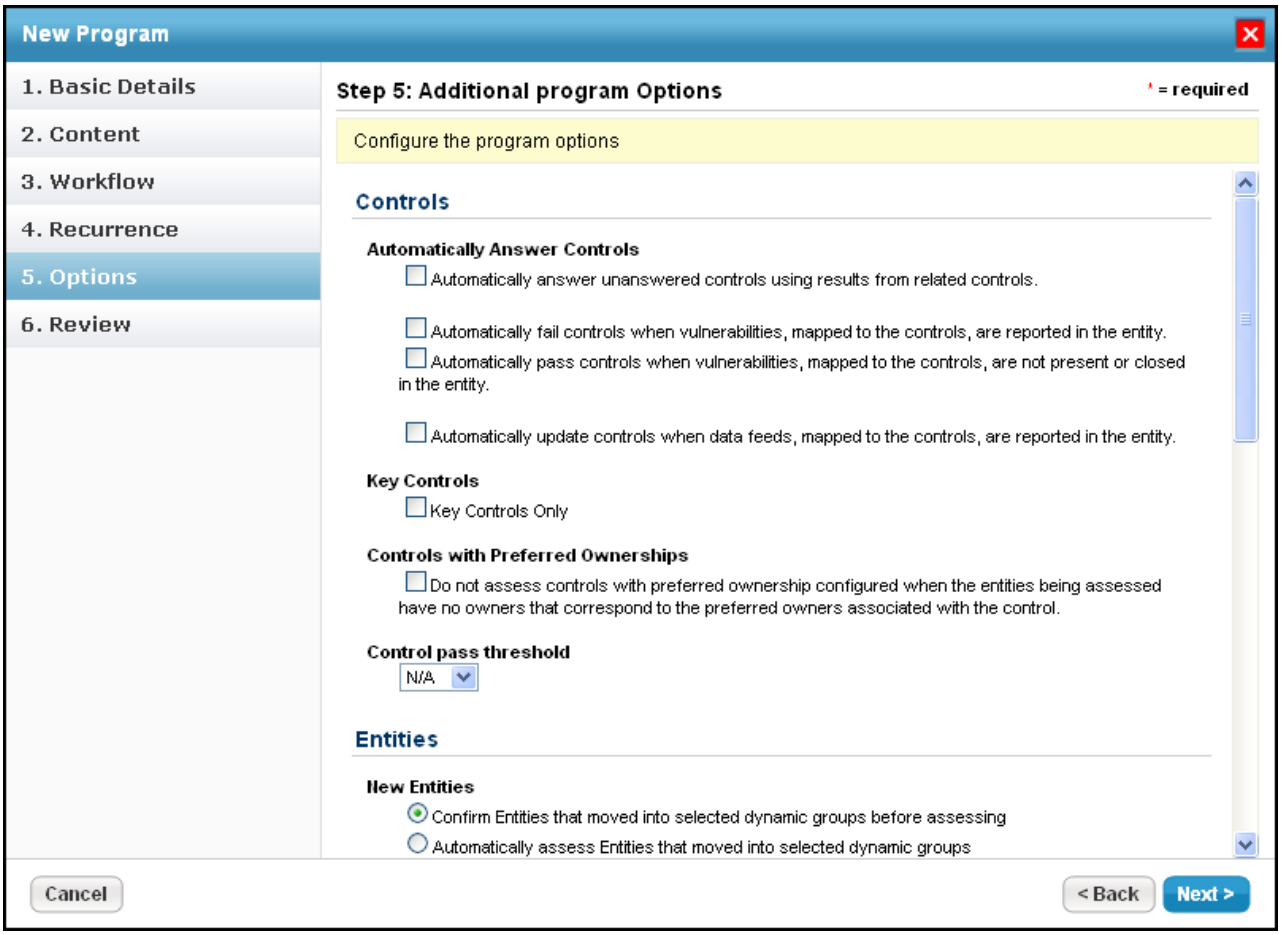
Recurrence options determine the assessment and questionnaire options for reassessments:



Setting	Option	Description
Copy data	Clear assessment data on recurrence	Clears information added to the workflow instance such as stakeholders as well as questionnaire answers and question delegations.
	Keep assessment data on recurrence	Retains information added to the workflow instance and answers if the assessment never reached the terminal stage.
When Restarting	Restart all assessments on recurrence	Starts all assessments in the first stage of the workflow n the recurrence date regardless of the stage they are in.
	Restart only closed assessments on recurrence	Leave assessments which have not reached the terminal stage in the stage they are in.
E-mail template for owner notification	All available assessment e-mail templates	Sends an e-mail and notification to the project owner and project team when the assessments in the project re-launch.

Setting Additional Program Options

The additional program options determine the questionnaire taking and set up options, new entity handling, scoring methods, and control response actions. These additional options can be changed only after the program is created.



Some of the following additional options are not presented, depending on the program type.

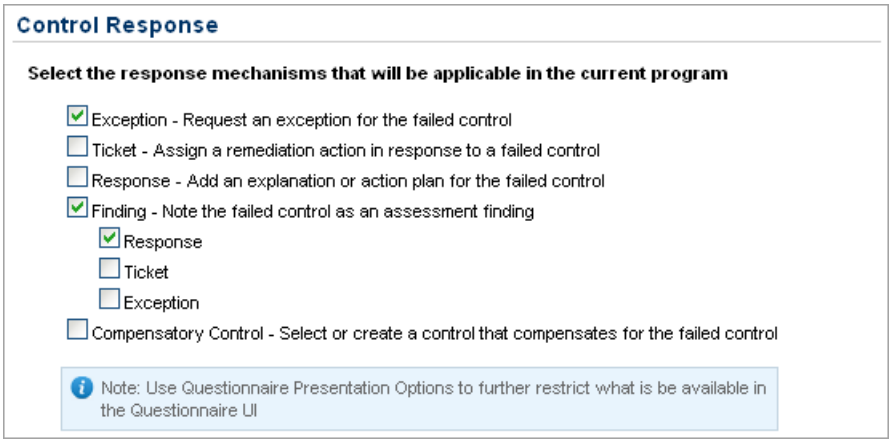
Option	Description
Automatically answer unanswered controls using results from related controls.	Answer controls if checked (not KRI programs).
Apply answer with the same score from related controls (note: This option automatically answers the choice in the current unanswered control whose score corresponds to the score in the already answered related control.)	Apply compliance score when the reference number of subcontrols are similar.
Apply answer only if the question text and choices are identical (note: This option will only select a corresponding choice in the current unanswered control if the matching answered control has both identical question text and identical choices)	Apply answers when the question text, set of choices and the reference number of subcontrols are similar.
Automatically fail controls when vulnerabilities, mapped to the controls, are reported in the entity.	Fail controls if checked (not KRI programs).
Automatically pass controls when	Pass controls if checked (not KRI programs).

vulnerabilities, mapped to the controls, are not present or closed in the entity	
Automatically update controls when data feeds, mapped to the controls, are reported in the entity.	Update controls if checked (not KRI programs).
Automatically pass controls when data feeds, mapped to the controls, are not present in the entity.	Pass controls if checked (not KRI programs). This option is not shown, by default. In order to use this option, set the following property in the agiliance.properties file. use.control.autoanswer.finding.absent=true
Key Controls Only	If checked, only assess key controls (not KRI programs).
Questionnaire Presentation Options	Select a previously - defined set of Questionnaire Presentation Options, such as "Control Assessments" or "Risk Profiling."
Controls with Preferred Ownership	Check to skip assessing controls with preferred ownership configured when the entities being assessed have no owners that correspond to the preferred owners associated with the control.
Control pass threshold	A number between 0 and 10, inclusive, or "N/A," the default.
New Entities	Confirm entities that moved into selected dynamic groups before assessing them, or automatically assess such entities.
Remove Entities	Confirm removal of entities that have moved out of selected dynamic groups, or automatically remove them.
Create Assessments	Select whether to create assessments for only entity collections or for entity collections as well as its members. Be aware while making a selection for Create Assessments. Because if you are assessing an entity collection containing 10,000 entities and you choose to create assessments for entity collection and its members, then the RiskVision application will launch 10,001 assessments. After creating the program, you will not be able to change the Create Assessments options.
Control Assessments	Specify the desired email template to notify the stakeholders in the first stage of an assessment workflow that a new assessment has been launched. Once the assessment is launched, the stakeholders in the subsequent workflow stages get notified using the email templates selected in the assessment workflow stages.
Notify only when there are questionnaires that require stakeholder attention.	Select to send notifications only when stakeholders are required to answer a questionnaire. For more information, see Sending Notifications to Stakeholders.
Send assessment update notification when entity target profile change impact questionnaire content	Check to send notification only when target profile is changed.
Control Response	Use one or more control response options in response to a failed control. For information about how to use the response mechanisms, see Setting Control Response Options.

Setting Control Response Options

Associating a questionnaire presentation option with a program will allow stakeholders to perform a wide variety of control response actions while answering a questionnaire. At a program level, failed controls are addressed using the control response mechanism. In the program options, a program owner can configure control response mechanisms to restrict stakeholders from performing several control response actions.

Control response options are unavailable in the program options if you are creating a Key Risk Monitoring (KRI) program.



The following are some of the common control response settings that are available in a program and questionnaire presentation options.

When you choose one or more options to customize, the changes that affect the questionnaire and **Control Results** page of the **Assessment Details** are listed below.

Control Response	Program options	Questionnaire Presentation Options	Control Results page	Questionnaire
Exception	Yes	Yes	The More Actions dropdown will list the Exception option.	Display Exception tab.
	Yes	No	The More Actions dropdown will not list the Exception option.	Hides Exception tab.
	No	No	The More Actions dropdown will not list the Exception option.	Hides Exception tab. The questionnaire will display the Exception tab to answer a subcontrol that requires an exception even if you disable the exception at questionnaire presentation options and program level.
	No	Yes	The More Actions dropdown will list the Exception option.	Hides Exception tab. Creating an exception from the Control Results page will also be shown in the questionnaire, but you may not create a new exception from the questionnaire.
Response	Yes	Yes	The More Actions dropdown will list the Add Response option.	Response tab is shown.
	Yes	No	The More Actions dropdown will list the Add Response option.	Hides Response tab.

	No	No	The More Actions dropdown will not list the Add Response option.	Hides Response tab.
	No	Yes	The More Actions dropdown will not list the Add Response option.	Hides Response tab.
Ticket	Yes	-	The More Actions dropdown will list the Add Ticket option.	-
	No	-	The More Actions dropdown will not list the Add Ticket option.	-
Compensatory Control	Yes	-	The More Actions dropdown will list the Compensatory Control option.	-
	No	-	The More Actions dropdown will not list the Compensatory Control option.	-

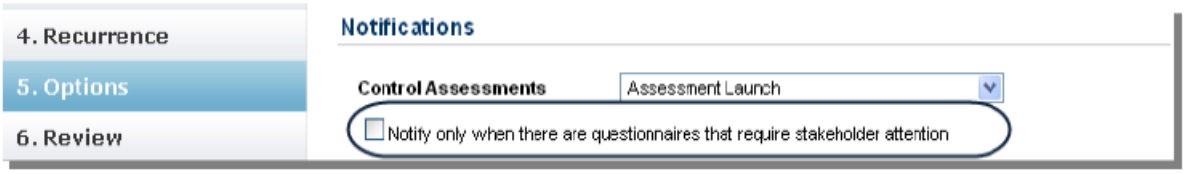
When you choose one or more finding options, following are the changes that affect the questionnaire and the Control Results and Findings page of the Assessment Details.

Control Response	Program Options	Questionnaire Presentation Options	Control Results page	Findings page	Questionnaire
Select only Finding	Yes	Yes	Display Mark as Finding button	Displays New and Delete button. The More Actions dropdown will list Import Audit Findings and Assign Owner options.	Displays Findings tab
	Yes	No	Display Mark as Finding button	Displays New and Delete button. The More Actions dropdown will list Import Audit Findings and Assign Owner options.	Hides Findings tab
	No	No	-	Hides New and Delete Button	-
Select Finding with Response, Ticket, and	Yes	-	Display Mark as Finding button	Displays New and Delete button. The More Actions	

Exception				dropdown will list Import Audit Findings, Add Finding Response, Show Finding Response, New Exception, New Ticket options, and Assign Owner options.	

Sending Notifications to Stakeholders

By default, an assessment sends notifications to workflow stage stakeholders even though there no questionnaires and/or controls to answer. However, as a program owner, you can select the "Notify only when there are questionnaires that require stakeholder attention" option on the Options tab of the program wizard to send notifications to workflow stage stakeholders only when there are questionnaires to answer. For more information, see Checklist for Notifying Stakeholders Only when there are Questionnaires.



Checklist For Notifying Stakeholders Only When There Are Questionnaires

In addition to enabling the option on the program wizard, you must ensure that the following checklist is in place to recognize the effect of notifying the stakeholders only when there are questionnaires to answer.

1. Ensure that a control target profile with appropriate target selection criteria is available, or create a new control target profile with a target selection criteria that will make sense while assessing your entities. For example, create a control target profile with the target selection criteria "entity severity equals to low" to assess only entities that have a low criticality.
2. Determine the controls that need to be associated with the control target profile.
3. Create a program using the content which has a control target profile attached to it.
4. Create assessments for entities that match the control target profile settings and for entities that do not match the control target profile settings.

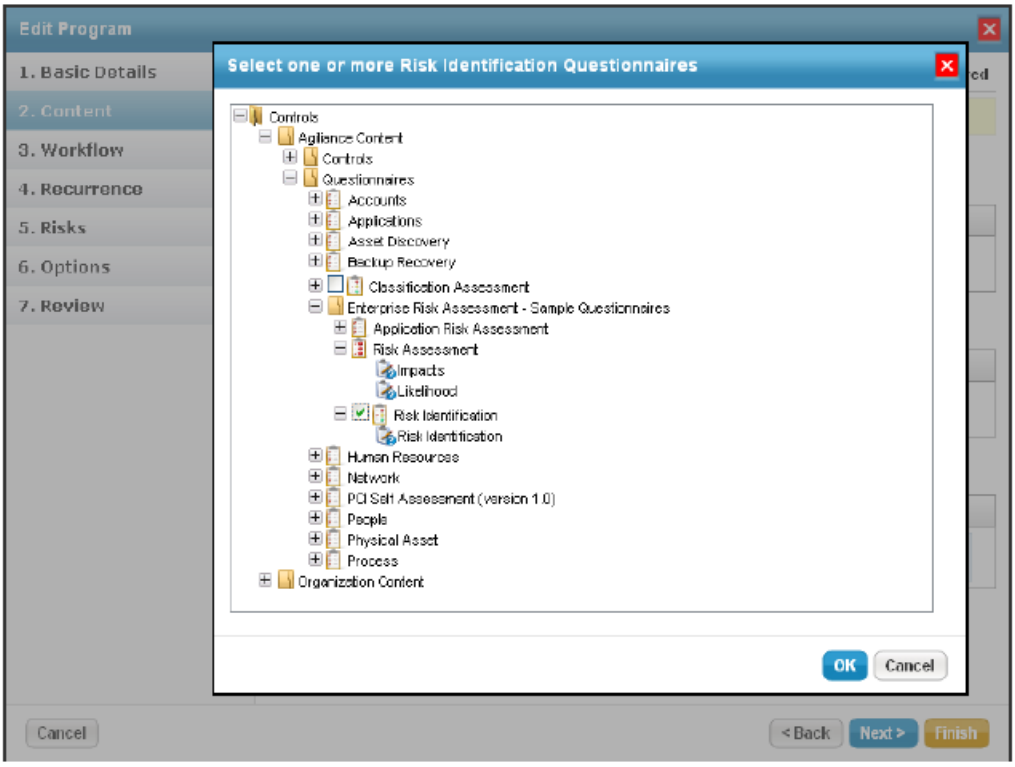
Notifications Behavior

1. Notify only when there are questionnaires that require stakeholder attention option is turned **on**
    - When entities settings match the control target profile, only the controls and/or questionnaires associated with the control target profile are assigned to the stakeholders. As a result, when a workflow stage is transitioned, a notification is sent to the workflow stage stakeholders using the template that is defined for that particular stage. In case an entity settings do not match the control target profile, the controls and/or questionnaires are not assigned to the stakeholders, and as a result, the Message Center does not display the notification message.

2. Notify only when there are questionnaires that require stakeholder attention option is turned **off**
    - When the entity settings match the control target profile, only the controls and/or questionnaires associated with the control target profile are assigned to the stakeholders. As a result, when a workflow stage is transitioned, a notification is sent to the workflow stage stakeholders using the template that is defined for that particular stage. In case an entities settings that do not match the control target profile, the controls and/or questionnaires are not assigned to the stakeholders, however, the assessments continue to send the notifications.

Assigning Risk Assessment Questionnaires

The **Content** wizard page on the program wizard allows you to choose either RiskVision Content or your own organization's Controls and Questionnaires, see About Controls and Questionnaires for additional information on content.



Enterprise Risk Management (ERM) select an ERM questionnaire type and IT Risk Management (IT RM) select an IT RM questionnaire type that allows the program owner and stakeholders to select risks that apply to the entities being evaluated.

Resolver provides the following questionnaires for ERM and IT RM programs:

- **Content > Questionnaires > Enterprise Risk Assessment > Risk Identification** Allows each stakeholder in the Information Gathering stage to add risks that all stakeholders of the information gather stage evaluate. Note that risks are assigned once the questionnaire is complete.
- **Content > Questionnaires > Enterprise Risk Assessment > Risk Assessment** Allows the program owner to select the risks. A blank questionnaire is sent to the stakeholders of the information gathering stage when you launch the assessment. The risks are automatically added to the questionnaire when the program owner selects them. Stakeholders determine the likelihood and impact for each risk.
- **Content > Questionnaires > Enterprise Risk Assessment > Application Risk Assessment** Allows all the authorized users to assess the controls, whether it is applied or not to a risk in an assessment.

Checklist for Creating an Assessment

Assemble the following RiskVision objects before creating an assessment:

1. A program with ownership that satisfies all your assessment needs. If you are using an existing program, it is recommended that you walk-through all the options that are available in the program wizard. If any of the options do not suit your assessment methodology, you must create a new program.

2. An entity to be assessed in the RiskVision application with an ownership to select in an assessment.

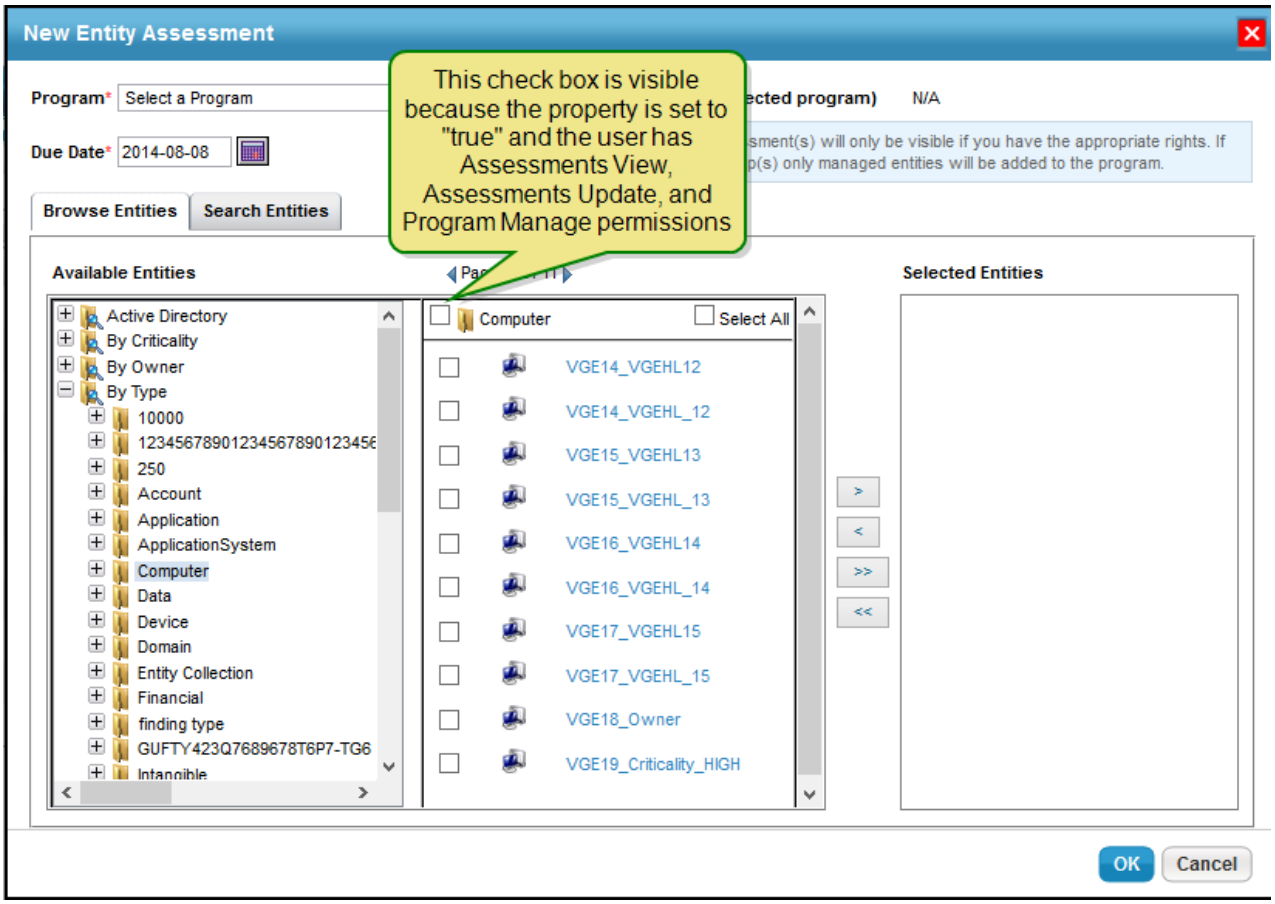
3. If an entity is related to another entity, define a relationship between entities and specify the settings that propagate control assignments, control results, risk scores, tag or criticality values.

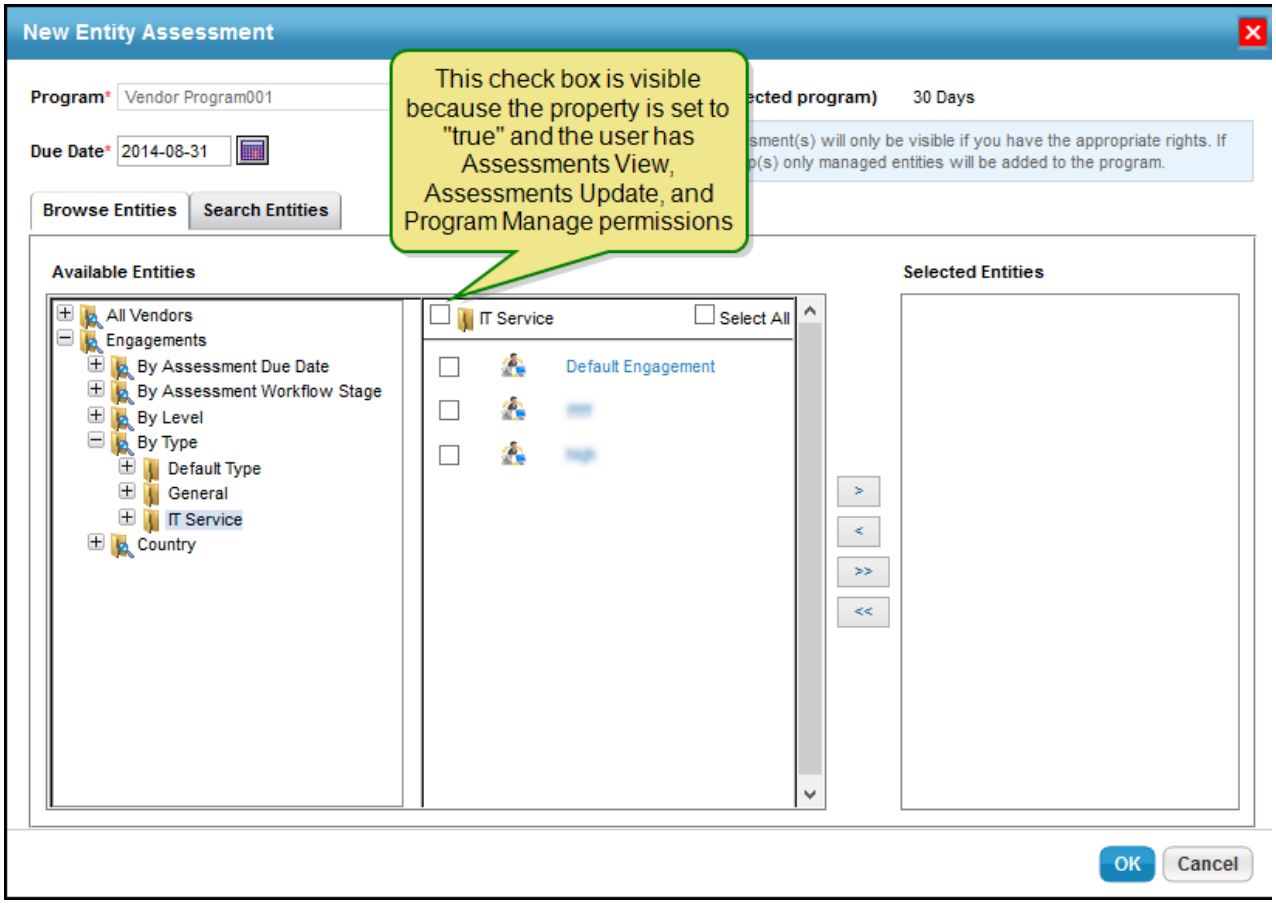
4. Adjust the threshold value of a configuration range according to your assessment criteria.

5. Must have Assessments View, and Assessments Create or Assessments Manage permissions. If you have Assessments View and Assessments Create permissions, you will be able to create assessments. If you have Assessments View and Assessments Manage permissions, you will be able to create assessments and manage actions, such as deleting assessments irrespective of the ownership.

Controlling Dynamic Group Visibility in Assessment Creation

Dynamic groups are shown by default in the New Entity Assessment dialog to users with Program View and Program Manage permissions. To help prevent accidental inclusion of dynamic groups as a whole in assessments, you can hide the checkbox next to a dynamic group in the New Entity Assessment dialog using the dynamicGroup.selection.visible property. When you set the property to "false," you can no longer select the dynamic group as a whole, but will still be able to select individual entities that are part of a dynamic group.




New Entity Assessment
Program* Vendor Program001
Due Date* 2014-08-31
ected program) 30 Days
sment(s) will only be visible if you have the appropriate rights. If
p(s) only managed entities will be added to the program.
This check box is visible because the property is set to "true" and the user has Assessments View, Assessments Update, and Program Manage permissions
Browse Entities
Search Entities
Available Entities
Selected Entities
All Vendors
Engagements
By Assessment Due Date
By Assessment Workflow Stage
By Level
By Type
Default Type
General
IT Service
Country
IT Service
Select All
Default Engagement
>
<
>>
<<
OK
Cancel

Controlling the Visibility of Propagation Tab

The **Propagation** tab on the assessment details page and the **Propagate Control Results** option in the **More Actions** drop-down list on the **Assessments** tab of the **Program** details page are shown by default for users who have the Assessment Update and/or Assessment Manage permissions. These features are visible in both Compliance Manager and Enterprise Risk Manager applications. If you do not want to implement the propagation feature in your use cases, you can hide it by mentioning the enable.propagation = false property in the .properties file.

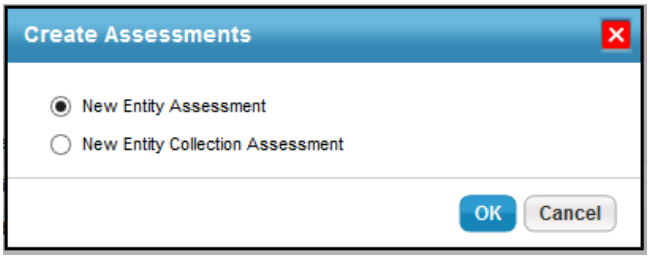
Creating an Entity Assessment

Creating an assessment consists of choosing a program and entities. The program specifies many of the details and selections of the assessment, which can be applied to any number of entities. In order to create an entity assessment, your user role must have Assessments View and Assessments Update permissions. With these permissions, you can create assessments for standalone entities and entities that are part of a dynamic group. For information about the property setting and permission to include a whole dynamic group in an assessment, see Controlling Dynamic Group Visibility in Assessment Creation.

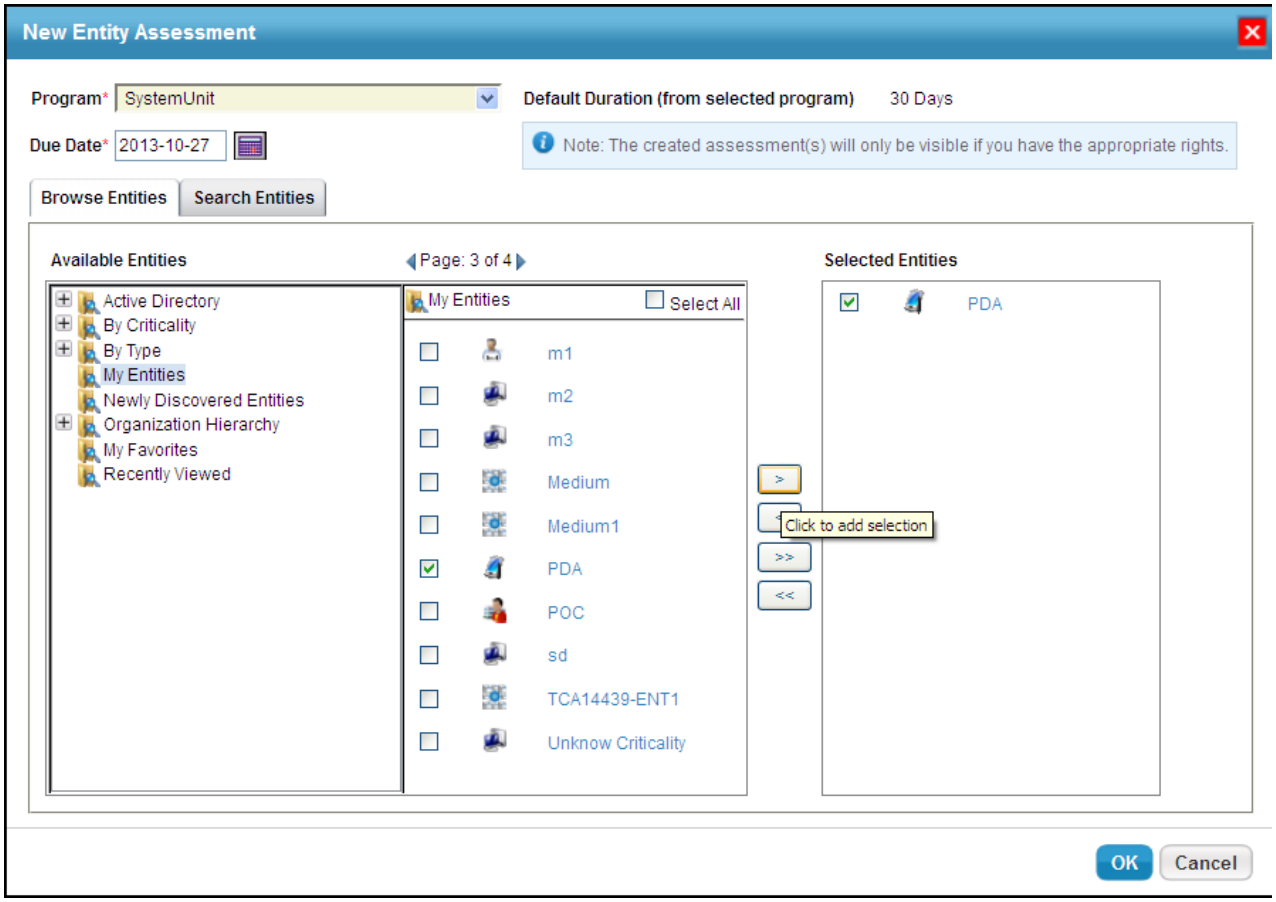
Before creating an assessment, you must create a program.

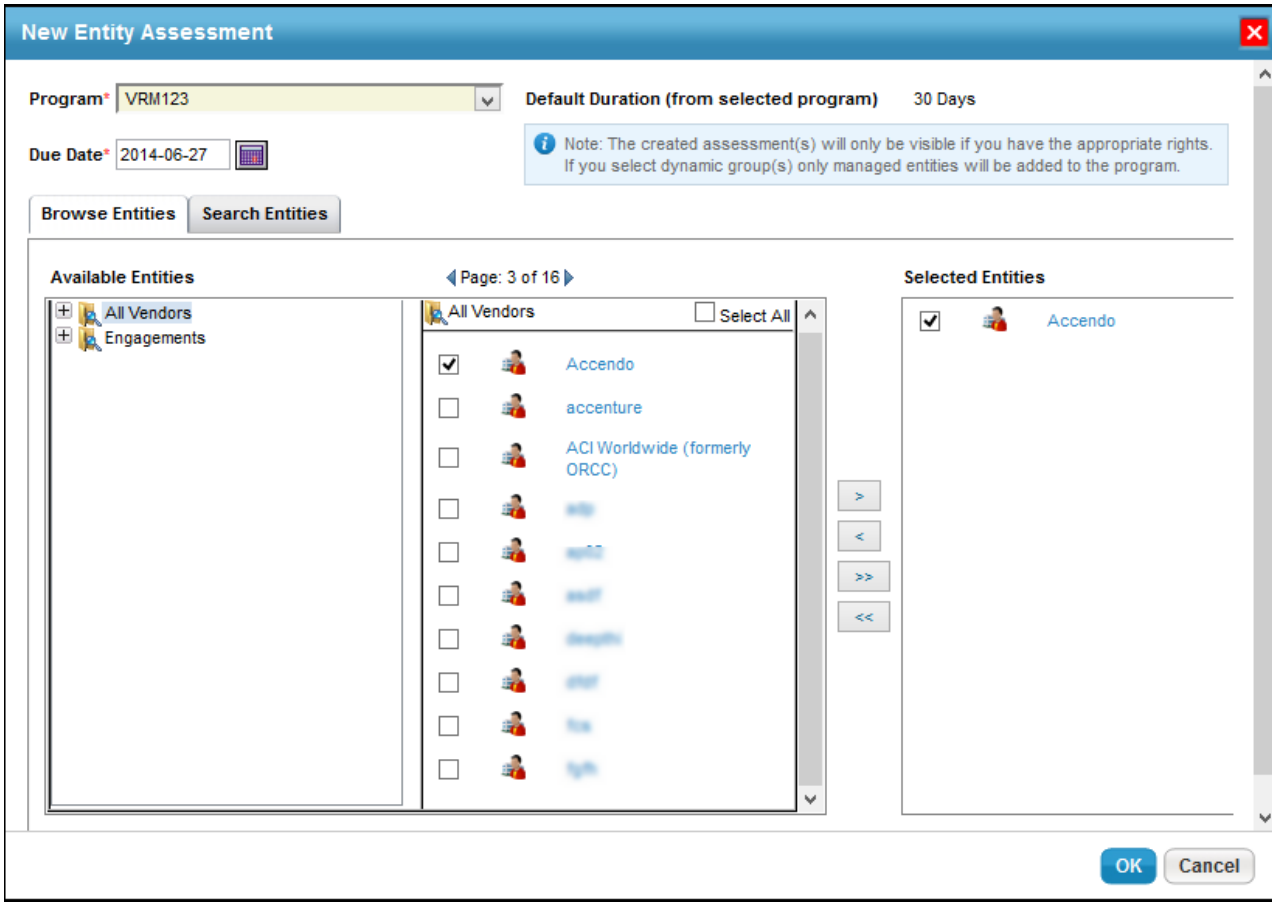
To create and launch a new assessment:

1. In the RiskVision application, go to the **Assessments** > **Assessments** page.
2. Click **Create**. The **Create Assessments** dialog appears.



3. Select **New Entity Assessment**. The **New Entity Assessment** dialog appears.





4. Select a program in the Program drop-down list. The default duration associated with the program is displayed, and the due date is automatically set to those many days from the current date. You can revise the due date manually.

5. Select at least one entity to assess. Within the **Available Entities** of **Browse Entities** tab, expand the group in the tree containing the entity you want to assess, or click the **Search Entities** tab to find the entity using search criteria. To specify search criteria, select a field in the first drop-down box, then select a condition in the second drop-down box, and enter the search value in the box. Click **+** to add a new search condition. Click **Search** to retrieve the results for selecting entity(s). After the entity(s) is found, select desired entities by checking the box next to them. Clicking the entity title pops up a window to display the entity's details.

6. Click OK after the entities to assess are in the **Selected Entities** list.

7. Launching an assessment can be a time-consuming process. If you close the dialog, you will be notified when the assessment has actually launched.

   If you have to create assessments for entities imported without the primary owner, make sure to assign the primary owner after importing entities so that entity assessments show up in the Assessments page.

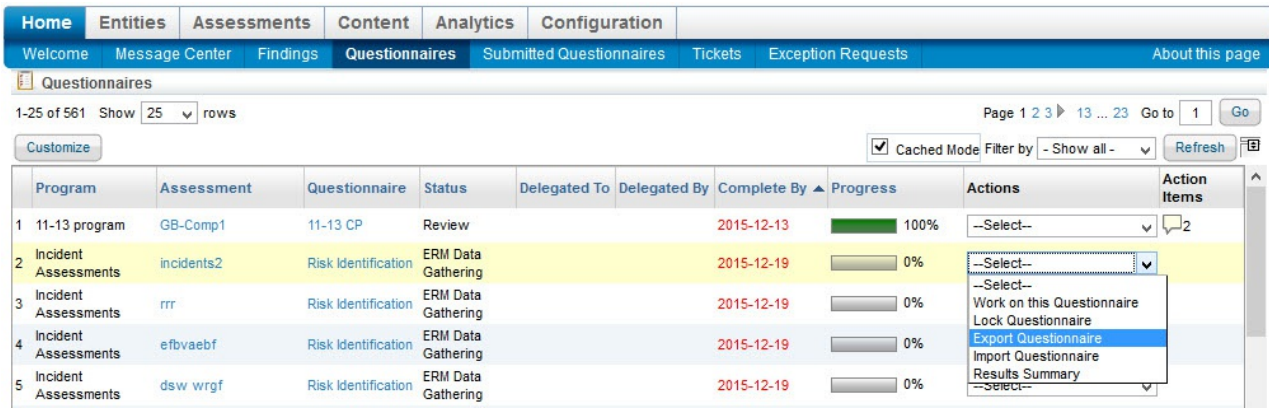
There are other alternative methods of creating an assessment, but then the assessment created is specific to the program or entity. The alternate method of assessment creation are given below:

- The Programs page
- The Entities page, within Entities Details page
- The Entities page, from the More Action drop-down menu, the Copy Entities action

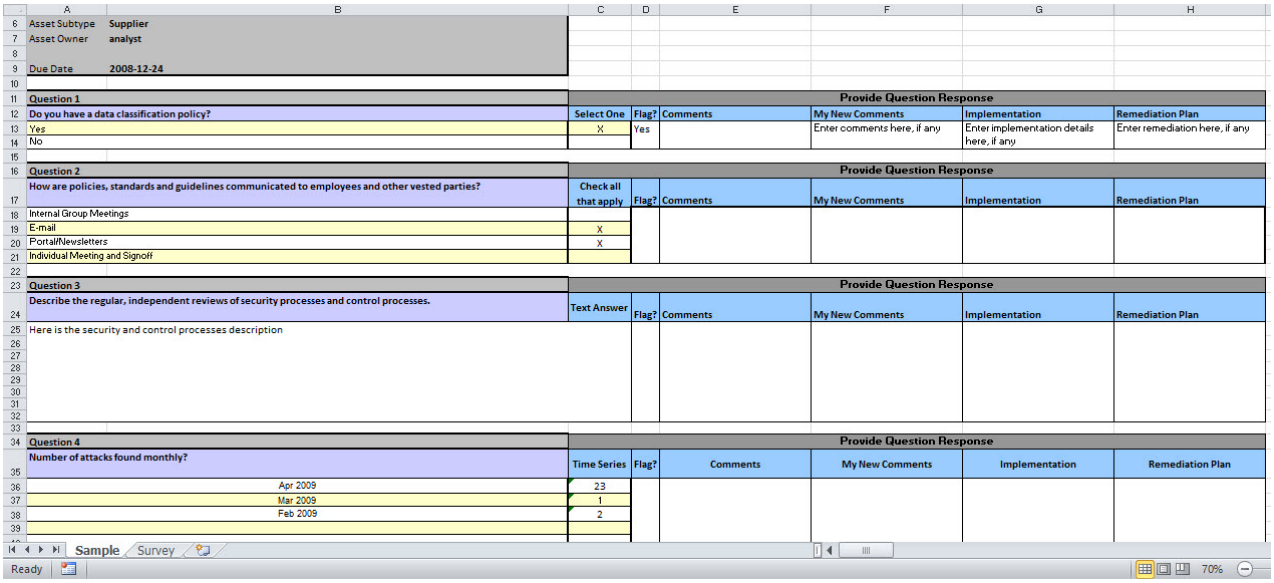
Importing Answers to Questionnaires

RiskVision lets you export questionnaires to an Excel spreadsheet. You can export questionnaire spreadsheets, provide answers in the spreadsheet, and then import it back to RiskVision. The 'Sample' sheet serves as a reference to answer questions, using which you can fill up the 'Survey' sheet.

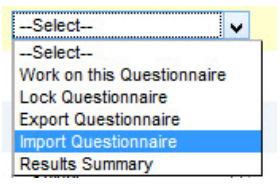
In the **Questionnaires** tab, for a program, select **Export Questionnaire** from the drop-down in the **Actions** column.



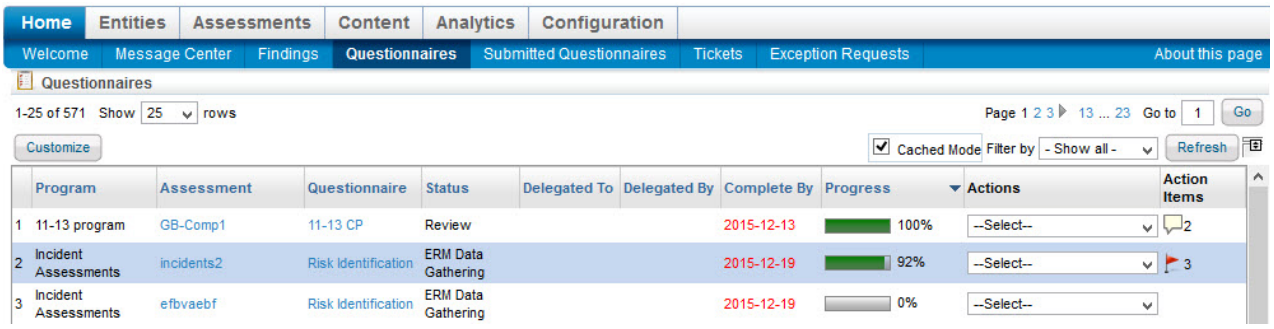
Download and save the excel spreadsheet. You can use the '*Survey*' sheet to fill out the answers to the questionnaire.



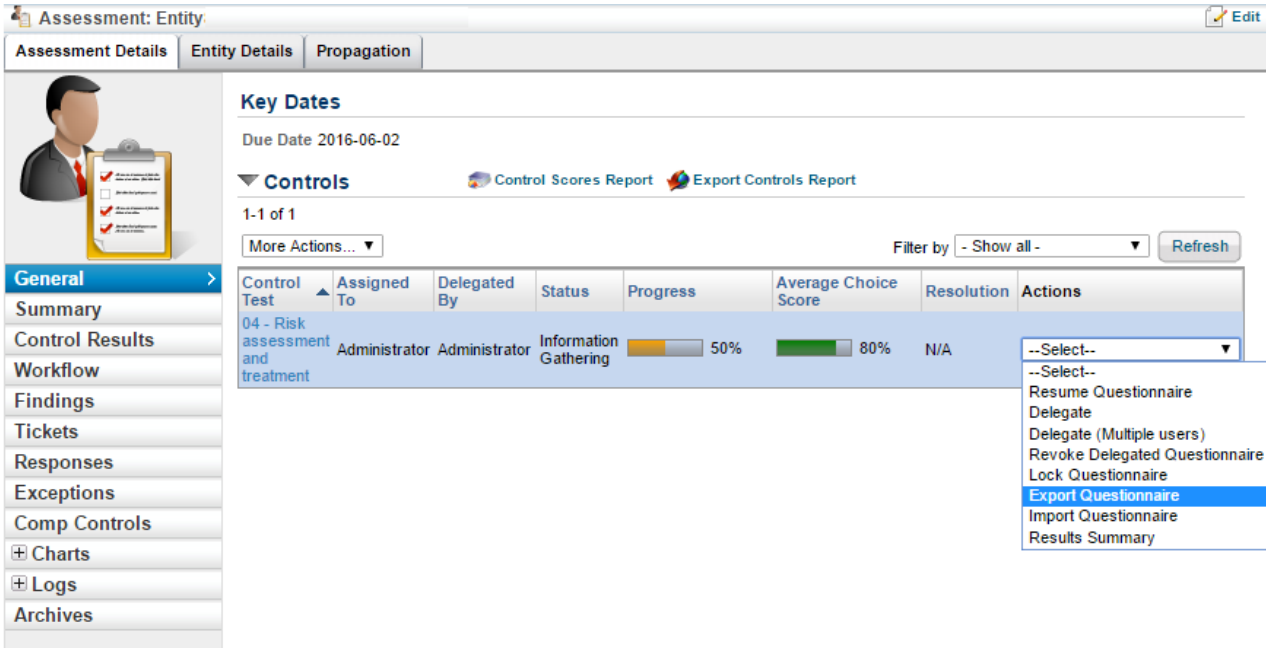
After you have provided your answers, you can import the same spreadsheet back to RiskVision using the **Import Questionnaire** option from the drop-down in the Actions column.



The responses provided by you in the spreadsheet are now imported and recorded in RiskVision.

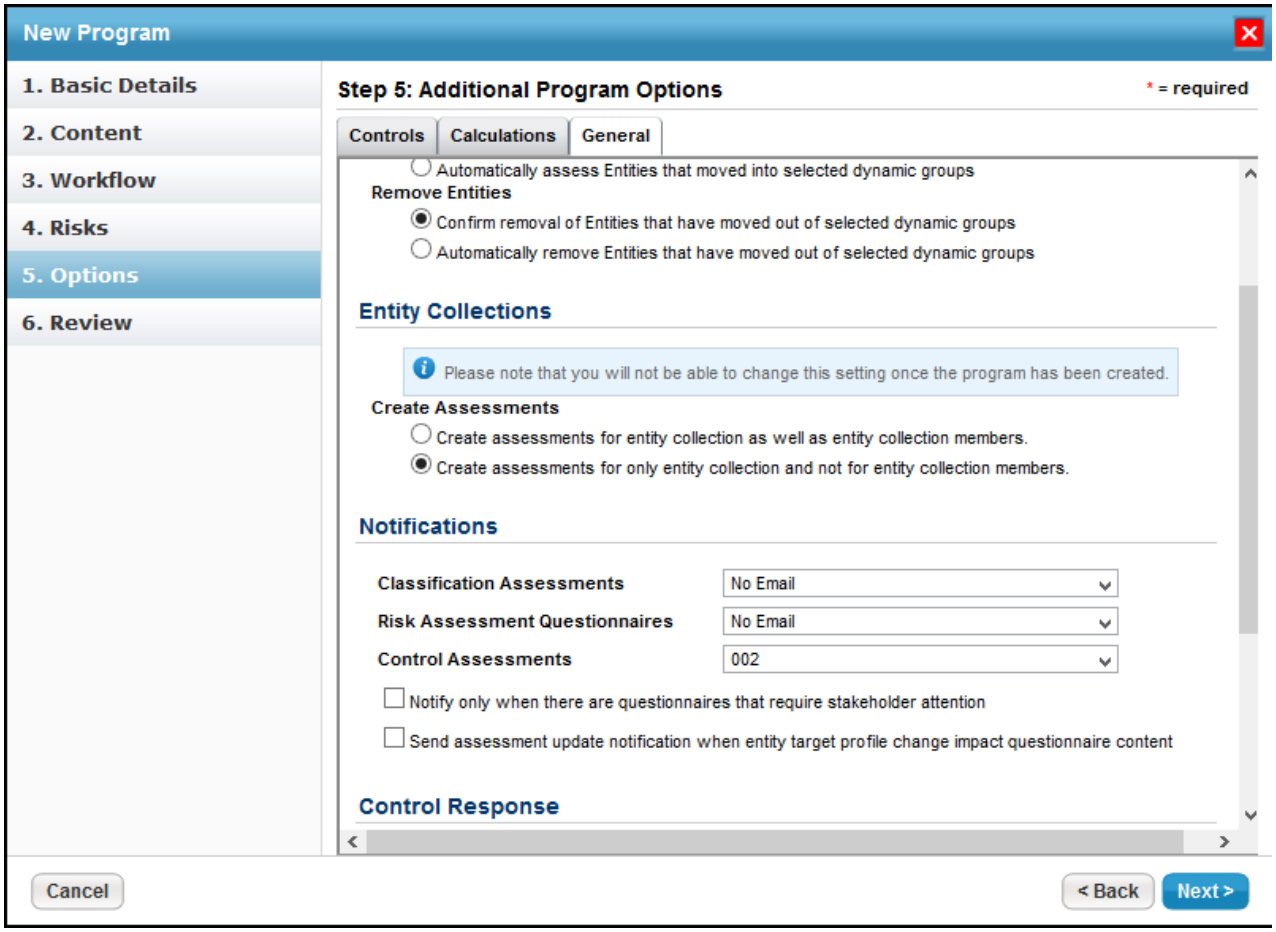


Additionally, you can also import and export questionnaires from the Assessment details page.



Creating an Entity Collection Assessment

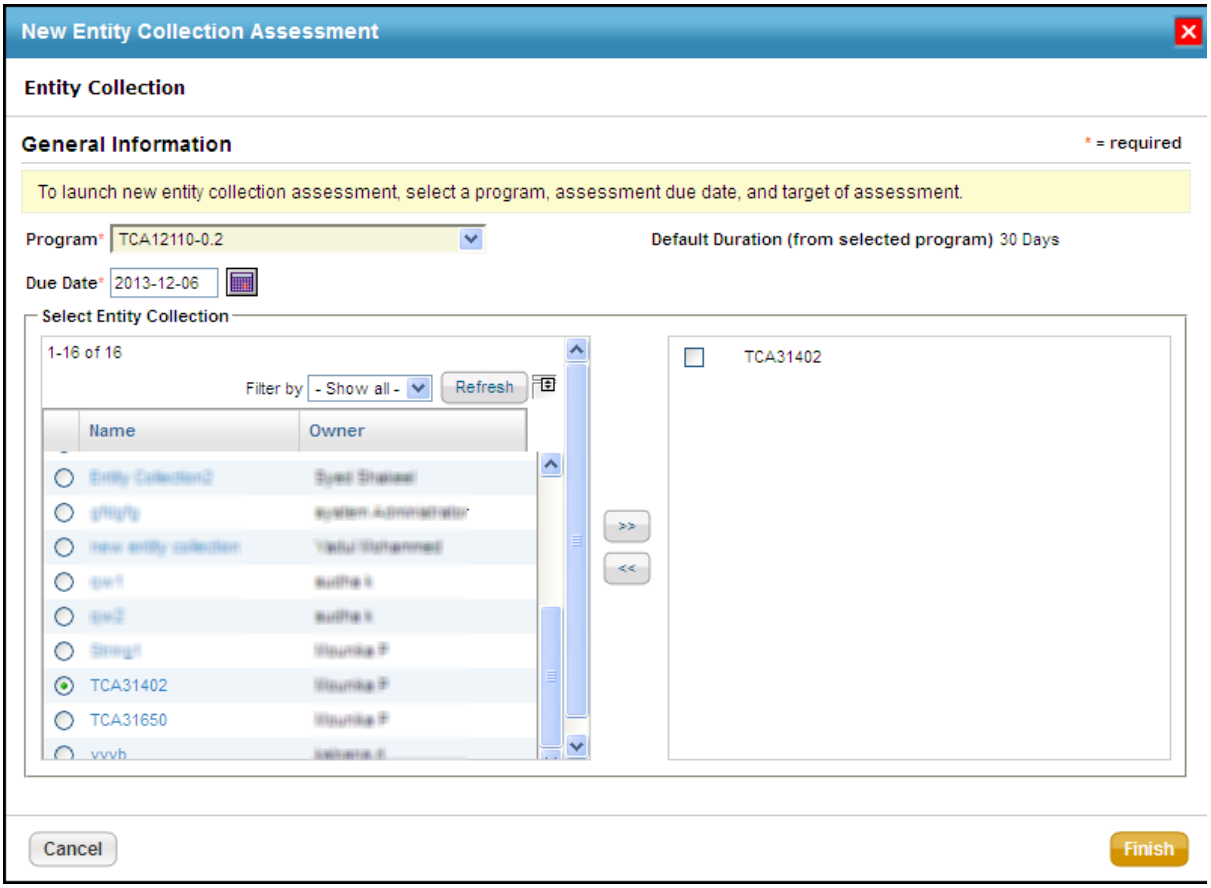
An entity collection ensures that an entity is assessed only once within a program. You can accomplish assessing an entity collection in two ways: assess an entity collection and all of its members, or assess only an entity collection. This behavior is governed by the **Create Assessments** settings of the **Entity Collections** on the **Options** tab of the **New Program** wizard that you will create to run an entity collection assessment. You must determine your entity collection assessment strategy before a program is created. Because once a program is created or if your entity collection assessments are in progress, you would not be able to change the **Create Assessments** settings for the entity collection. By default, the assessments are created only for the entity collection and not for entity collection members. For example, if you have to create an entity collection that comprises of 10 entities and you chose to create assessments for entity collection as well as entity collection members, then 11 assessments will be added to a program.



The Assessment View and Assessment Create permissions allows you to create an entity collection assessment.

To create an entity collection assessment:

1. **In the RiskVision application, go to the Assessments > Assessments page, and click New Entity Collection Assessment. Assessments can also be created from the Assessments tab of an entity's details page or a program's details page.**



2. The **New Entity Collection Assessment** wizard appears with the- **Entity Collection** tab selected. On the **Entity Collection** tab, select a program in the drop-down list. The default duration associated with the program is displayed, and the due date is automatically set to those many days from the current date. You can manually revise the due date if required.

3. In the **Select Entity Collection** pane, select an entity collection to assess, and click **>>** to move that entity collection to the next box. Use **Filter by** to search and select an entity collection.

4. Click **Finish** to exit the wizard and to launch the assessment(s).

Entity collection assessment task limitation

Earlier to release 6.5 SP1, if you have programs that will assess entity collections, such programs will create assessments only for entity collections when you upgrade to v6.5 SP1, but not for its members.

Solution: After upgrading to v6.5 SP1, if you want to create assessments for entity collection and its members (entities), create a new program with the "Create assessment for entity collection as well as its entity collection members" option selected on the Options tab of New Program wizard and then create a new entity collection within that program.

Choosing Entities

Select all target entities you want to evaluate against risk and controls. The entity is automatically assessed using the select controls and questionnaires when you launch the program. To map controls to specific entities, click Advanced Mapping.

You can assign controls and questionnaires to the following:

- **Dynamic groups.** Sort entities automatically based on attributes. Entities are added and removed as their configurations are updated. When a new entity is added to the group, you can configure an assessment to automatically launch as long as the program is open or when the program recurs.
- **Individual entities.** Selects a specific entity only. The select entity is assessed against the selected controls.

To select entities

1. To add a specific entity, select a dynamic group to display a list of entities in Entities pane, select an entity and click the arrow button.
2. To add a dynamic group, expand the top-level group, select a group checkbox and click the arrow button.

The entities move to the selected list.

Launching the Assessment

When you create an assessment, the corresponding questionnaires are created and sent, the automatic checks run, and the assessment process begins. All assessments are automatically moved to the initial stage.

The RiskVision solution verifies settings as transitions through the following launch sequence. If any of the checks fail, the assessments creation and program launch fail. The following table provides a list of possible errors and suggestions on how to correct the issues for a successful assessment launch.

It is recommended to allow sufficient time when consecutively performing the add or delete assessment actions.

Phase	Errors	Remedy
Validation and creating base program	Program Team does not have any members	Add members to the selected team on the Teams page of Users menu, in the Administration application. Remove the team from the Name and owners section. See Naming the program and assigning owners.
	No risk or control selected.	Select a control or questionnaire. See Assigning Controls or Questionnaires
Gathering snapshot of entities	No entities selected.	Select an entity or dynamic group with members. See Choosing Entities.

An assessment fails to launch when you restart the RiskVision Tomcat service while the assessment launch is in progress. This situation will result in the assessment status displaying as "Creation in Progress". In addition, the stakeholders of the first stage do not get notified about the assessment launch. To overcome this situation, recreate the same program assessment. This enables reconciliation of the failed assessment. Be sure that assessments have been launched successfully, however, if assessments still display the "Creation in Progress" status, delete the assessment and recreate it.

Removing an Entity Collection Assessment

You can remove an entity collection assessment within a program, only if you have the Assessment View and Assessment Manage permissions.

To remove an entity collection:

1. In the RiskVision, go to **Assessments** > **Programs**, and select the program to open its details. The **Assessments** tab displays the entity and entity collection assessments.
2. Select the entity collection type assessment and select **Remove**. A confirmation appears asking if you would like to remove the entity collection and its entities.
3. Click **OK**. The entity collection and all of its member assessments are removed.

Managing Entity Collections

You need to manage an entity collection if the entities are added or removed from an entity collection that is being assessed. The most obvious situation is linking a dynamic group to an entity collection. Because the number of entities keep fluctuating in a dynamic group, new entities may become the members of a linked dynamic group, or the existing entities may no longer be a part of the linked dynamic group after an entity collection assessment has commenced. For this reason, you must manage such entities to run your entity collection assessments in a meaningful way.

To manage an entity collection:

1. In the RiskVision Enterprise Risk Manager application, go to **Assessments > Programs**, and select the program to open its details. The **Assessments** tab displays the entity and entity collection assessments.

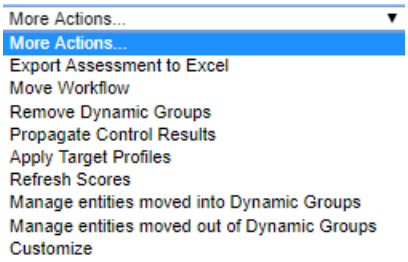
2. Select the entity collection type of assessment and perform the following tasks:

- Select **Manage entities moved into entity collections** in the *More Actions* drop-down list. Then select the newly added entities on the **Entities moved into entity collections** dialog, and click **OK** to add those entities to the entity collection assessment.
- Select **Manage entities moved out of entity collections** in the *More Actions* drop-down list. Then select the entities on the **Entities moved out of entity collections dialog**; (Ctrl+click to select multiple entities), and click **OK** to remove those entities from the entity collection assessment.

For information about how a dynamic group and its members function when added to an entity collection, see Using Entity Collections.

Assessment Actions Overview

This section describes actions that are available in the More Actions drop-down list on the **Assessments** tab of the **Program** details page. Available actions are limited by the assessment status and the user's permissions. Some actions can be performed on multiple assessments at a time.



Action	Description
Export Assessment to Excel	Exports assessment results as an Excel spreadsheet file.
Move Workflow	Perform an action such as Approve or Reject, to move the assessment workflow to another stage.
Remove Dynamic Groups	Removes all dynamic groups that are associated with the specified assessment. For more information, see Remove Entities section in the Options page of New Program wizard.
Restart Assessments	Restarts assessments
Propagate Control Results	Propagates control results for the selected assessments using entity relationships.
Apply Target Profiles	Applies a selected target profile
Refresh Scores	Updates risk and compliance scores. Restarting a closed assessment of a recurring program is one of the instances where this action can be used by a user. **Note:** Refreshing scores may take a few minutes to accomplish.
Manage entities moved into Dynamic Groups	Update assessment entities that have moved into dynamic groups.
Manage entities moved out of Dynamic Groups	Updates assessment entities that moved out of dynamic groups.
Customization	Allows to have a customization of the program page.

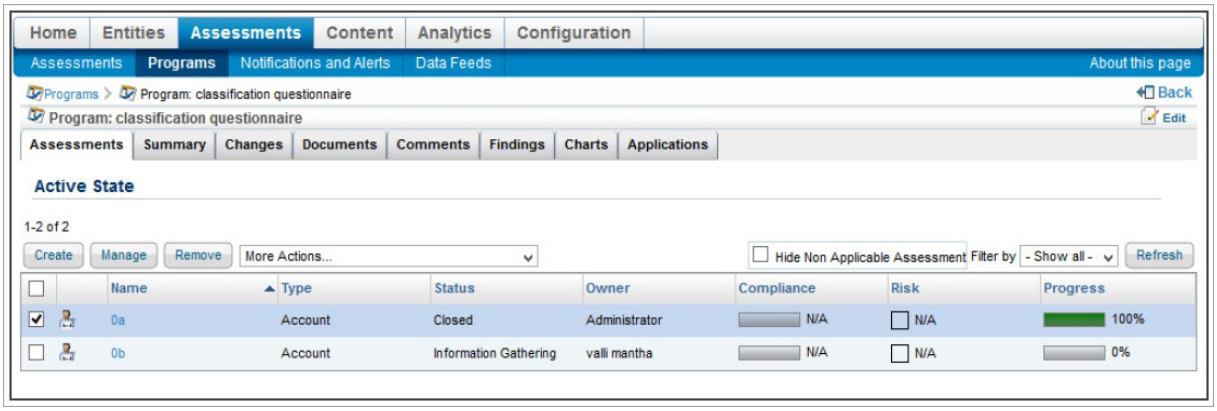
Ensure that you do not update content tied to a program immediately after executing the "*Propagate Control Results*" action. Please wait for at least 30 minutes after executing the "*Propagate Control Results*" action before updating content.

Restart Assessments

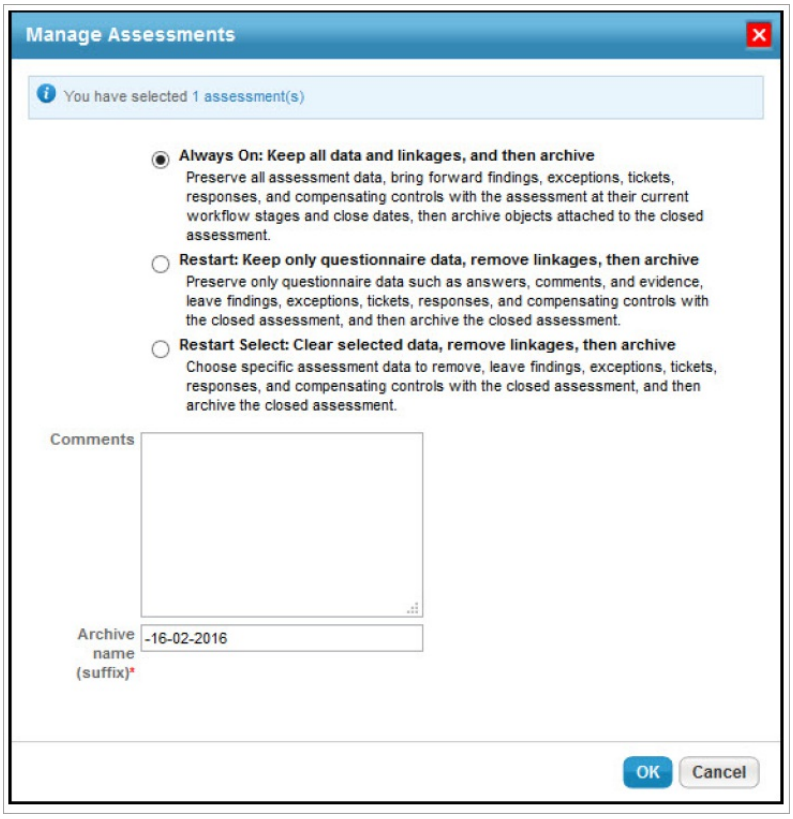
For assessments that you intend to perform more than a single assessment on, you will need to restart the assessment at some point during this process. When you restart assessments, you will have an option to keep some, none, or all of the data for the assessments that you restarted. The rest of this section will discuss these options, as well as all applicable options, for restarting assessments.

To restart assessments:

1. Open RiskVision Compliance Manager.
2. Go to **Assessments** > **Programs**.
3. Select a program to open. Click the **Assessments** tab.
4. Check the box in the closed assessment row, then click **Manage**.



5. Click one of the options in the **Manage Assessments** dialog to select how you want to deal with the objects in the existing closed assessment.



Option	Description
Always On: Keep all data and linkages, and then archive. Preserve all assessment data and bring forward findings, exceptions, tickets, responses, and	Archives the objects associated with the assessment, and then restarts the closed assessment as a fresh new assessment.

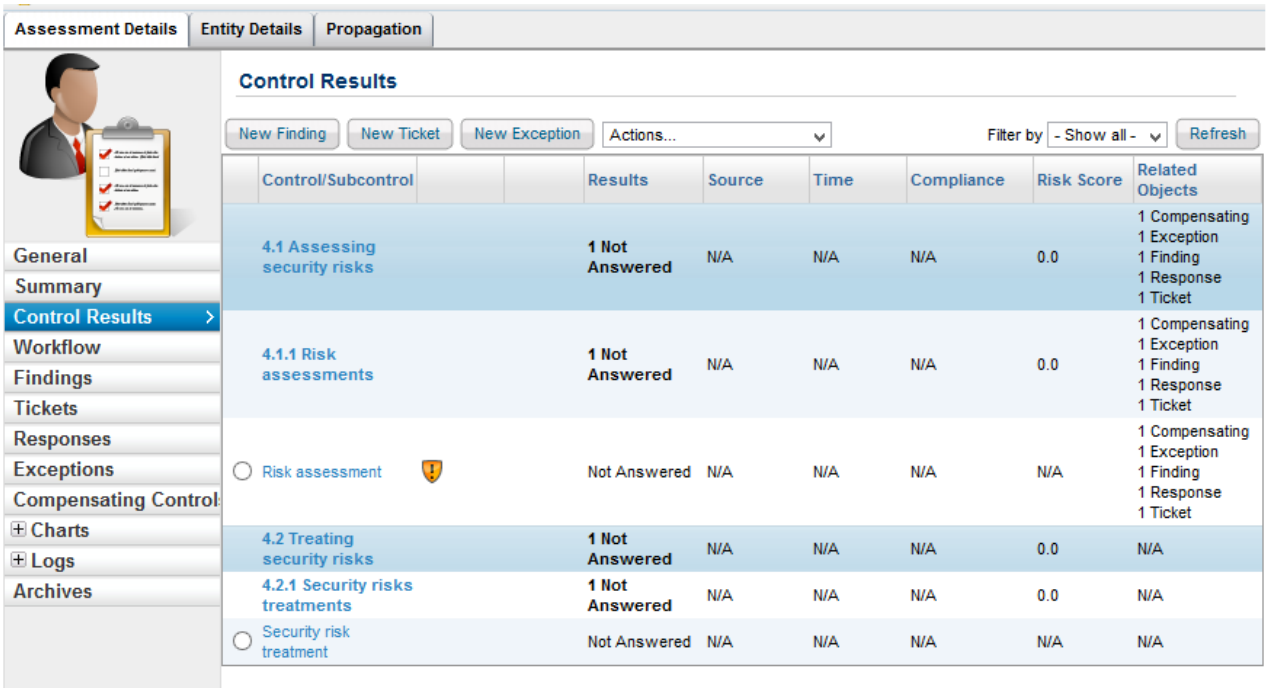
compensating controls with the assessment at their current workflow stages and close dates. Then archive objects attached to the closed assessment. **Note**: You can view this option as enabled when the Always on license key is available.	
Restart: Keep only questionnaire data, remove linkages, then archive. Preserve only questionnaire data, such as answers, comments, and evidence, leave findings, exceptions, tickets, responses, and compensating controls with the closed assessment, and then archive the closed assessment.	Archives the objects associated with the assessment, and then restarts the assessment while including the following read-only objects in the same workflow stage and state: • Assessment answers • Comments in the Comments tab • Implementation details in the Implementation tab • Remediation comments in the Remediation tab • Evidence • Findings - This includes the exceptions, responses, and tickets attached to a finding. • Tickets • Exceptions • Responses • Compensating controls
Restart Select: Clear selected data, remove linkages, and then archive. Choose specific assessment data, to remove, leave findings, exceptions, tickets, responses, and compensating controls with the closed assessment, and then archive the closed assessment.	With this option, you can remove specific objects linked to the assessment. Available options include: • Clear answers; • Clear comments - general; • Clear comments - implementation; • Clear comments - remediation; • Clear compensating controls; • Clear evidence; • Clear exception requests; • Clear findings; • Clear responses; and • Clear tickets. **Note**: If you are unable to view the options compensatory controls, exceptions, findings, responses, and tickets set the property #assessment.restart.clearAssessmentData.showHiddenOptions as true. (By default this property is set as false.)

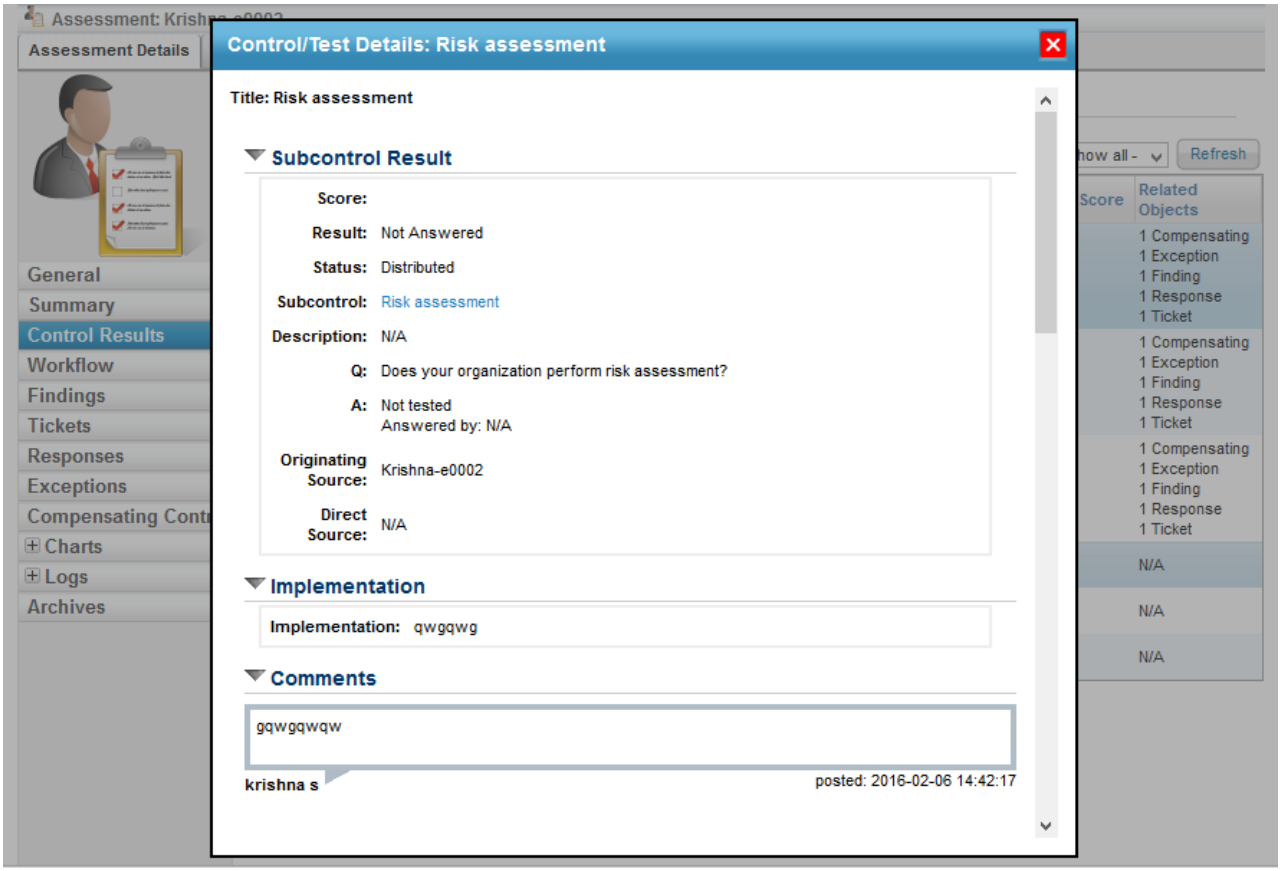
5. Click **OK**.

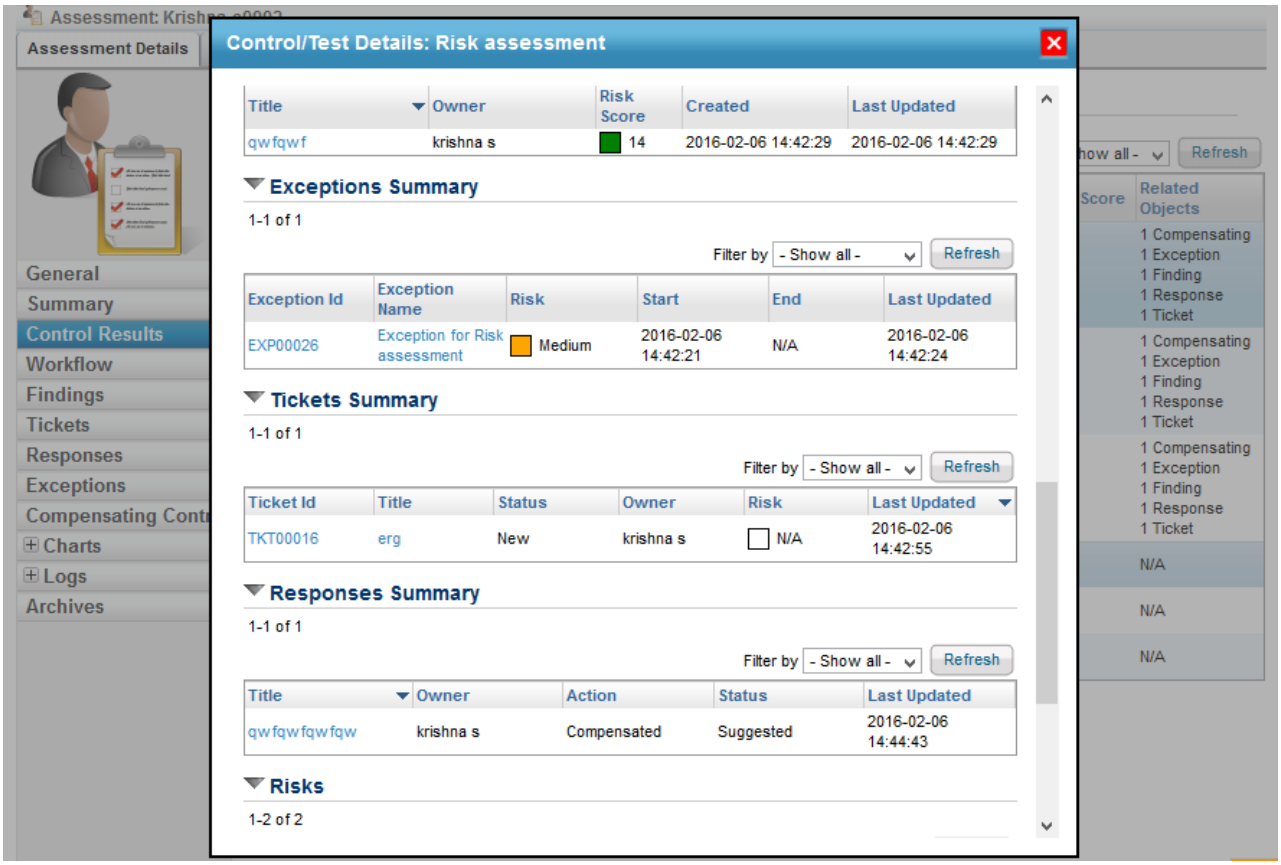
The archived objects will appear identical to the live view of assessments and response objects. However, they are in a read-only state and cannot be edited. The archived objects will show the same details of the state that they were in at the time when they were archived. The workflow options will no longer be available, and the workflow history will show the stage of the object as well as the workflow history prior to the point of archival.

Assessments restarted with the **Always On** Assessments functionality will not be available until the **Assessment Objects Carry Forward** and the **Update Questionnaires for Always On Assessments** jobs have run. The **Assessment Objects Carry Forward** job is required to archive questionnaire data and objects attached to the assessment, such as findings, tickets, exceptions, and responses, and to carry forward these objects to the continuous assessment. The **Update Questionnaires for Always On Assessments** job is required to ensure that the questionnaires for **Always On Assessments** appear on the **Home** > **Questionnaires** page of each user who is assigned questions for the continued assessment.

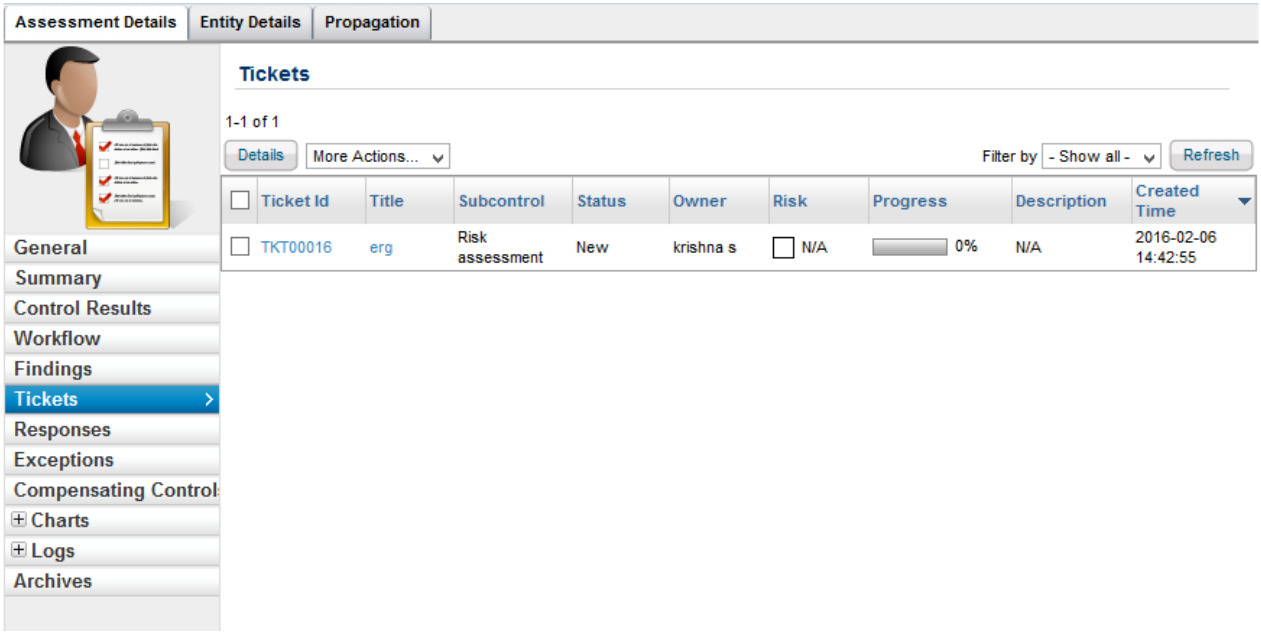
Control Results


Assessment Details
Entity Details
Propagation
Control Results
New Finding
New Ticket
New Exception
Actions...
Filter by - Show all -
Refresh
Control/Subcontrol
Results
Source
Time
Compliance
Risk Score
Related Objects
4.1 Assessing security risks
1 Not Answered
N/A
N/A
N/A
0.0
1 Compensating
1 Exception
1 Finding
1 Response
1 Ticket
4.1.1 Risk assessments
1 Not Answered
N/A
N/A
N/A
0.0
1 Compensating
1 Exception
1 Finding
1 Response
1 Ticket
Risk assessment
Not Answered
N/A
N/A
N/A
N/A
1 Compensating
1 Exception
1 Finding
1 Response
1 Ticket
4.2 Treating security risks
1 Not Answered
N/A
N/A
N/A
0.0
N/A
4.2.1 Security risks treatments
1 Not Answered
N/A
N/A
N/A
0.0
N/A
Security risk treatment
Not Answered
N/A
N/A
N/A
N/A
N/A
General
Summary
Control Results
Workflow
Findings
Tickets
Responses
Exceptions
Compensating Control
Charts
Logs
Archives

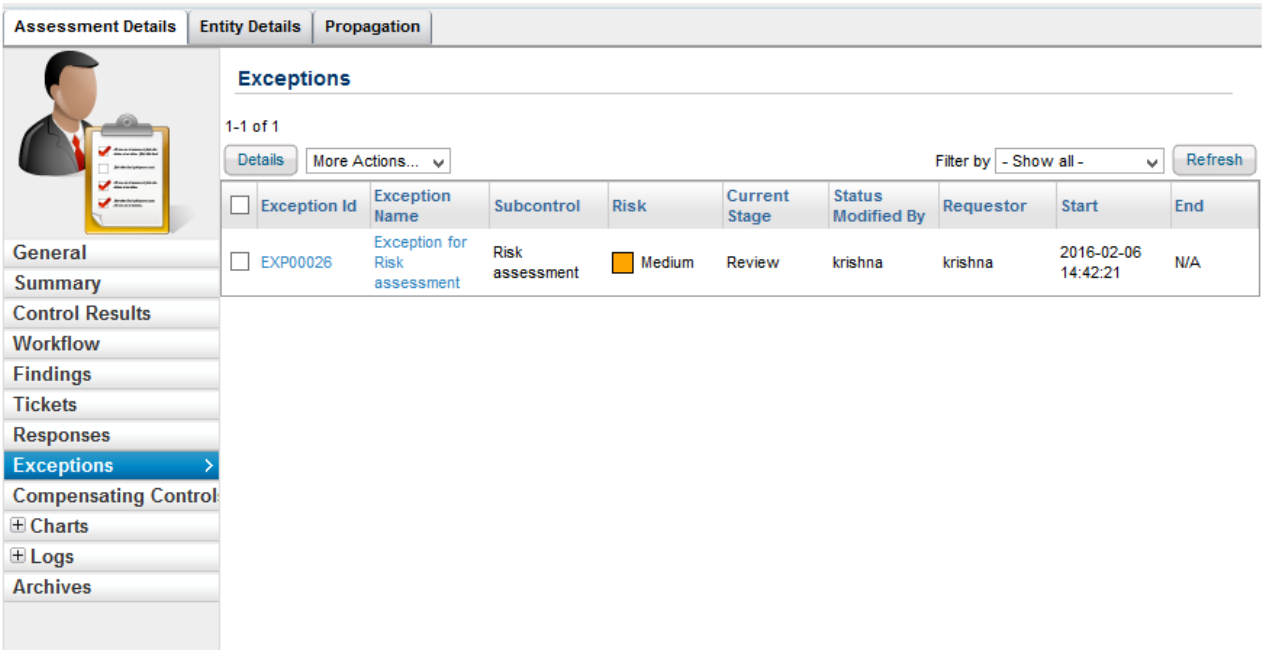

Assessment: Krishna-e0002
Assessment Details
Control/Test Details: Risk assessment
Title: Risk assessment
Subcontrol Result
Score:
Result: Not Answered
Status: Distributed
Subcontrol: Risk assessment
Description: N/A
Q: Does your organization perform risk assessment?
A: Not tested
Answered by: N/A
Originating Source: Krishna-e0002
Direct Source: N/A
Implementation
Implementation: qwgqwg
Comments
gqwgqwqw
krishna s
posted: 2016-02-06 14:42:17
General
Summary
Control Results
Workflow
Findings
Tickets
Responses
Exceptions
Charts
Logs
Archives



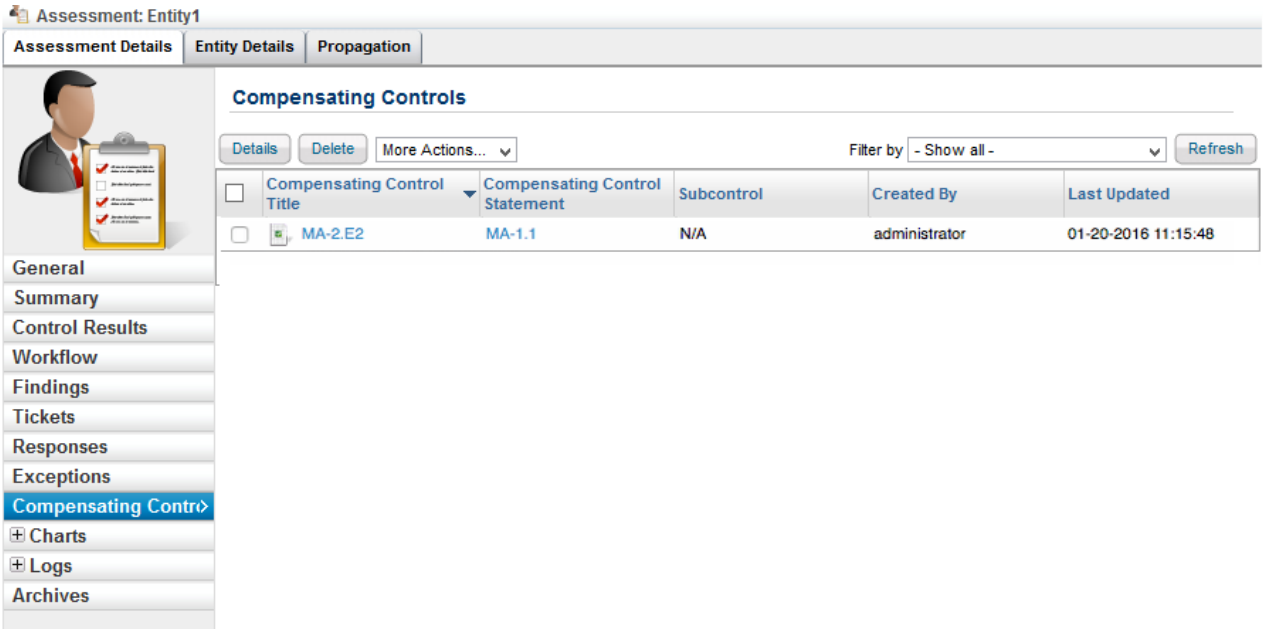
Tickets



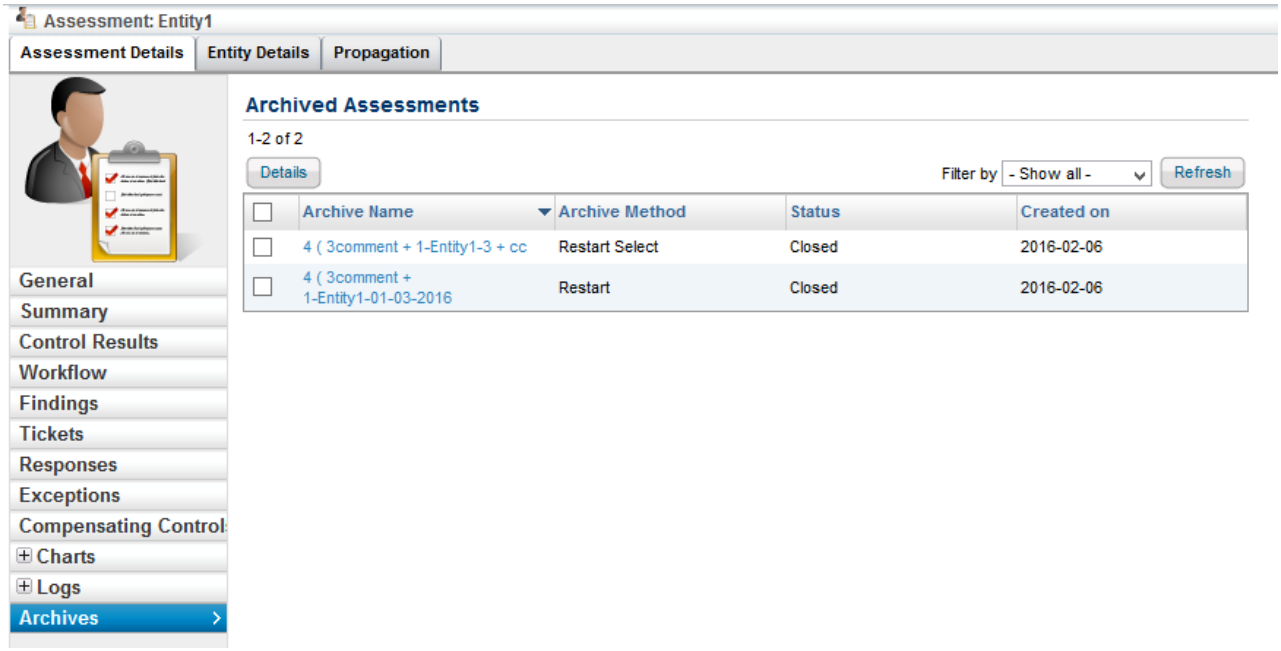
Exceptions



Compensating Controls



Archived Assessments

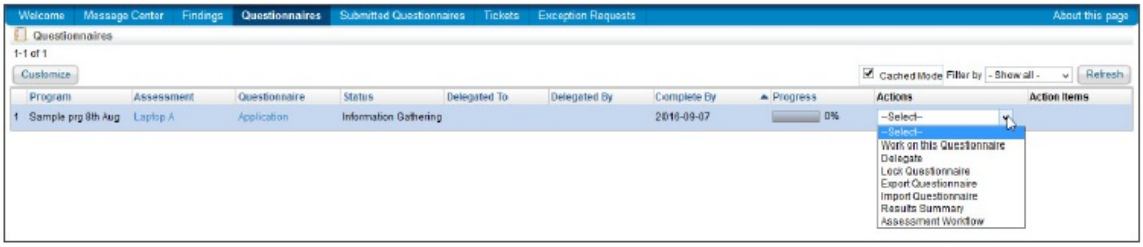

Assessment: Entity1
Assessment Details
Entity Details
Propagation
General
Summary
Control Results
Workflow
Findings
Tickets
Responses
Exceptions
Compensating Control
Charts
Logs
Archives
Archived Assessments
1-2 of 2
Details
Filter by - Show all -
Refresh
Archive Name
Archive Method
Status
Created on
4 (3comment + 1-Entity1-3 + cc
Restart Select
Closed
2016-02-06
4 (3comment + 1-Entity1-01-03-2016
Restart
Closed
2016-02-06

About the Questionnaire Answering Interface

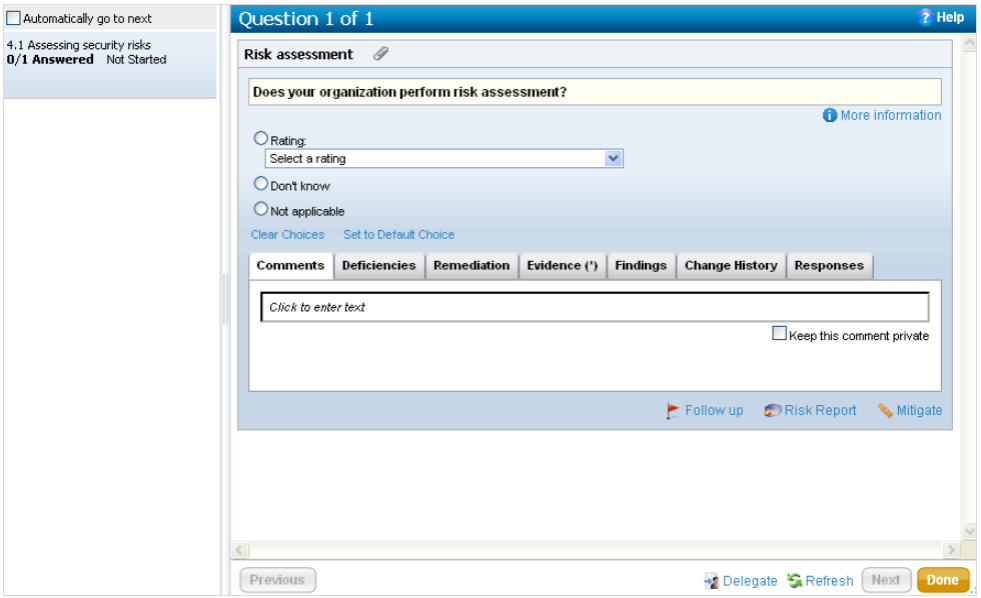
To answer a questionnaire, you must have the Questionnaire Answer permission.

To view the Questionnaire Answering Interface from the Questionnaires page, choose anyone of the below mentioned options:

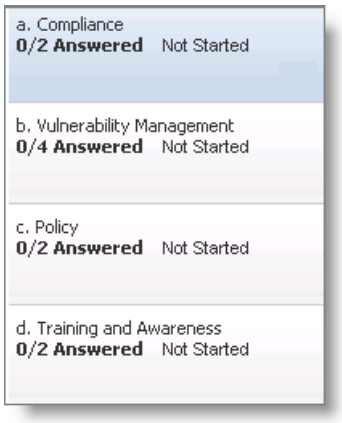
- Click the **Questionnaire** link
- In the **Actions** drop-down list, choose the below:
    - **Work on this Questionnaire**
    - **Resume Questionnaire**



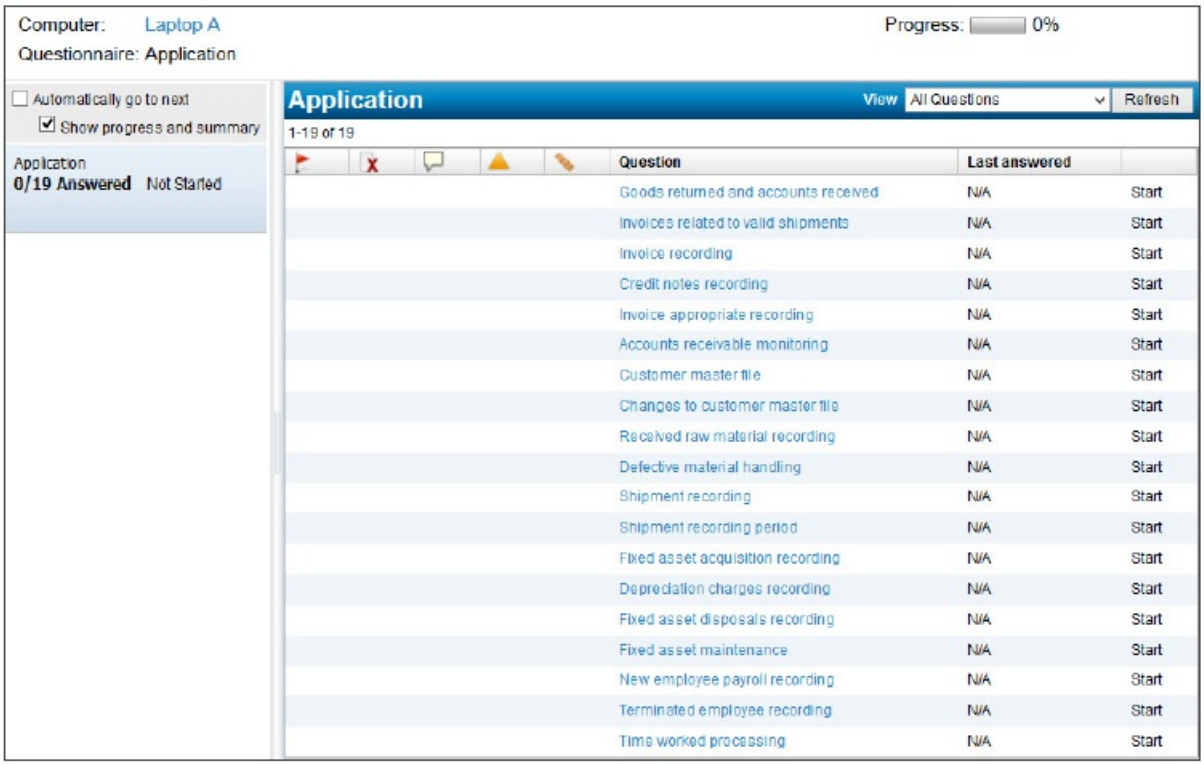
The **Questionnaire Answering Interface** page appears as shown below:



- The left side navigation pane displays the questionnaire details and if the questionnaire is subdivided into sections pertaining to a specific policy or control the sections of the questionnaire. Click the section to display a table with a list of questions in the main pane.
- The sections of the questionnaire displays the controls and policy titles, the number of questions in the section, and status.



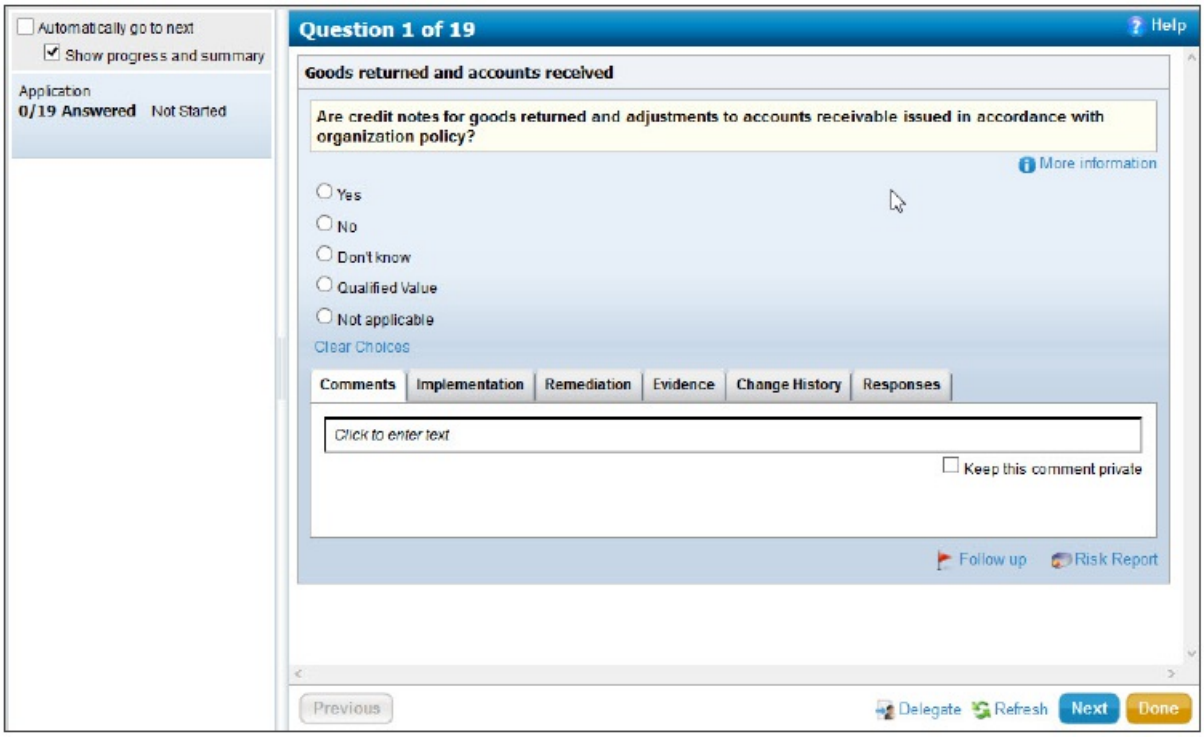
- Click this section to display a list of questions in the main pane. The right side pane displays a list of questions in case there are more than one question. The questionnaire details include the assessment name, the entity name, the stage progress and the questions.



The actions associated with the questions are displayed with icons as shown below:

Icons	Description
	Flagged for follow-up
	Answer requires resolution
	Comments
	Exception
	Mitigation
	Evidence

- Click the question to open it in the main pane.



- The questions are displayed in the right-hand side of the window. You can specify an answer or rating for each question and then click the Previous or Next button to move to the next question.

Some questions are designed to have dependent questions, such that when a user selects a choice, it enables the dependent question.

- Click the **Done** button, to stop the questionnaire-taking process. User is navigated to the **Thank You** page.
- Select any one of the options below:
  - Select **Submit for Review**, when user wants to submit the questionnaire and move to the workflow stage 'Review' after all questionnaires are submitted.

    OR

  - Select **Close now and resume later**, when user is not done with this questionnaire, but wants to close it for now and resume later.

Questionnaire-taking preferences associated with an assessment determine specific behavior and options available to questionnaire-takers. For example, you may have an option Skip Answered Questions, then the questionnaire display skips next or previous questions that have already been answered.

View Program Details

Programs in RiskVision Compliance Manager display their results in a tabbed view under **Assessments** > **Programs**. Click the program of interest to display the assessments, changes, findings, associated documents, relationships, and more. It is possible to drill down further into the underlying data of a program. A"breadcrumb" line in the upper left of the window contains a navigation trail and allows you to click to return to any level.

The tabs on a program details page include:

- **Assessments**. The Assessments tab contains running and closed assessments. Here you can create a new entity and entity collection assessments, remove assessments, and manage assessments using the actions available in the More Actions drop-down list. For information about each action option, see Assessments Actions Overview.
- **Summary**. The Summary tab displays the details you entered when creating a program. In other words, it displays the information that was entered by you on each program wizard page.
- **Changes**. The Changes tab contains the Assessment Activity and Changes sections. The Assessment Activity section displays the last updated date of assessment, the last run time of the Dynamic Group Entity Map Builder and Dynamic Group Entity Map Updater jobs, and the number of entities moved into and out of dynamic groups. The Changes section allow you to apply the changed controls and the changed questions to the assessments. For more information about how to apply the changed content, see Updating Content.
- **Documents**. The Documents tab allows you to manage documents and web links. For more information, seeDocuments.
- **Comments**. The Comments tab allows you to enter comments.
- **Findings**. The Findings tab displays the findings in different assessments.
- **Charts**. The Charts tab contains charts on entities, controls, questionnaires, and vulnerabilities in different formats.
- **Application**. The Application tab displays the application(s) in which a program can be accessed. For more information, see Controlling Object Visibility.
- **Relationships**. The Relationships tab displays the entity relationships in different graphical layouts.

Synchronizing the Changes in a Program

When content and workflow which are a part of the program, undergo any changes, the program will also need to be updated to synchronize the changes so that all assessments within that program receive the changes and continue to function in a meaningful way. You can use the following options to synchronize the changes in a program:

- Synchronizing the Workflow
- Updating Content

Synchronizing the Workflow

If you make any modifications in the workflow that is associated with a program, you will need to make sure that changes are experienced at the program level as well.

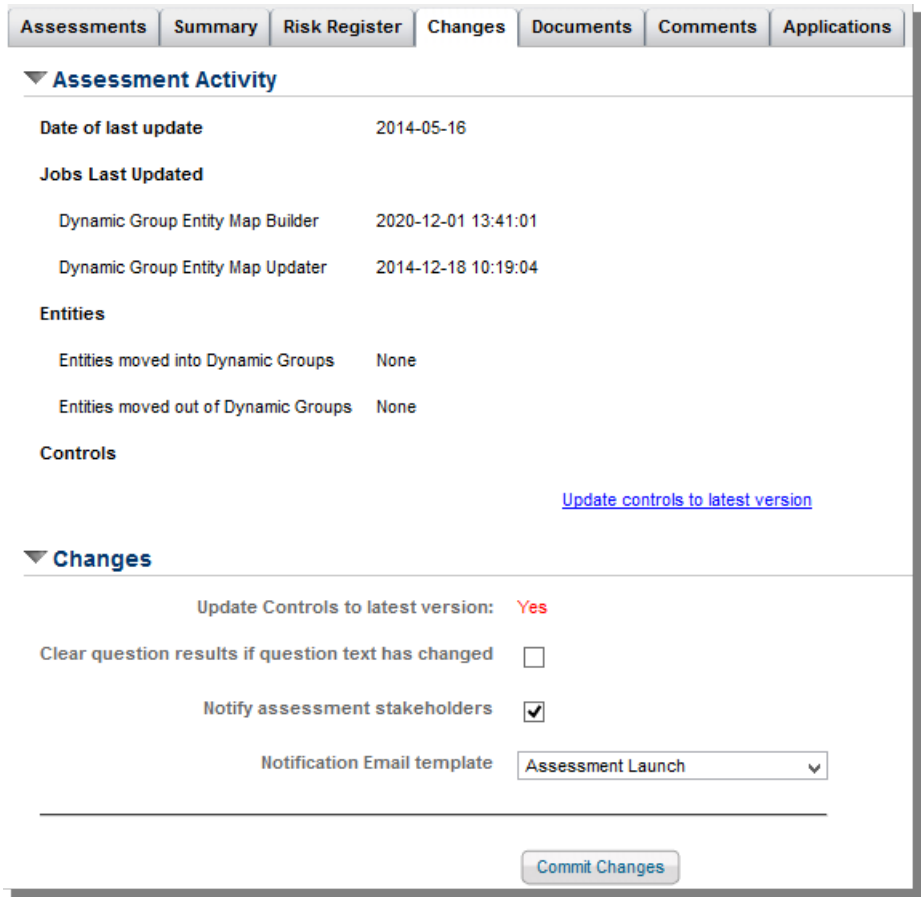
1. Go to **Assessments** > **Programs**.
2. Locate the program of interest, check the box next to the program, and then select **Synchronize Workflow** in the **More Actions** drop-down list. A prompt box appears asking if you would like to synchronize the selected program with the latest template. Click **Yes** to inherit the changes. Note that the **Synchronize Workflow** action cannot be reverted.

Updating Content

You may always want to update the content to incorporate the changes suggested by your auditors. When the content that is being used in a program is changed, you must update the controls to the latest version.

To update the controls to the latest version at program level:

1. **Go to Assessments > Programs.**
2. Locate the desired program and select the program to open its details.



3. Click the **Changes** tab, and click the **Update controls to the latest version** link which appears at the bottom of the **Assessment Activity** section. Then set the following options in the **Changes** section:
   - Update Controls to the latest version. By default, this option is selected as 'Yes' so that controls are updated to the latest version.
   - Clear question results if question text has changed. If the questions in the content are changed, you may check this option to clear the answers to the questions provided by the stakeholders when a questionnaire is in progress.
   - Notify assessment stakeholders. By default, stakeholders are notified about the change in content. Clear this option if you do not want the stakeholders to know about the change in content.
   - Notification Email template. Select an appropriate template to send an email to stakeholders.
4. After you set the options, click **Commit Changes**.

Each time the workflow attached to the control or control objective is moved to the deployed stage, the version number is automatically incremented.

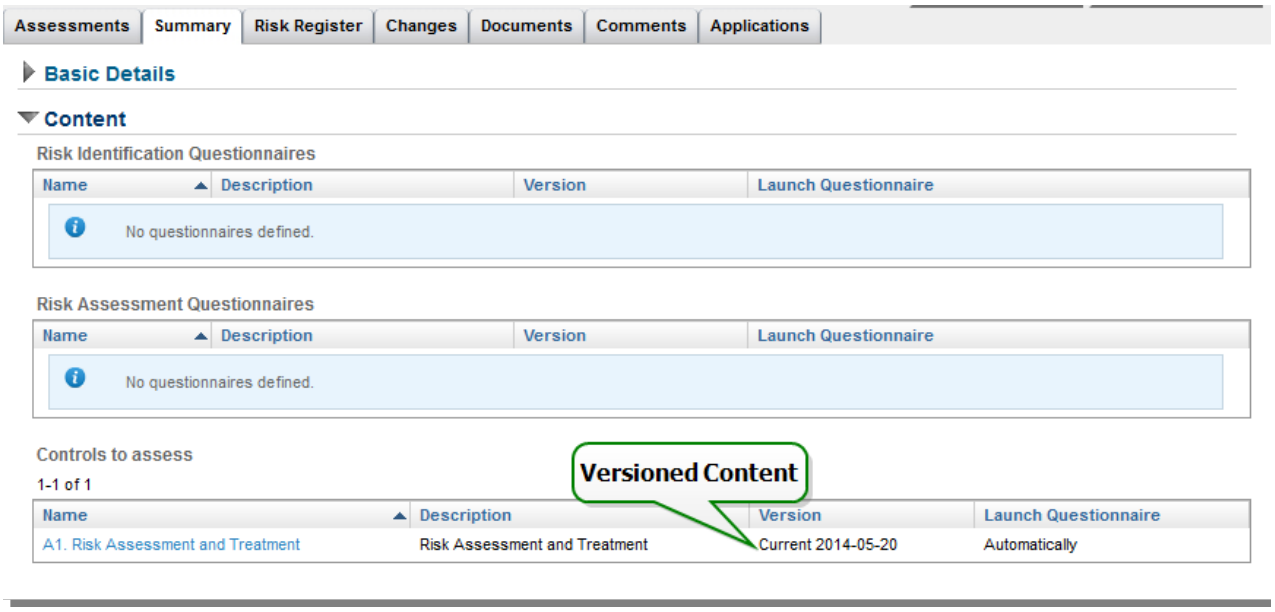
You will not be able to update the content changes for assessments in read-only or closed stage.

Ensure that you do not update content tied to a program immediately after executing the "*Propagate Control Results*" action. Please wait at least 30 minutes after executing the "*Propagate Control Results*" action before updating content.

Viewing Content Version

Content versions can be viewed on the **Summary** tab of **Program** details page. Only the controls and/or questionnaires that are created within a content pack or control objective will be versioned when the workflow associated with a content pack or control objective is moved to the deployed stage. Only the latest version of the deployed content is visible in the **Content** section of the **Summary** tab. But to be able to incorporate the content changes in your program, you must update the controls at the program level. For information about how to apply the content changes at a program level, see Updating Content under the Synchronizing the Changes in Program topic.

The following graphic shows the version information of the content in the **Content** section.



Viewing Assessments Based on Group Definitions

Viewing assessments requires the Assessment View permission to be assigned to your user role. Users with the Assessment Manage permission can view all assessments irrespective of the ownership, whereas users with Assessment View permission can only view their own assessments.

By default, the **Assessments** grid displays the entity assessments by of the attributes you have specified to group the entities. You can enable the Assessments hierarchical tree on the left-side of the **Assessments** grid to provide a number of default categories or virtual groups as nodes for displaying specific entity assessments.

To enable the Assessment hierarchical tree:

1. In the directory `%AGILIANCE_HOME%\config` , open the .propertiesfile using a text editor, and add the property assessments.landing.page.shownavigation=true.
2. Reload the server configuration to apply the latest changes.

Viewing Assessment Details

The **Assessment Details** page contains interdependent tabs with in-depth information for your analysis. Only a program owner or an assessment owner can access the **Assessment Details** page. Click a tab to understand how different stakeholders have responded in identifying or mitigating the risks. By default, the following tabs are visible on the **Assessment Details** page:

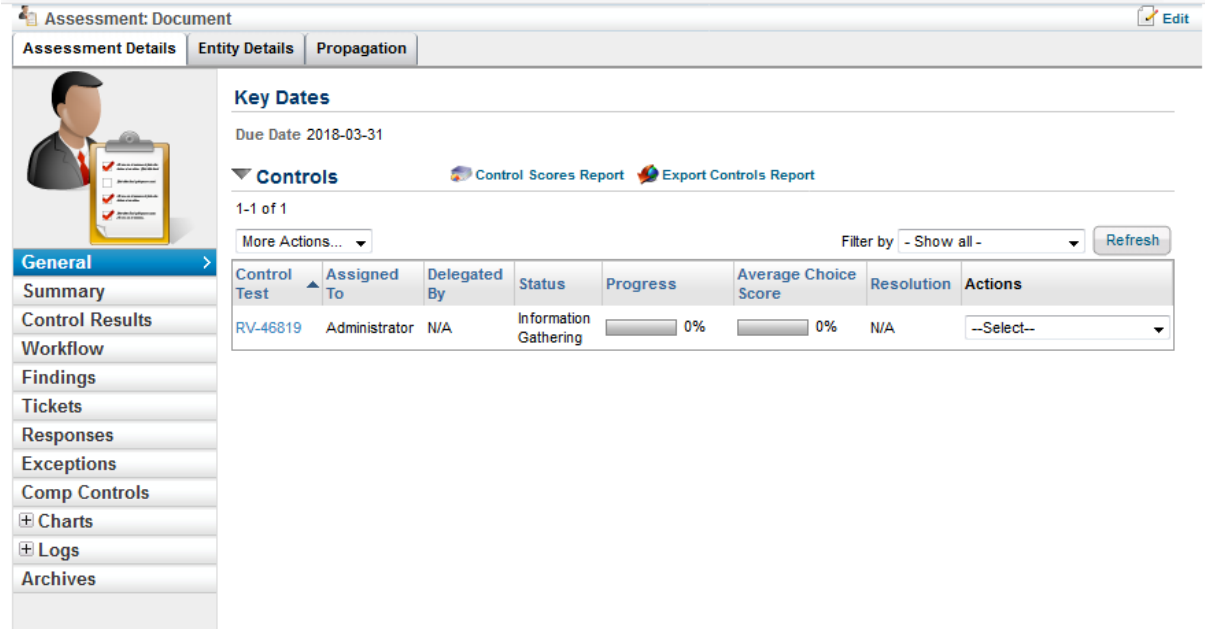
Actions	Description
General	This tab provides a questionnaire's details, such as progress, workflow status, average choice score, and the owner of workflow stage.
Summary	This tab contains the default dashboards – Overall Compliance, Risk Score, and more. In addition, the Workflow section shows you the current stage of the assessment.
Findings	This tab lists all the findings associated with an assessment. For information about how to create a finding, see Findings.
Control Results	This tab provides details about the stakeholders' answer choices for controls and subcontrols that are in place for risks. Using the control results, the compliance and risk scores are calculated. Risks that are associated with weak or unfit controls, or when no controls are in place, stakeholders will respond to using one or more response control mechanisms that are stipulated by the program owner. In the Response column, you can view a stakeholders' response for the controls which do not meet your objective.
Responses	This tab provides details about responses that are created by stakeholders for the purposes of overriding the compliance score and mitigating the finding score. For information about how to create a response, see Responses.
Tickets	This tab lists all the tickets associated with an assessment.
Exception	This tab provides details about exceptions that are created by stakeholders for the purposes of overriding the compliance score of a subcontrol.
Workflow	This tab provides current and historical details of a workflow. You can view the workflow current stage details, such as stage name, owner, and time since the workflow entered into current stage. The Status History section shows complete stage transition information for transitions that have already occurred.
Comp Contrtols	This tab lists all the compensating controls associated with an assessment.
Charts	This tab contains charts and information that display the security risk score, compliance and risk score history, and data feeds.
Logs	This tab provides information about evidences and workflow.
Archives	This tab provides a list of all archived assessments.

Adjusting Assessment Due Dates

For every assessment that you perform, there will be an associated deadline. If you have not closed the assessments by the due date and have received the time extension for completing the pending items, you can adjust the assessment due date so that every stakeholder knows of the current due date.

To adjust assessment due date:

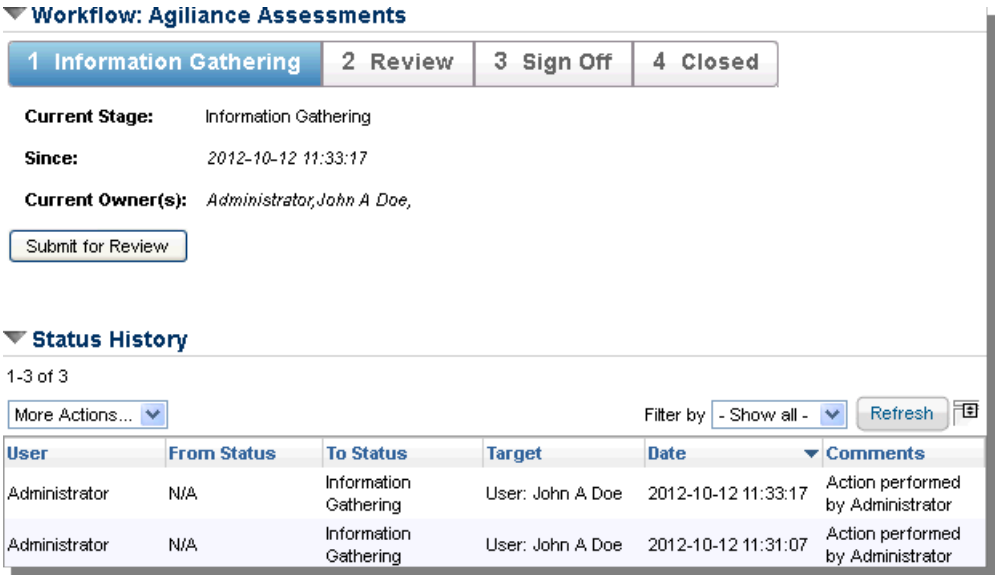
1. In the RiskVision application, go to **Assessments > Assessments**. The **Assessments** page is displayed.
2. Select an assessment to open its details page, and displays the **General** tab.



3. Click **Edit** at the upper top-right corner.
4. Click the icon associated with the **Due Date*** field and select a date of interest.
5. Click **Save** at the upper top-right corner. The due date is adjusted.

Monitoring Assessment Progress

After you launch the assessment, as a program owner or assessment owner, you must track the progress on all assessments or an individual assessment. By navigating to the **General** and **Workflow** tab of **Assessment** details, you can monitor the details of workflow stage information, such as progress, average choice score, names of stakeholders working on the current workflow stage, and the date since the workflow entered a particular stage. That means you will know since how many days the current stage stakeholders are working on the questionnaire. Moreover, you can mouse hover a stage name to know which stakeholders will work on the questionnaire when the workflow is transitioned to the next stage and its subsequent stages.



The workflow status history provides a complete log of activities until the assessment is closed, and the log is updated again when the assessment is re-started.

Understanding Assessment Propagation Details

After stakeholders answer the assessment(s), the propagation details in the assessment details page allow you to view inherited controls, direct controls, and propagated results. Data will only be populated in the **Propagation** tab when the entity or entity collection is related to another entity or entity collection and propagation is enabled for that relationship. The **Propagation** tab in the assessment details page is only visible if you have the Assessment Manage permission.

The **Propagation** details tab includes the following tabs:

1. **Inherited Controls** - This tab contains controls and subcontrols inherited from a related entity or entity collection. In order to be inherited, controls must have been published by the entity or entity collection that is propagating the results. Inherited controls will be automatically updated when an assessment associated with an entity or entity collection is related to the current entity or entity collection, either directly or indirectly, is answered, added to, or removed from the program. If you decide that, instead of inheriting a control result that you would rather meet a control on your own, you can override the inherited controls by selecting the winning control or subcontrol. For more information about choosing a winning control, see Overriding Inherited Controls. To completely remove the inherited result, select the control/subcontrol, and click **Revoke Inherited Results**. This will effectively remove the inherited control result and insert the question for the specific control result that was revoked, into the assessment questions for your entity or entity collection.

   An entity or entity collection can be automatically subscribed to two or more of the same controls/subcontrols. When you come across this kind of situation, the RiskVision system helps an entity or entity collection automatically subscribe the result that adheres to the following rules of precedence:

   - Intrasystem relationships take precedence over intersystem relationships. For example, if an entity is a member of an entity collection and has a relationship with another entity, then that entity inherits the controls/subcontrols of the entity collection.
   - If there are multiple intersystem relationships, the result with the highest score shall win.

2. The grid in this tab provides inherited controls details, such as which controls and subcontrols are inherited, their originating source, direct source, type, and compliance score. The Originating Source represents the entity or entity collection that is propagating the control or subcontrol and the Direct Source indicates the immediate entity or entity collection relationship with which the receiving entity or entity collection has established.

3. **Direct Controls** - This tab contains controls and subcontrols that are directly mapped to an entity or entity collection. The inheriting controls and subcontrols do not appear in this tab; they will appear only after you revoke any inherited controls.

4. **Propagated Results** - This tab contains controls and subcontrols that can be propagated to a related entity(s) and entity collections. You can choose to propagate none, a few, or all of the controls and subcontrols. For entity collections, you can also choose to propagate to entity collection members.

   The following options are available to manage propagation results:

   - Propagate Externally. Enables results to propagate down to the related entity. This option is available for both entity and entity collection. The recipient can also be an entity or entity collection.
   - Propagate Internally. Enables results to propagate down to only the members of an entity collection. This option is available only for entity collection.
   - Do not Propagate. Enables to stop propagating the results. This option is available for both entity and entity collection.

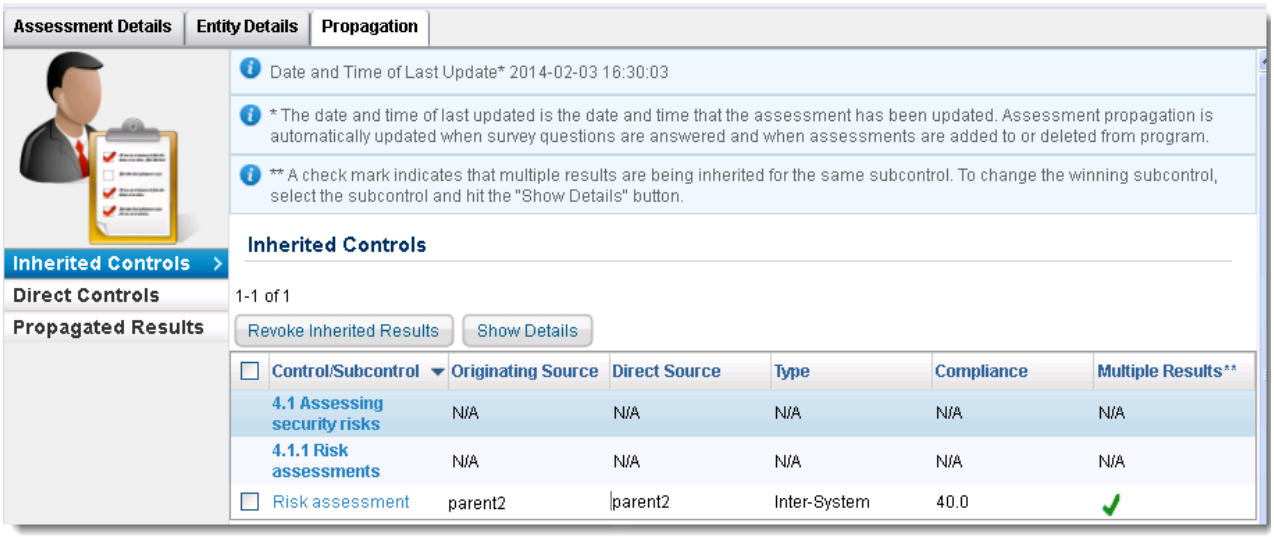
Note: Propagation of control results is not currently supported for dependent questions.

Overriding Inherited Controls

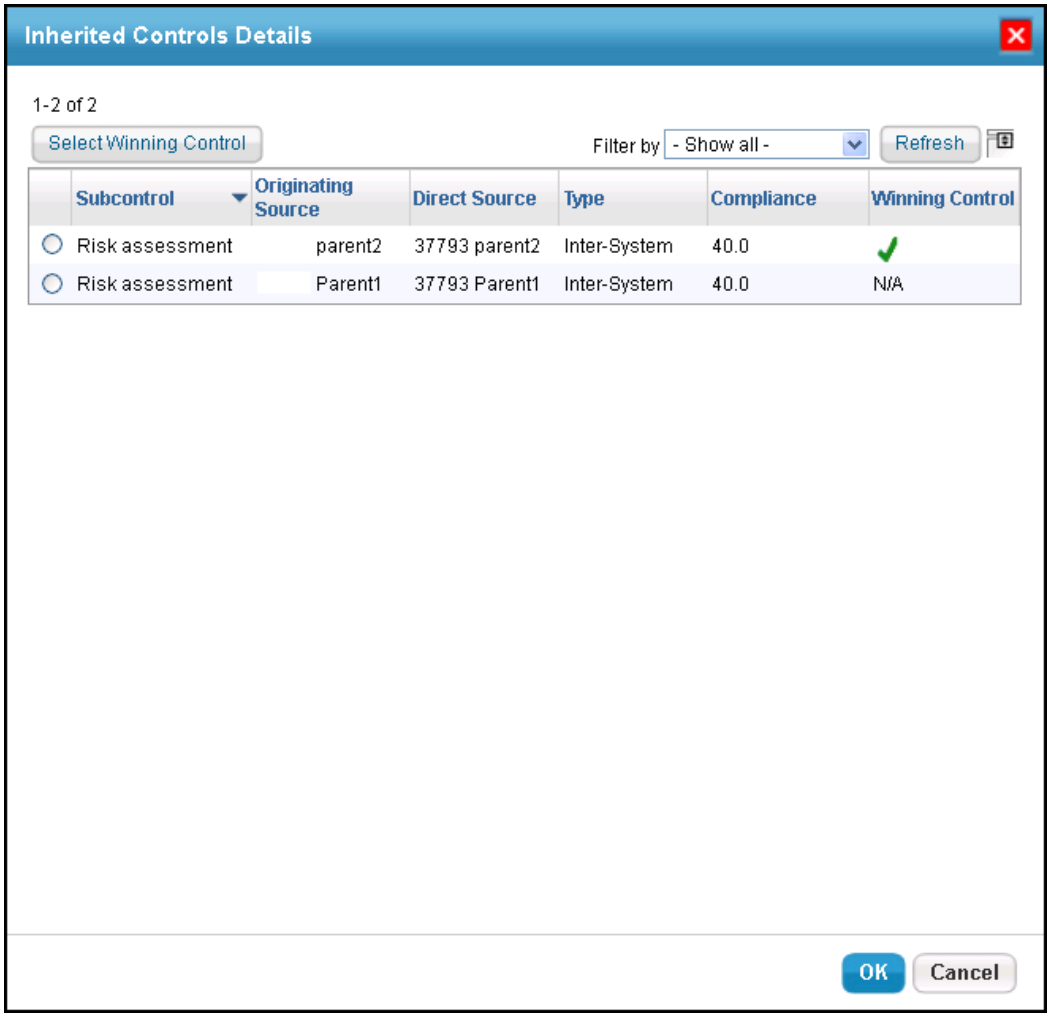
When an entity or entity collection inherits two or more of the same controls/subcontrols rather than accepting the auto-subscribed results, you can choose the winning control/subcontrol on your own.

To override an inherited control:

1. In the RiskVision application, go to **Assessments** > **Assessments**. The **Assessments** page is displayed.
2. Select an assessment to open its details page and click the **Propagation** tab to display the **Inherited Controls Details**.



3. Check the box next to the control/subcontrol for which you would like to select a winning control, and then click **Show Details**. The **Inherited Controls Details** dialog appears.



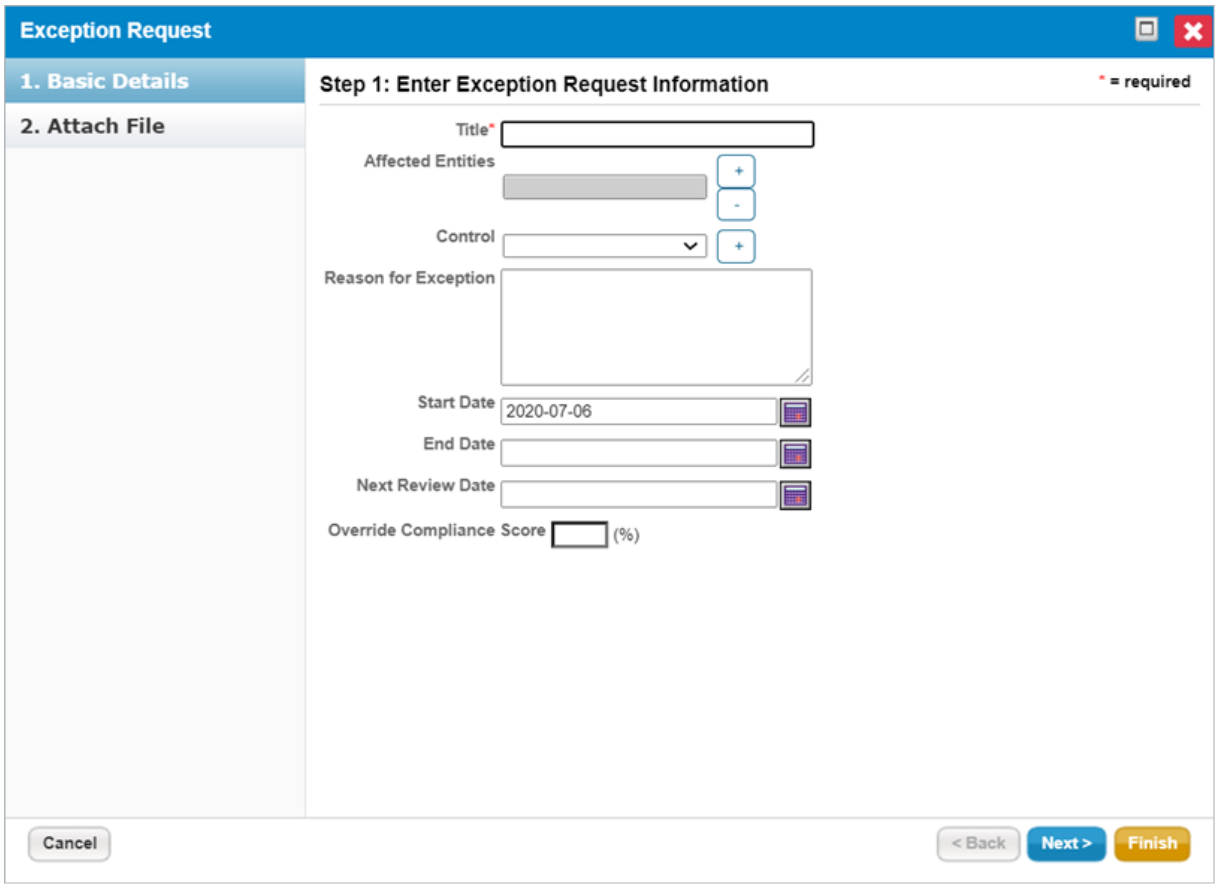
4. Choose a control/subcontrol instance, and click **Select Winning Control**.
5. A message to confirm the selection of winning control appears. Click **OK** to select the winning control.
6. Click **OK** to exit the **Inherited Controls Details** dialog. The newly-created winning control has overridden the inherited control/subcontrol.

Create an Exception Request - Assessment

You can create an exception for an entity, a failed control, or any control that is not compliant. An exception for a failed control can be created on the **Assessment Details** page > **Control Results** tab or **Exception** tab, or on the **Home** > **Exceptions** page.

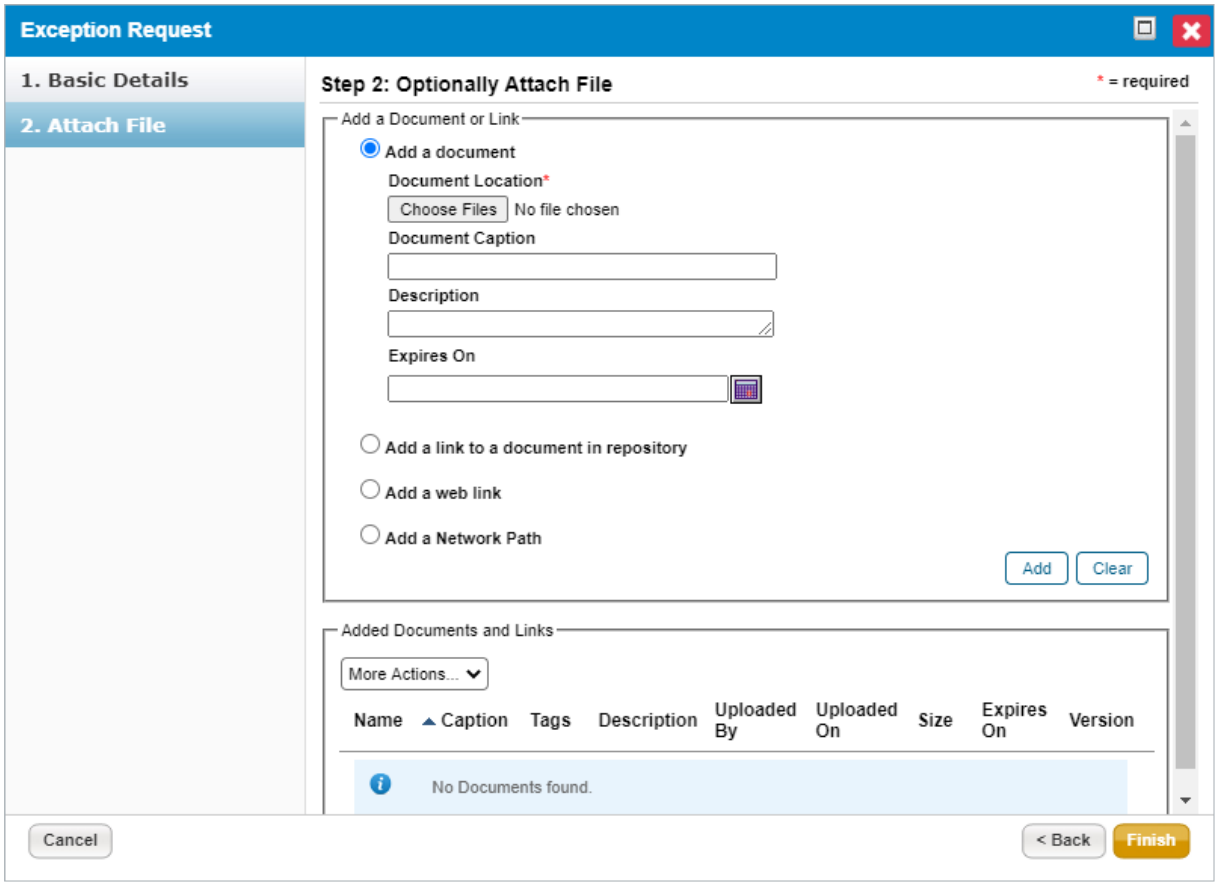
To create an exception:

1. Go to **Assessments** > **Assessments**.
2. Select an assessment to open the **General** tab on the **Assessment Details** page.
3. Click the **Control Results** tab, then select a control or subcontrol.
4. Click **New Exception** to launch the **Exception Request** wizard.



The Exception Request wizard.

5. Enter the exception information, then click **Next**.
6. **Optional**: Add a document from your desktop, link to a document in the repository, or URL. For more information, see Exception Request Attachments.



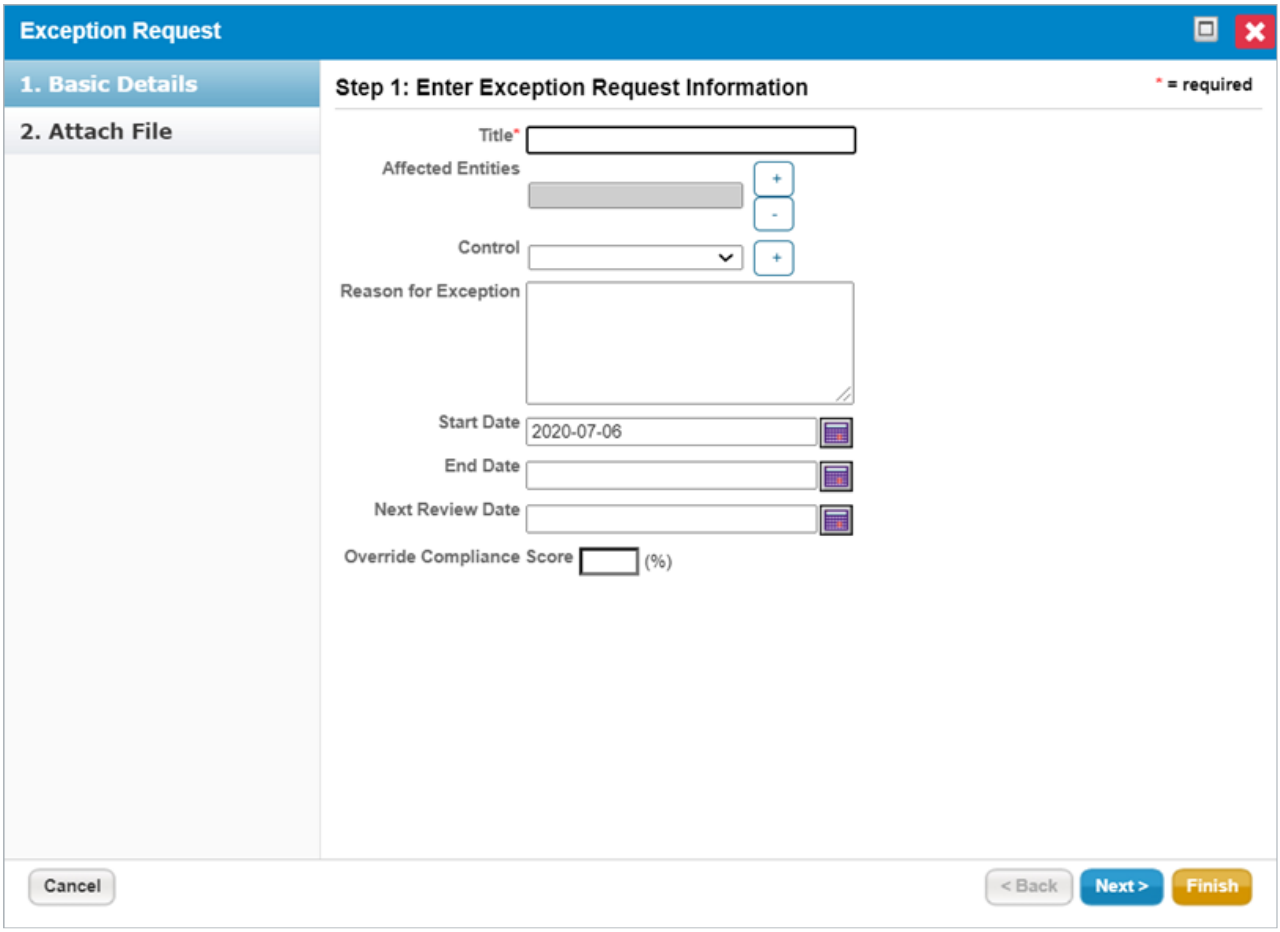
The Attach File section of the Exception Request wizard.

If you cancel the attachment, it will appear to cancel the entire exception request. Wait a few moments and the exception request will appear without the attachment.

7. Click **Finish** to exit the wizard and to add an exception on **Home** > **Exceptions** page.

Exception Request Basic Details

The following fields in the **Basic Details** wizard page of **Exception Request** must be specified when creating an exception.



The Basic Details section of the Exception Request wizard.

- **Title.** Enter the text to name the exception request.
- **Affected Entities.** Select entities for which you want to create an exception.
- **Applicable Controls.** Select controls that are applicable to the exception.
- **Reason for Exception.** Enter comments that explain why the exception is required.
- **Compensatory Controls.** Select subcontrols to compensate the non-performing subcontrol.
- **Start Date.** Select a date from when you want to start applying the exception.
- **End Date**. If the exception is for a specific period, select an end date. Otherwise, leave the End Date field empty if the exception is on-going.
- **Next Review.** Select the date and time that you want to automatically send a reminder to review the exception.
- **Override Compliance Score**. Enter a value to override the compliance score.

Exception Request Attachments

The **Attach File** wizard page of an exception request allows you to add documents to an exception. Stakeholders requesting an exception, or exception workflow stage stakeholders, can attach documents or web links.

To attach documents to an exception:

Select one of the following options:

1. **Add a document** Specify the following fields:
    - **Document Location**: Click **Browse** to select the document.
    - **Document Caption**: Enter the text to name the document.
    - **Description**: Enter the text that describes the document.
    - **Expires On**: Select the date when the document will expire.
2. **Add a link to a document in repository**: Click **Browse** to select a document collection.
3. **Add a web link**, specify the following fields:
    - **URL**: Enter a complete URL including the protocol HTTP or HTTPS.
    - **Link Caption**: Enter the text to name the URL.
    - **Description**: Enter the text that describes the URL.
    - **Expires On**: Select the date when the document will expire.
4. **Add a Network Path**, specify the following fields:
    - **URL**: Enter a complete Network Path.
    - **Link Caption**: Enter the text to name the Network Path.
    - **Description**: Enter the text that describes the Network Path.
    - **Expires On**: Select the date when the document will expire.
5. Click **Add** to display the documents in the **Added Documents and Links** grid. Click **Clear** to clear the selection.

Default Exception Workflow

The following table describes the default exception workflow:

Stage	Options	Next stage	Status	Description
Requested	Request	Review	Requested	Start of workflow stage, exception automatically transitions to Executive owner of the entity for *Review*.
	Close	Closed	Expired	When rejected by stakeholders of the review or sign off stage, gives the requestor the opportunity to add more information and request again or close the ticket as rejected. **Note**: Exception permissions are required.
Review	Sign off	Sign off	—	Transitions the request to Security owner of the entity for *Sign off*.
	Reject	Requested	Rejected	Returns the request to Exception Requestor and transitions the request back to the *Requested* stage.
	Delegate	—	Delegated	Assigns the request to another user, and allows that user to sign off or reject the exception as the temporary stakeholder of the Review stage. **Note**: If the delegate rejects the request, it moves back to the requestor.
Sign off	Accept	Closed	Accepted	Closes the request with an accepted status and removes the out-of-compliance results from related reports and assessments.
	Rejected	Rejected	Requested	Returns the request to Exception Requestor and transitions the request back to the *Requested* stage.
Closed				Terminal stage, either Accepted or Expired depending on the action that closed the ticket.

Edit an Exception

Exception workflow stage stakeholders can edit exceptions to these fields:

- **Information** tab > **General** details;
- Comments in the **Comments** tab; and
- Documents on the **Exception Request Details** page > **Attachments** tab.

Not all fields can be updated under the **General** details. The fields in the **Information** tab use a box to help you understand which fields can be updated when you click the **Edit** link. For information about the description of each field, see Exception Request Basic Details.

Transition Exception Requests

Only workflow stage stakeholders can modify settings and transition an exception to another stage. The user who submits a global request must manually move the exception into the next stage of the workflow.

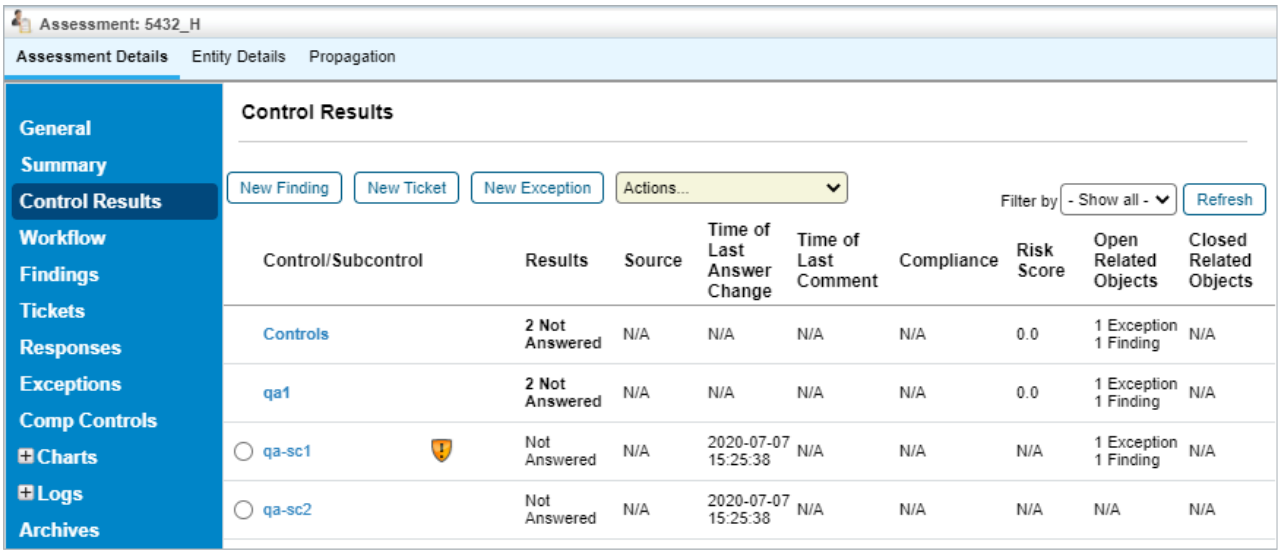
To transition an exception to the next stage:

1. Go to **Home > Exception Requests**.
2. Click the **My Exceptions** folder.
3. Click the name of the exception.
4. Click the **Workflow** tab.
5. Click an action button to transition the exception to another workflow stage.
6. Enter a comment.
7. Click **OK**.

Your comment is added to the log and the exception is transitioned to the next stage.

Control Results Grid

The **Control Results** tab shows the details of the stakeholders' answers regarding the controls and subcontrols attached to a risk. The results of these choices are used to calculate compliance and risk scores. The details of these choices are displayed in a grid. Only subcontrols are selectable. The controls will be read-only.



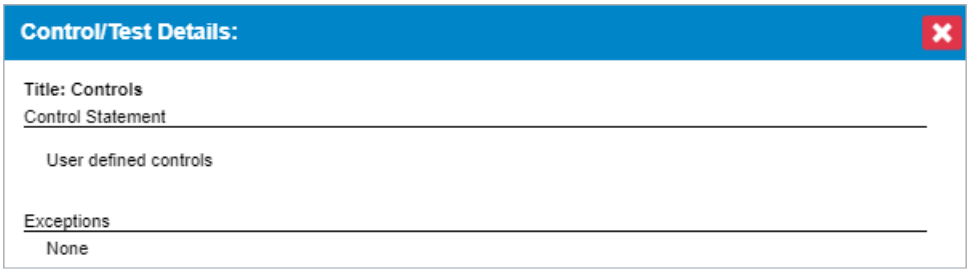
The Control Results tab.

The **Control Results** grid shows the following information:

- **Control/Subcontrol:** The ID of the control or subcontrol attached to this assessment.
- **Results:** Whether or not the questions associated with the control or subcontrol are complete, and how many are still unanswered.
- **Source:** Where the control or subcontrol came from.
- **Time of Last Answer Change:** When the stakeholder last updated his or her answers to the questions.
- **Time of Last Comment:** When the stakeholder last left a comment on the related question.
- **Compliance:** The control or subcontrol's compliance score %.
- **Risk Score:** The control or subcontrol's current risk score.
- **Open Related Objects:** A list of the control or subcontrol's outstanding exceptions, tickets, or findings.
- **Closed Related Objects:** The quantity of exceptions, tickets, or findings attached to the control or subcontrol have been closed.

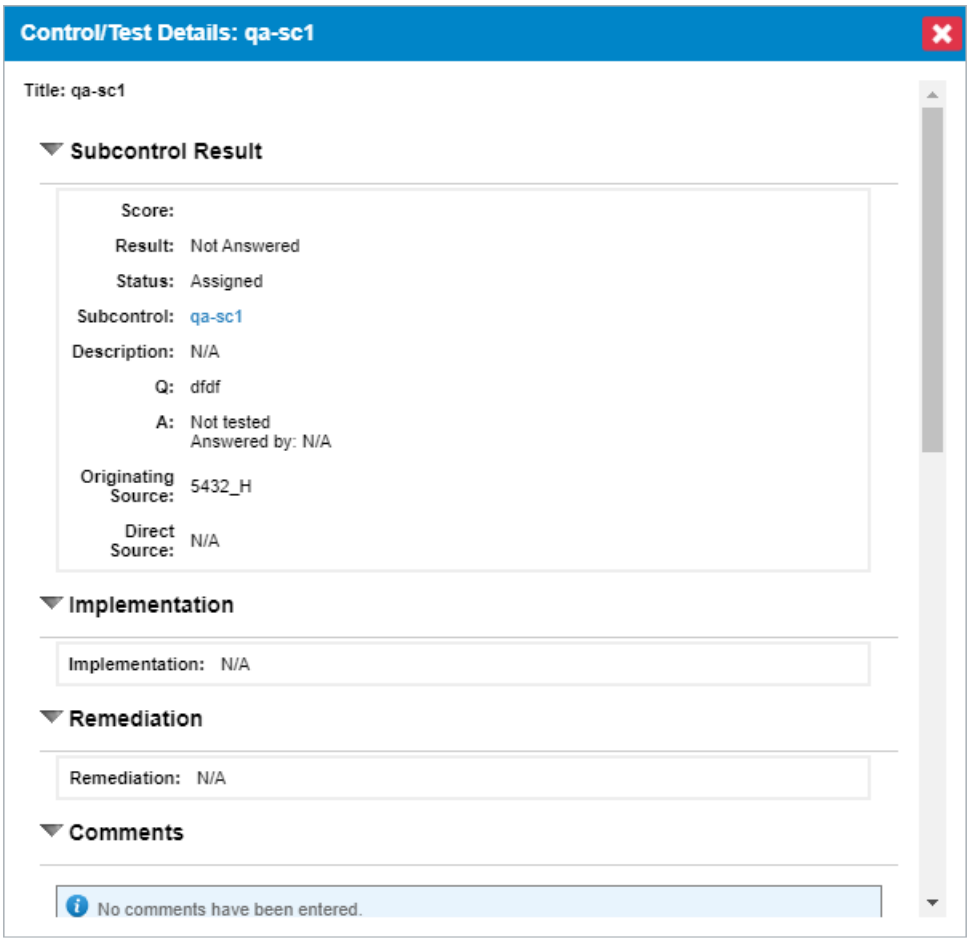
Control/Test Details

By clicking on a control or subcontrol in the Control Results grid, users can view the **Control/Test Details** page which offers more detailed read-only information about each one. For controls, the page will show the **Control Statement** and **Exceptions**.



The Control/Test Details page for controls.

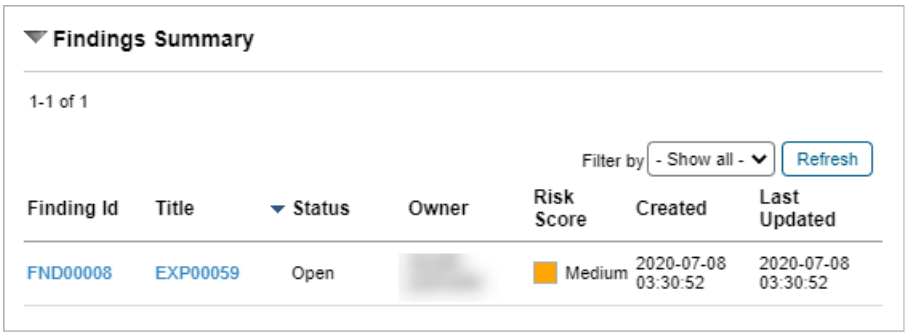
For subcontrols, the page will show the data from the subcontrol's **Subcontrol Result**, **Implementation**, **Remediation**, and **Comments** sections.



The Control/Test Details page.

In addition to the above information, the **Control/Test Details** page for subcontrols shows grids for the attached findings, tickets, and exceptions.

Findings Summary:

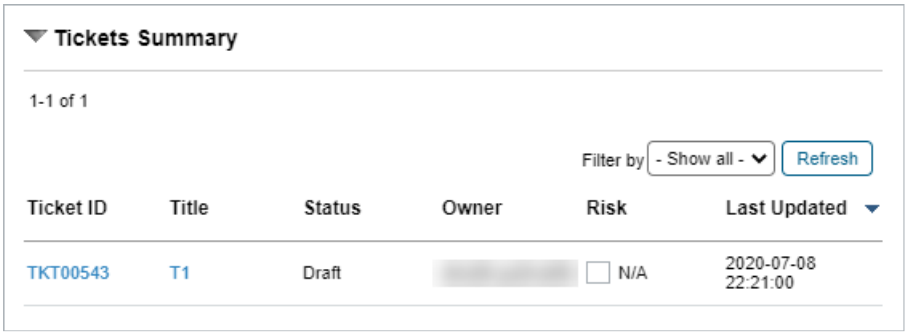


The Findings Summary grid.

The **Findings Summary** grid shows the following information:

- **Finding ID:** The ID of the finding attached to the subcontrol.
- **Title:** The name that the finding's creator assigned to the finding.
- **Status:** The current status of the finding.
- **Owner:** The user who created the finding.
- **Risk Score:** The current risk score attached to the finding.
- **Created:** The date and time that the finding was created.
- **Last Updated:** The date and time that the finding was last updated.

Tickets Summary:



The Tickets Summary grid.

The **Tickets Summary** grid shows the following information:

- **Ticket ID:** The ID of the ticket attached to the subcontrol.
- **Title:** The name that the ticket's creator assigned to the ticket.
- **Status:** The current status of the ticket.
- **Owner:** The user who created the ticket.
- **Risk:** The current risk score attached to the ticket.
- **Last Updated:** The date and time that the ticket was last updated.

Exception Summary:

The Exception Summary grid.

The **Exception Summary** grid shows the following information:

- Exception ID: The ID of the exception attached to the subcontrol.
- Exception Name: The name that the exception's creator assigned to the exception.
- Status: The current status of the exception.
- Risk: The current risk score attached to the exception.
- Start: The date and time that the exception began.
- End: The date and time that the exception ended or is scheduled to end.
- Last Updated: The date and time that the exception was last updated.

About Findings

Findings are gaps in compliance or specific exposures to risk. Findings represent the results of an assessment or the issues that need remediation. Findings are always associated with an assessment and, typically, a single failed control. Findings can have associated responses, tickets, exception requests, and attachments.

Findings are created manually or are imported from Excel files. For more information, see Creating a Finding or Importing Findings. Once created, findings are managed in a grid with the ability to drill down to a finding's details.

You can respond to findings by creating tickets, requesting exceptions, performing a risk assessment on the finding, or creating a finding response.

In the Findings page, the tree only includes folders. Clicking on a folder usually displays the objects it contains in the grid pane.

Folder	Sub-Folder	
My Findings	By Status	Open Findings Remediated Findings Closed Findings
	By Stage	New In Progress Review Closed
	My Findings Delegated To Others	
	My Undelegated Findings	
All Findings	By Status	Open Finding Remediated Findings Closed Findings
	By Stage	New In Progress Review Closed
	All Delegated Findings	
	All Undelegated Findings	

1. The folder name under the By Stage depends on the workflow stage names
2. All **Findings** folders are available only if users have the object Mange permission privilege.

Creating a Finding - Assessment

Findings are associated with specific assessments, but the wizard allows you to either select an existing assessment or create a new one. Users with the Findings create permission can create a finding.

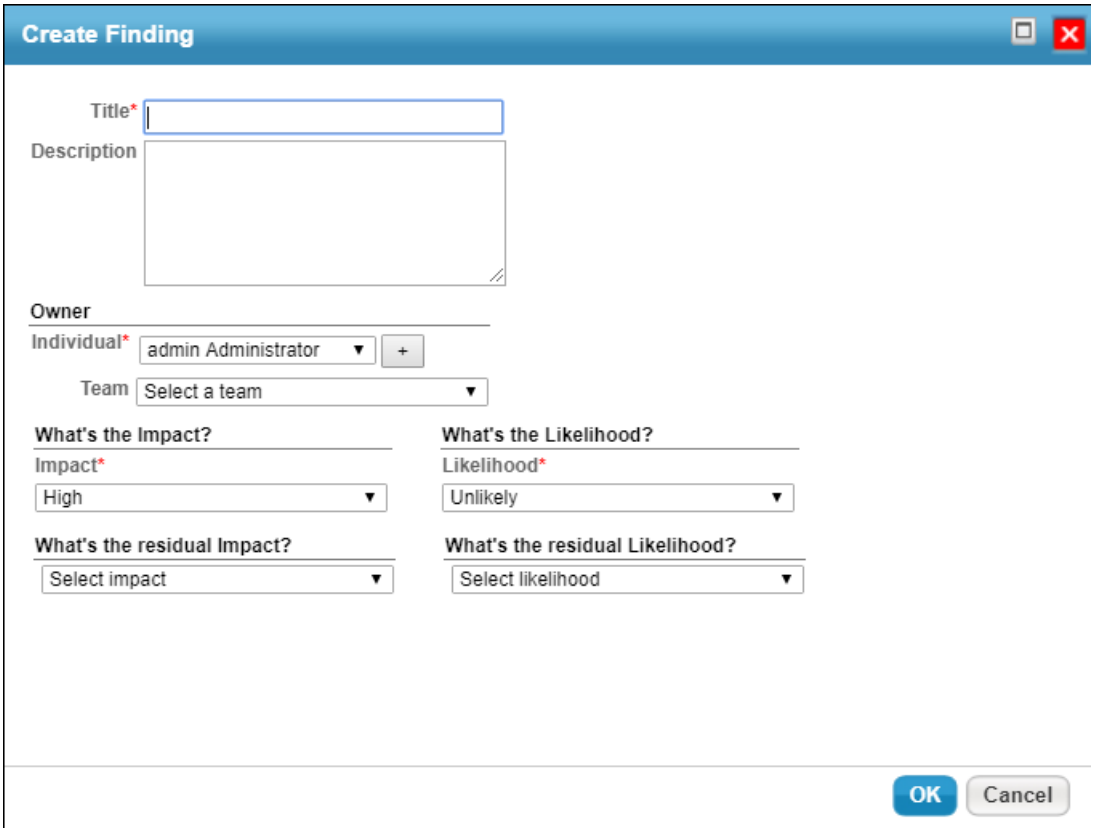
To create a finding:

1. In the Risk Vision application, go to **Assessments** > **Assessments**. The **Assessments** page is displayed.
2. Select an assessment to open its details page and display the **General** tab on the **Assessment Details** page.
3. Launch the **New Findings** wizard using one of the following navigation:

   Click the **Findings** tab and click **New** option.

   Or

   Click the **Control Results** tab, select a control or subcontrol, and select **New Finding** option.
4. In the **New Findings** wizard page:
   - Enter a name in the Title field
   - Enter text in the Description field to provide information about the need to create a finding
   - Select a user from the Individual drop-down list to assigning to a particular user
   - Select a team from the Team drop-down list to assign the finding to a particular team
   - In the What's the Impact? drop-down list select a value for the finding likelihood
   - In the What's the residual Impact? drop-down list select a value for the finding residual impact
   - In the What's the Likelihood? drop-down select a value for the finding likelihood
   - In the What's the residual Likelihood? drop-down select a value for the finding likelihood



5. Click **OK** button, a new finding is created.

Deleting a Finding

You can delete a finding if your user role has Finding View and Finding Delete permissions.

To delete a finding:

1. In the RiskVision, go to **Assessments** > **Assessments**. The **Assessments** page is displayed.
2. Select an assessment to open its details page, and display the **General** tab on the **Assessment Details** page.
3. Select the box next to finding(s) and click **Delete**. The finding is deleted.

Importing Findings

Findings can be imported from Excel files, using the file format as described in the Importing Data topic.

The following table shows the columns that are available in the Finding Import Template. The first section assigns labels to the columns in the second section. Not all columns are required.

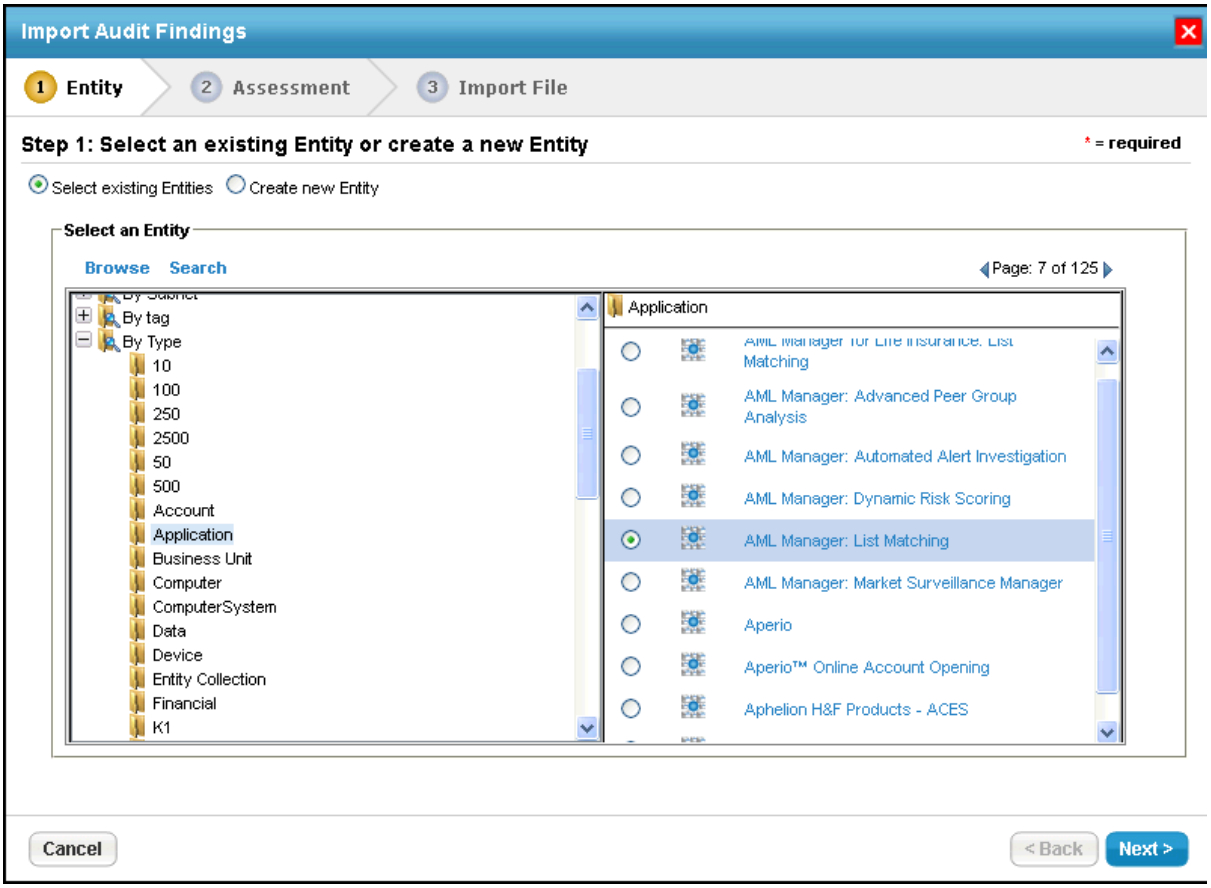
Column label	Description
Name	Finding name (Required)
Control	Control name
Status	0-Open; 1- Remediated; 2-Closed
Description	Description for the finding
Likelihood	Between 0 and 10
Impact	Between 0 and 10
Residual Likelihood	Between 0 and 10
Residual Impact	Between 0 and 10
Owner	Any RiskVision UserId or it takes Logged in user as the default owner
Team	Any RiskVision Team name
customAttributes.string1	(if defined)
customAttributes.long1	(if defined)
customAttributes.boolean1	(if defined)
customAttributes.text1	(if defined)
customAttributes.long1	(if defined)
Response Title	(if defined)
Response Action	(if defined)
Response Comment	(if defined)
Response Owner	(if defined)
Response Status	Suggested, Approved, Implemented/Completed, Verified, Canceled

To import findings:

Use one of the following procedures:

Procedure A:

1. Go to **Home** > **Findings** and select **Import Audit Findings** in the More Actions drop-down list.
2. The **Import Audit Findings** wizard appears, displaying the **Entity** wizard page. You can create a finding for existing and new entities.
3. Use one of the following ways to select an entity:



- *Existing entity*

  From the available entity groups, click **+** to expand a dynamic group, select the group, and then select the entity.

  Or

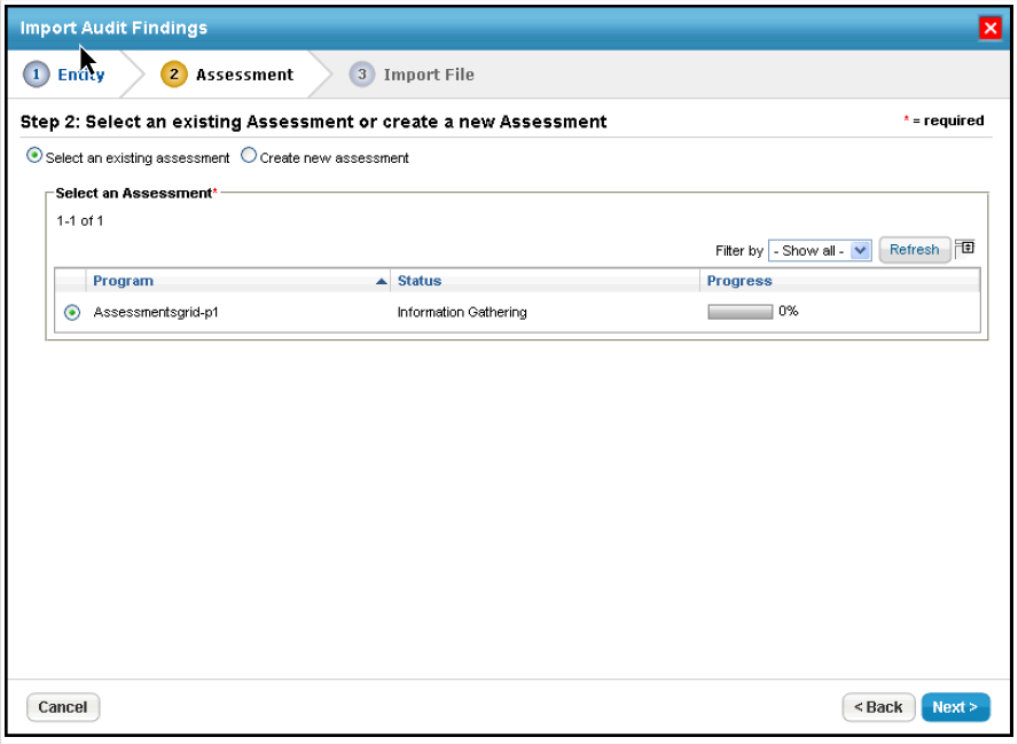
  If you know the name of the entity, click **Search**, enter the text, and then click **Search** again. Select the entity.

- *New entity*

  If the entity is unavailable in the RiskVision application, select **Create a new entity**.

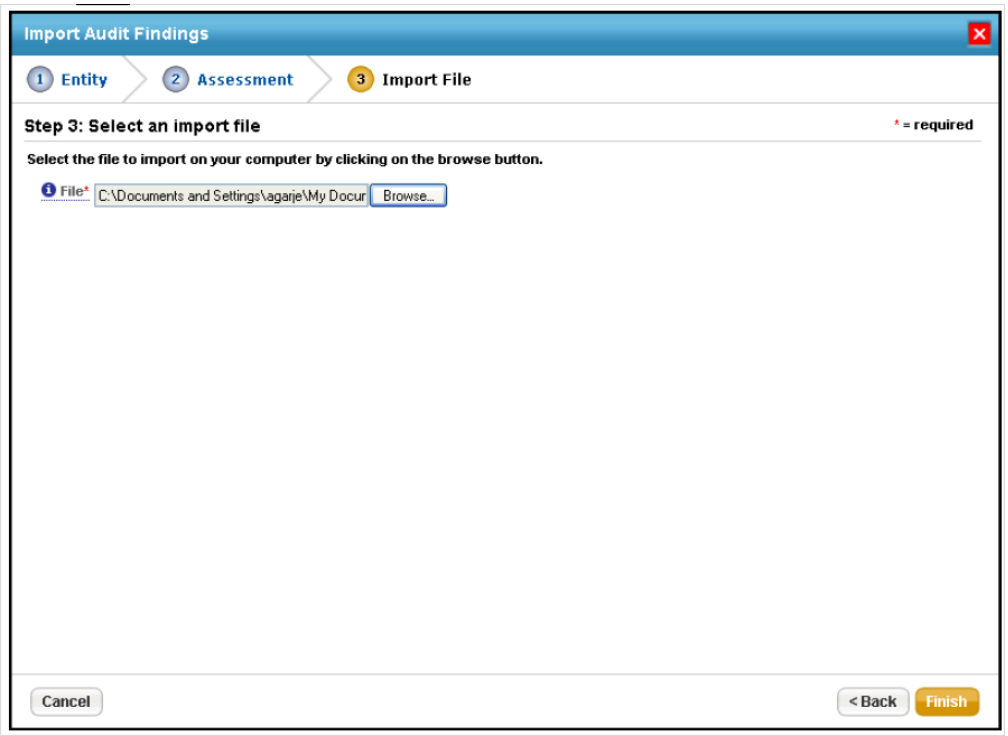
Click **Next** to continue.

4. The **Assessment** wizard page appears. Select the assessment in which you want to import the findings. If you have created a new entity in the previous step, you may want to select **Create a new assessment**, and then select a program in the **Program** drop-down list to create a new assessment.



Click **Next** to continue.

5. The **Import File** wizard page appears. Click **Browse** to locate and select the Finding Import Template.



6. Click **Finish** to add the findings and to exit the wizard.

Procedure B:

You can use this procedure to directly import the findings into the assessment.

1. In the **Assessment Details** page, go to **Findings** tab, and select **Import Audit Findings** in the **More Actions** drop-down list.
2. The **Import** dialog appears. Click **Browse** to locate and select the **Finding Import Template**, and click **OK**.

You can import multiple response details by updating 'Finding map' sheet details based on the number of responses that you are going to import and then by providing values under the respective columns in the template's second sheet.

Finding Analysis

A finding can be assessed based on the impact and likelihood ratings provided by workflow stage stakeholders. These ratings have a corresponding threshold value defined in the Findings Configuration range that will derive the inherent risk and residual risk scores for a finding.

Assume that you have set up threshold values for the following findings configuration ranges:

Inherent Impact Score

Threshold	Label
Score < 2	Low
2 <= Score < 5	Medium
5 <= Score	High

Inherent Likelihood Score

Threshold	Label
Score < 1	Unlikely
1 <= Score < 3	Possible
3 <= Score < 5	Likely
5 <= Score < 8	Almost Certain
8 <= Score	Certain

Inherent Risk Score

Threshold	Label
Score < 30	Low
30 <= Score < 60	Medium
60 <= Score	High

An inherent risk score is calculated as follows:

Inherent impact rating X Inherent Likelihood rating

For a finding, if you have rated the inherent impact as 'Medium,' and the inherent likelihood as 'Almost Certain,' then the high value that constitutes the selected rating is applied in calculating the inherent risk score value. That is, the equivalent values for the inherent impact and inherent likelihood ratings are 4 and 7, and the Inherent Risk score is 4 * 7 = 28.

Likewise, the residual risk score is calculated as follows:

Residual Impact rating X Residual Likelihood rating

Create a Response

A response created from the **Assessment Details** > **Responses** tab overrides the compliance score. When created with the **Add Finding Response** action on the **Assessment Details** > **Findings** tab, it mitigates the finding score.

To create a response:

1. Open RiskVision Compliance Manager.
2. Go to **Assessments > Assessments**.
3. Click an assessment. Click the **General** tab on the **Assessment Details** page.
4. Launch the **New Response** wizard using one of the following methods:
   - Click the **Findings** tab, then click **More Actions** > **Add Finding Response**.
   - Click the **Control Results** tab, select a control or subcontrol, then click **Actions** > **New Response**.
3. Expand the **Response** section. Enter a name in the **Title** field, then enter text in the **Comments** field to provide information about the need to create a response.
4. Click the **Response Action** field to display a list of options then select the appropriate value. Repeat this process with the **Mitigation Status** field.
5. Click the **Start Date** field to select a date. Repeat this process with the **End Date** field.
6. Click the **Owning Organization** field and enter a name.
7. Expand the **Return of Investment** section, then enter a percentage value in the **Risk Reduction** (percentage) field to override the risk score.
8. Enter a value in the **Implementation Cost** field to forecast the implementation cost, and enter a value in the **Time to Implement** (in days) field to calculate the effort.

   The risk score is reduced using the formula as follows: `risk - risk - (risk * riskReduction)`. For example, if you have to override the risk score of 100 by twenty-five percent, the risk will be reduced to 75.

   There are a number of response actions depending on the specifics of a finding. Response actions include:

   - Compensate
   - Mitigate
9. Click **Next**.
10. To link tickets, click the box next to the **Link an existing or new Ticket with this Response** option. You can link an existing ticket or create a new ticket that will help track the response.
11. Select existing tickets that you want to link. In the **Available Tickets** box, click the box corresponding to each row, and click **>>** so that tickets are moved to the **Selected Tickets** box.
12. Optional: Click **Create new Ticket** to create a new ticket, specific to a response.
13. Click **Next** to open the **Attach File** wizard page.
14. Use one or more options below to attach files:
    - **Add a document**: Allows you to upload a document from your local system.
    - **Add a link to a document in the repository**: Allows you to provide references to a document collection in the document repository.
    - **Add a web link**: Allows you to provide external references.
15. Click **Add**.
16. Click **Finish**. The response is created and appears on the **Responses** tab of the **Findings** detail page, and on the **Responses** tab of **Assessment Details** page.

Update a Response

Updating a response involves operations, such as updating fields, adding and creating tickets, and managing attachments.

To update a response:

1. Open RiskVision Compliance Manager.
2. Go to **Assessments > Assessments**. The **Assessments** page is displayed.
3. Select an assessment to open its details page and display the **General** tab on the **Assessment Details** page.

   Use one of the navigation's below:

   - Click the **Findings** tab, click a finding to open its details page, and click the **Responses** tab.
   - Click a response to open its details page and display the **General** tab.

     OR

   - Click the **Responses** tab.
   - Click a response to open its details page and display the **General** tab.

3. Click **Edit** at the top right corner of the details page.
4. Click **Save** after you finish updating the fields. Similarly, navigate to the **Linked Tickets** and **Attachments** tabs and update the information.

Delete a Response

You can delete unwanted responses from within the **Findings** details page or within the **Responses** tab of the **Assessment Details** page.

To delete a response:

1. Open RiskVision Compliance Manager.
2. Go to **Assessments** > **Assessments**.
3. Select an assessment to open the **General** tab on the **Assessment Details** page.
4. Complete one of the following actions to delete the response:
    - **Findings** tab:
        - Click the **Findings** tab, click a finding, and then click the **Responses** tab.
        - Check the box next to the response(s) you want to delete, then click **Delete**.
    - **Responses** tab:
        - Click the **Responses** tab.
        - Check the box next to response(s) you want to delete, then click **Delete**.

Tickets

The RiskVision solution provides a ticket management system that lets you create and track tickets for tasks, risk assessment mitigation and remediation, and entity control resolution. Tickets are also used for vulnerability resolution. In addition, sites may deploy and integrate the RiskVision solution with other external ticket management systems, such as Remedy.

In the Tickets page the tree only includes folders. Clicking on a folder usually displays the objects it contains in the grid pane.

Folder	Sub-Folder	
My Tickets	By Status	Open Tickets Closed Tickets
	By Stage	New In Progress Review Closed
	By Type	Entity Control Resolution Incident Response Other Risk Assessment Response Risk Assessment Remediation Threat Mitigation Vulnerability Resolution
	My Tickets Delegated to Others	
	My Undelegated Tickets	
All Tickets	By Stage	New In Progress Review Closed
	By Types	Entity Control Resolution Incident Response Other Risk Assessment Response Risk Assessment Remediation Threat Mitigation Vulnerability Resolution
	All Delegated Tickets	
	All Undelegated Tickets	

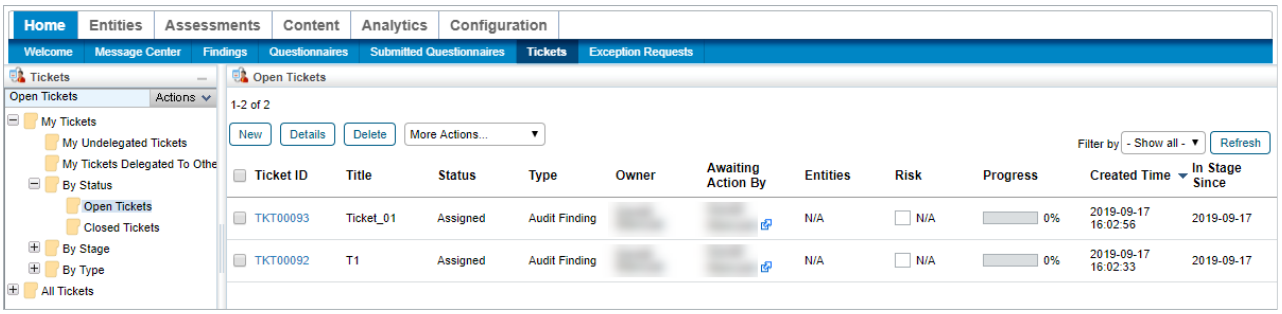
1. The folder name under the By Stage depends on the workflow stage names.
2. All Tickets folders are available only if users have the object Mange permission privilege.

Understanding Ticket Flow

Tickets are used to track efforts to review, analyze, and deploy remediation and prevention steps associated with specific vulnerability instances. The **Tickets** section of a vulnerability lists the tickets associated with the instance.

Tickets have an associated workflow. Vulnerability resolution tickets are related to their vulnerability instance. The status of the ticket corresponds to the current stage of the workflow. The workflow and its stages can be customized to suit specific requirements, but typical ticket workflow stages include:

- New
- In Progress
- Review
- Closed
- Closed via Exception



The Tickets page.

The disposition field affects the workflow while editing a ticket. Set the disposition to **Escalate** or **Exception** or customize the set of disposition choices.

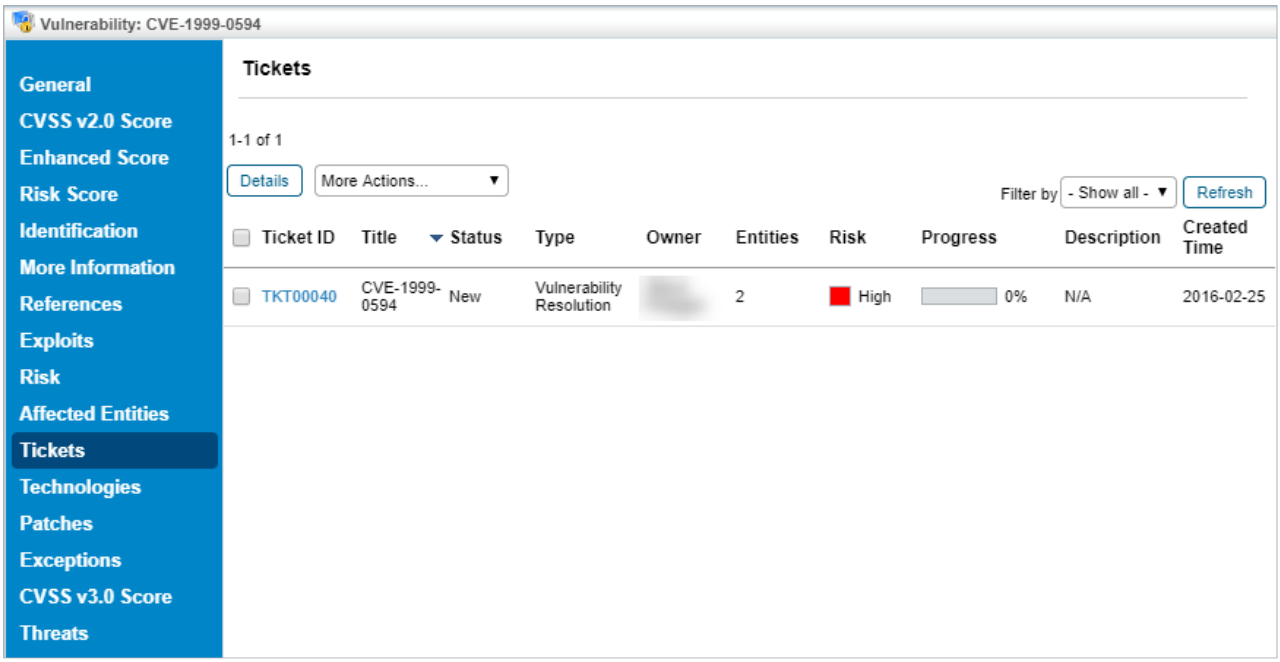
Ticket updates can change the ticket disposition. You can also select a disposition that will not generate escalations. However, changing the ticket disposition does not automatically close the ticket or prevent a closed ticket from being reopened.

Tickets also have an **Exception Expiration** field. If you specify a date in this field, the system will send an email to ticket stakeholders when the ticket is overdue. The email template used for this notification is specified in the property **ticket.exception.expired.notification.template.**

Ticket escalation templates can be specified by priority using the system property: com.agiliance.ticket.escalation.template with a value such as "high, Default Ticket Escalation Template; medium, Default Ticket Escalation Template".

Relevant system properties include:

- vulnerability.status.exception: Names the exception status for all vulnerabilities; and
- vulnerability.status.cannot.overwrite: Names the exception status that cannot be further modified by a scanner or other source reporting the same vulnerability instance again.



The Tickets tab of a vulnerability.

Tickets are associated with a vulnerability instance. Ticket email templates can contain the vulnerability title and description. To append vulnerability information in the notification that you send to stakeholders, use the object `getAttachmentVulnerabilities()` to specify the following html code in the email template.

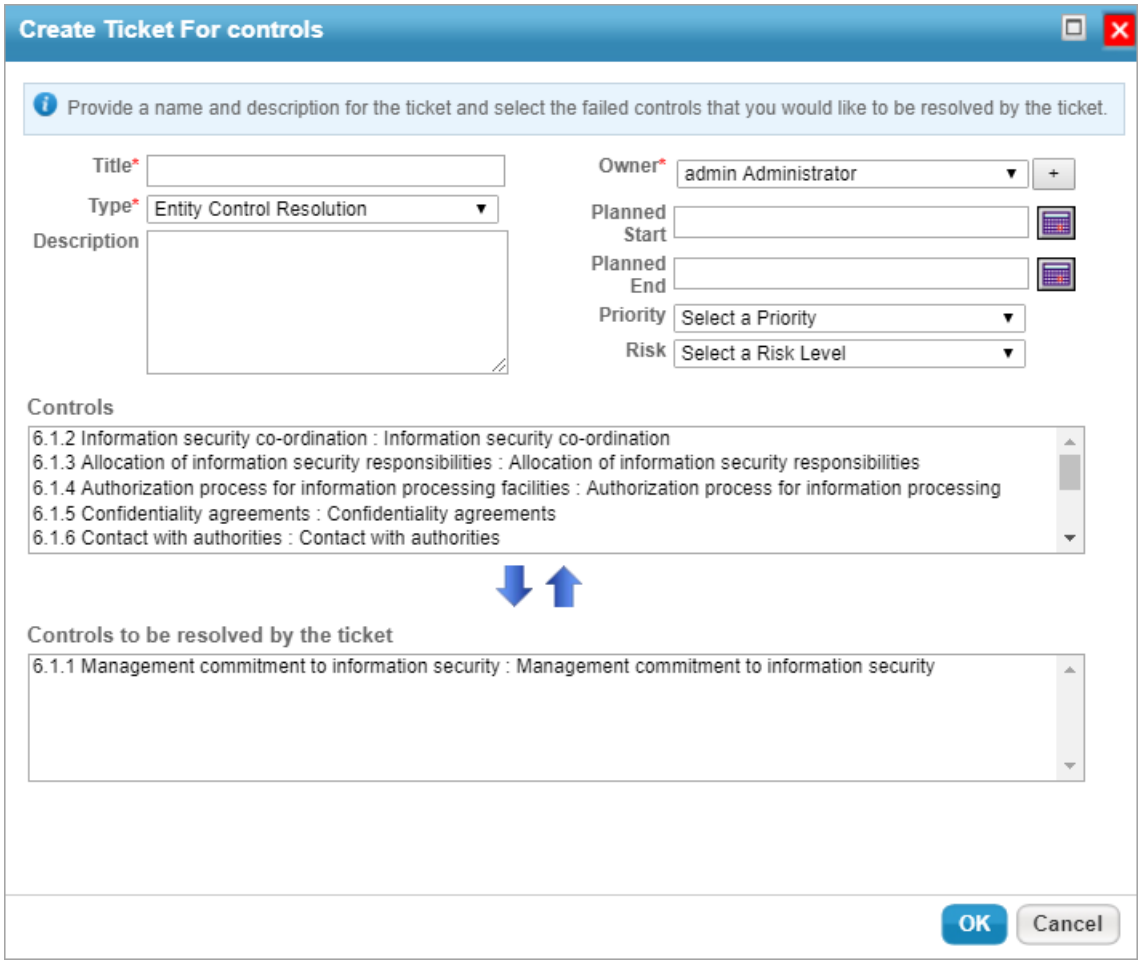
```
#set($vulnerabilities= $ticket.getAttachedVulnerabilities())
#foreach($v in $vulnerabilities)
Vulnerabilities: $v.getCaption()
#end
$ticket.getAttachedVulnerabilities()
```

Creating a Ticket - Assessment

Users with Ticket Create permissions can create a ticket from **Home** page or **Assessment** details page.

To create a ticket:

1. Go to **Assessments** > **Assessments**.
2. Select an assessment to open the **General** tab on the **Assessment Details** page.
3. Click the **Control Results** tab, then select a control or subcontrol.
4. Click **New Ticket** to launch the **Create Ticket For controls** wizard.



4. Enter a **Title** and **Description**.
5. Click the **Type** field to view a list of options, then select the appropriate type. Repeat this process with the**Owner**, **Priority**, and **Risk** fields.
6. Click the **Planned Start** field to view a calendar and select a date. Repeat this process with the**Planned End** field.
7. Verify if the selected control/subcontrol appears in the **Controls to be resolved by the tickets** table.
8. Click **OK**.

Link a Ticket to an Entity

Links between entities and tickets are permanent. Links map workflow stage stakeholders to entity ownership types and allow you to run reports on entities and their corresponding tickets.

The Default Ticket Workflow assigns stage stakeholders based on their entity ownership type. To automatically assign ownership of the tasks related to the ticket process, you must link the entity or entities to which the ticket applies.

Links to incidents display on the **Ticket** > **Link** page. You can link tickets to incidents from the **Home** > **Incidents** page.

To link a ticket to an entity:

1. Go to **Home > Tickets.**
2. Select a ticket you want to link, then click **Details**.
3. Open the **Linked To** section.
4. Click **Add Entities**.
5. Select a type of entity and click **Search**.
6. Select an entity and click the down arrow to move it to the **Selected Entities** field.
7. Click **OK**.

The ticket is now linked to the entity. If you are creating a new ticket, move it to the first stage of the workflow process as described in Transitioning a ticket to the next stage.

Starting and Transitioning the Ticket Process

When you submit a ticket, the ticket process begins in the first stage of the workflow. Only the current stage owner transitions the ticket to another stage. Ticket Administrators can assign the ticket to themselves and then move it to another stage.

The ticket type is mapped to a ticket workflow template. By default, all types are mapped to the Default Ticket Workflow. Each ticket has its own instance of the workflow. Workflow changes don't affect tickets after they start the workflow process. The user can apply workflow changes to tickets manually with the link "Click here to attempt a synchronization."

To transition a ticket:

1. Go to **Home** > **Tickets**.
2. Locate the ticket, select the ticket, and click **Details**.
3. Click **Workflow**.

   The Workflow page displays.
4. Click an action button, such as **Accept**, to transition to the next stage or **Reject** to send it back to the previous stage. The Comment window displays.
5. Enter your transition message and click **OK**.

The ticket moves to another stage and the comment is added to the ticket history.

Changing the Default Ticket Workflow

When a ticket is created, which can be an automatic or manual process, the new ticket will use the default ticket workflow if there is no appropriate custom workflow. The default ticket workflow is "Default Ticket Workflow." Users with sufficient privileges can modify certain aspects of the default workflow, but it is generally better to create a new ticket workflow and make it the default.

To change the default ticket workflow:

1. Create a new ticket workflow as described in Creating a New Ticket.
2. Open the file `%AGILIANCE_HOME%\config\agiliance.properties` by using a text editor. If the file does not exist, create it.
3. Add the following line:

   `default ticket workflow=NewTicketWorkflowName`

4. Reload the configuration, as described in the *Administrator's Guide*, or restart the RiskVision Tomcat service to affect the latest changes.

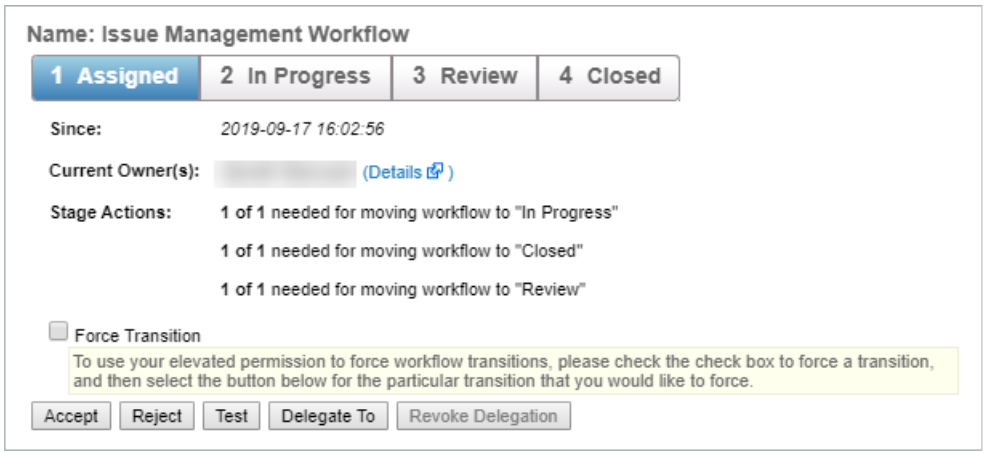
Alternatively, you can use the Selection tab of any custom ticket details page to change the default workflow.

Assigning a Ticket to Another User

Assigning a ticket to another user changes the ownership of current and subsequent workflow stages. You must have Ticket View and Ticket Manage permissions to view the **Delegate To** button to assign a ticket to another user.

To assign a ticket to another user:

1. Go to **Home** > **Tickets**.
2. Click the ticket you want to assign to another user, then click **Details**.
3. Click **Workflow**.



A ticket's workflow stages.

4. Click **Delegate To** to open the **Select User** window.
5. Locate the user or team that you want to assign, then click **OK**. You can select multiple users, if desired.

The ticket ownership will transfer from the old list of owners to the new list.

Delegating an Object to Another User

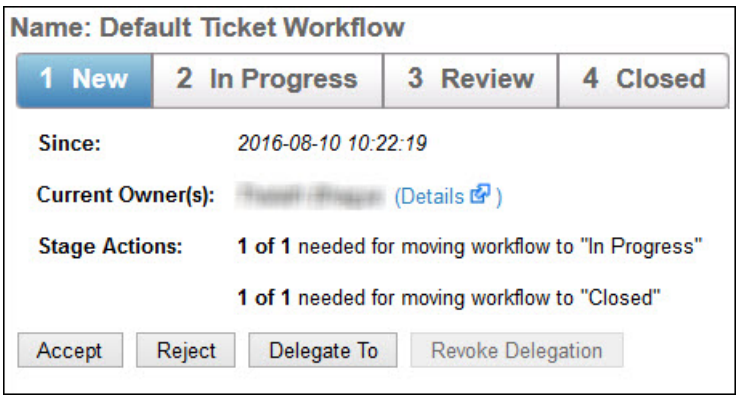
Assigning a ticket to another user changes the ownership of current and subsequent workflow stages. Unless you have the Ticket View and Ticket Manage permissions, the **Delegate To** button is not visible for you to assign a ticket to another user.

To assign a ticket to another user

1. Go to **Home** > **Tickets**.
2. Locate the ticket, select it, perform the below steps:
    1. From the **More Action** drop-down list, select the **Delegate** option.
    2. The **Delegate To** dialog box appears, locate the user or team that you want to assign, in the **Select User** or **Select Team** field.

       Here you can also select multiple users
    3. Enter the comment in the **Comment** field and then click **OK** button.

OR

> Locate the user or team that you want to assign. Here you can also select multiple users.
>
> 
>
>
> - Click **Details** option. The **Ticket** details page appears.
> - Go to **Workflow** section, in the **General** tab. The ticket workflow stage is displayed.
> - Click **Delegate To.** The **Delegate To** dialog box appears.
> - Enter the comment in the **Comment** field.
> - Click **OK** button.

The ticket ownership transfers from the old list of owners to the new list and the Revoke Delegation button is enabled.

Revoking A Delegated Object

Tickets that are delegated can only be revoked delegation. The revoke delegation will change the ownership of current and subsequent workflow stages. Unless you have the Ticket View and Ticket Manage permissions, the **Revoke Delegation** option is enabled for the tickets that are delegated.

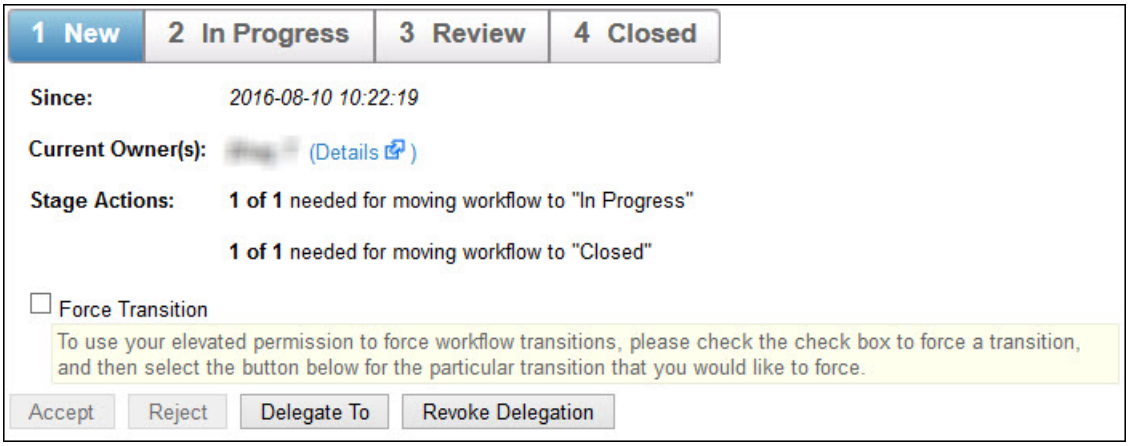
To revoke an Assigned Ticket:

1. ### Go to Home > Tickets.
2. Locate the ticket, select it and perform the below steps:
    1. From the **More Action** dropdown list, select the **Revoke Delegation** option.
    2. The **Comments** dialog box appears.
    3. In the **Comment** dialog box, enter the reason or comment for revoking delegation access.

4. Click the **OK** button.

OR

- Click **Details** option. The **Ticket** details page appears
- Go to **Workflow** section, in the **General** tab. The ticket workflow stage is displayed. If the ticket is delegated already then the **Revoke Delegation** button is enabled.



- Click **Revoke Delegation** button. The **Comments** dialog box appears.
- In the **Comment** dialog box, enter the reason or comment for revoking delegation access.
- Click **OK** button.

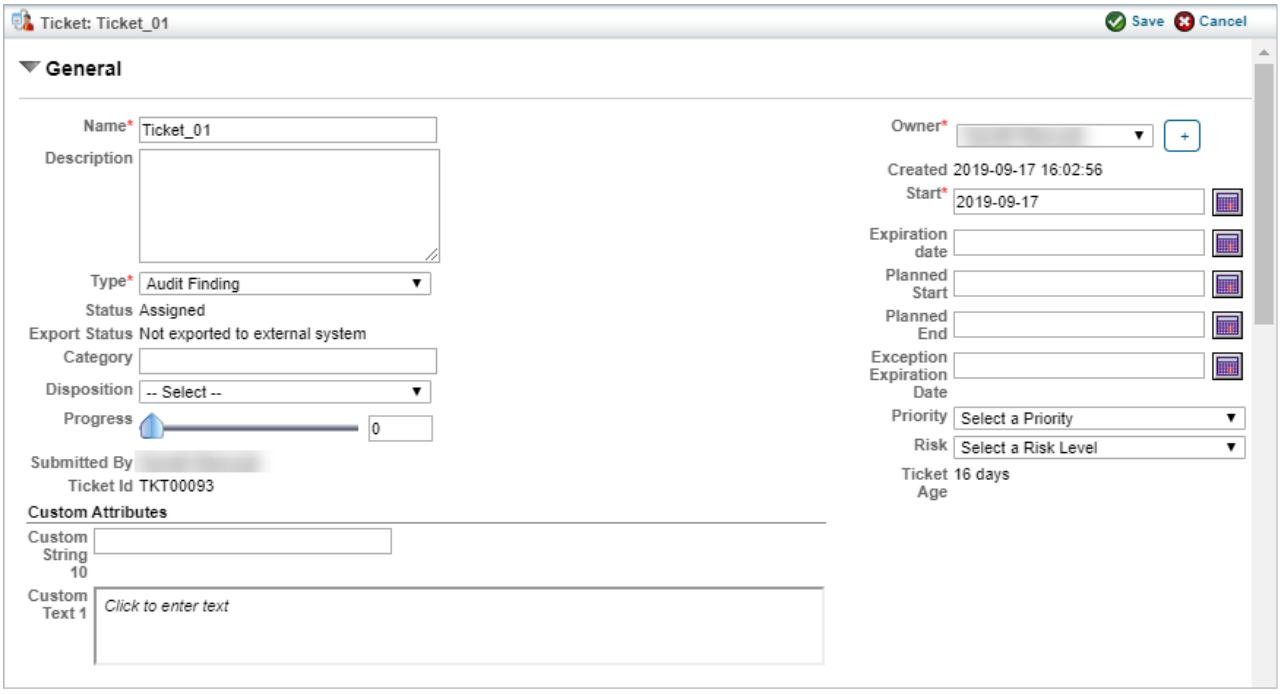
The ticket ownership transfers from the delegated user to the delegated by the user.

Setting General Ticket Information

Once a ticket is created, only the workflow stage owner can change the general ticket information, depending on their permissions. Workflow stage owners can have the following combinations of permissions:

- **Ticket View** permissions: Can view the ticket.
- **Ticket View** and **Update** permissions: Can view the ticket and change the general ticket information.
- **Ticket View** and **Classify** permissions: Can view the ticket and change the general ticket information, ticket priority, risk, and delete attachments.

Ticket administrators only need **Ticket View** and **Manage** permissions to modify the ticket settings, regardless of their participation in the ticket workflow.



The General tab on the Edit Ticket screen.

Updating any of the settings sends an email notification to the owner of a ticket. To avoid sending email notifications to the owner each time settings are updated, use the following property: `com.agiliance.ticket.update.email.enabled=false`

Parameter	Description
Title	Identifies the ticket
Description	Text description for the ticket
Type	Ticket types include: • Entity Control Resolution • Incident Response • Risk Assessment Mitigation • Risk Assessment Remediation • Vulnerability Resolution
Status	Current workflow stage
Export Status	Indicates whether the ticket is linked to a remote ticket system, such as Remedy

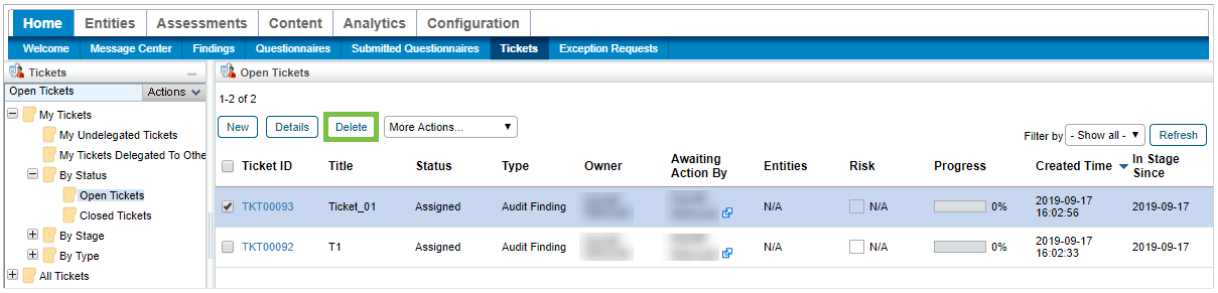
Parameter	Description
Category	Label that you can run reports on
Disposition	Ticket disposition, as specified in Ticket Management Preferences
Progress	Allows workflow stage owner to set the progress of the stage
Owner	The user who owns the ticket
Created Time	The time when a ticket was created
Start	By default, the date the ticket is created
End	By default, the date the ticket is closed
Planned Start	Date when the ticket must begin. You can also select a date in the past
Planned End	Date within which the ticket must be completed
Exception Expiration Date	Expiration date for exception
Priority	Indicates the importance of the ticket
Risk	Indicates the risk exposure of the ticket

Deleting a Ticket

You can delete a ticket if you are the owner and if you have Ticket View and Delete permissions. Users with Ticket View and Manage permissions can delete any ticket, regardless of ownership.

To delete a ticket:

1. Go to **Home > Tickets** and check the box next to the ticket you want to delete.
2. Click **Delete**, then **OK**.

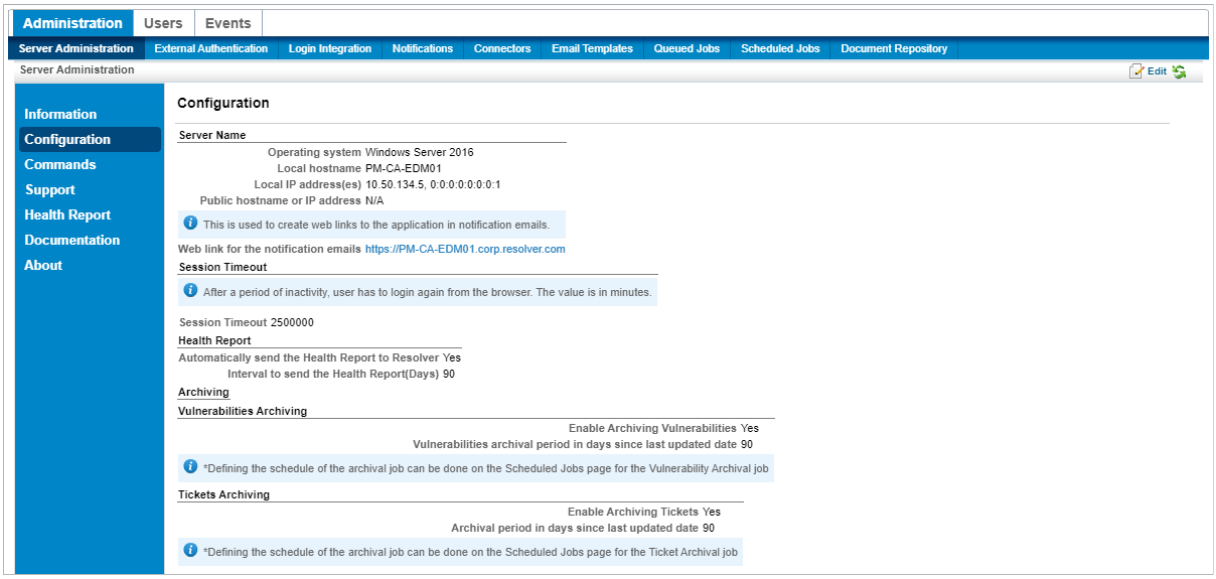


The Delete button on the Tickets page.

Automatic Ticket Archiving

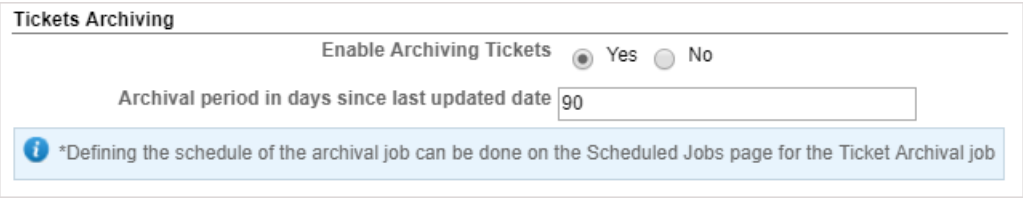
To Enable Automatic Ticket Archiving:

1. In the Administration application, go to **Administration** > **Server Administration**.
2. Open the **Configuration** tab.



The Configuration tab of the Server Administration page.

3. Click **Edit**.
4. Click the **Yes** radio button to enable archiving in the **Vulnerabilities Archiving and Tickets Archiving** sections.
5. Enter the number of days you want the archival period to last.



The Tickets Archiving section of the Edit Configuration screen.

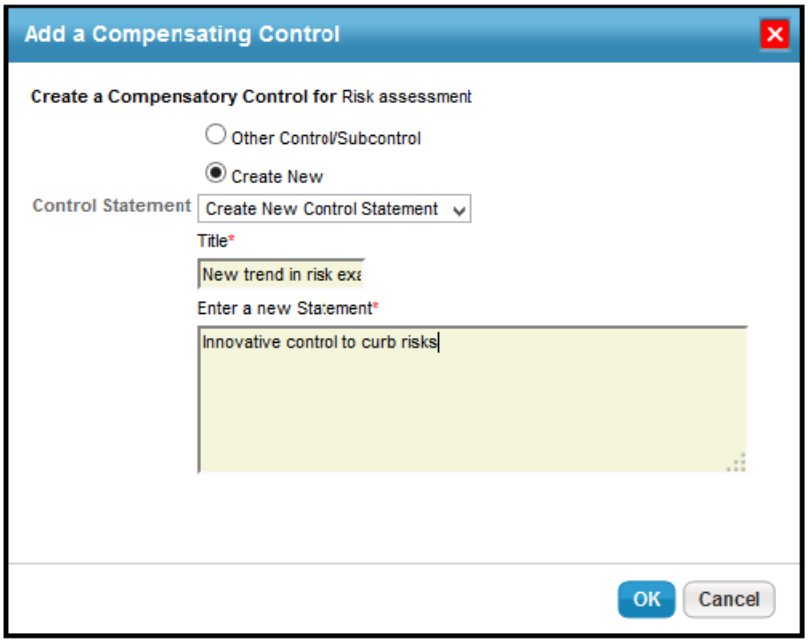
Ticket records will be archived after the specified amount of time has passed since their last update.

Compensating Controls

Compensating controls are applied when an entity does not comply with one or more controls due to technical or business constraints. Putting the compensatory controls in place mitigates the associated risk; however, you must run an internal audit to confirm that there are no deficiencies. To compensate the non-performing controls, you can create a new control or select an existing control from your organization's controls library.

To add a compensating control

1. Select an assessment, that your stakeholders have responded to the controls, to open its details page.
2. On the **Assessment Details** page, click the **Control Results** tab.
3. Select a control and then select **New Compensating Control** in the **Actions** drop-down list.
4. The **Add a Compensating Control** dialog appears.



Do one of the following:

- By default, the **Create New** option is selected in the dialog. Enter a title and statement. This will create a new compensating control.
- Select **Other Control/Subcontrol** and click **+**.
- The **Select a Controls/Subcontrols** dialog appears. Expand the groups or content packs beneath the **Controls/SubControls** folder, locate and select the compensating control, and then click **OK** to exit the **Select a Controls/Subcontrols** dialog. This will add an existing control from the controls library
- Click **OK**. The compensating control is added.

There are three error conditions we need to check for when a user tries to add a compensating control to a control:

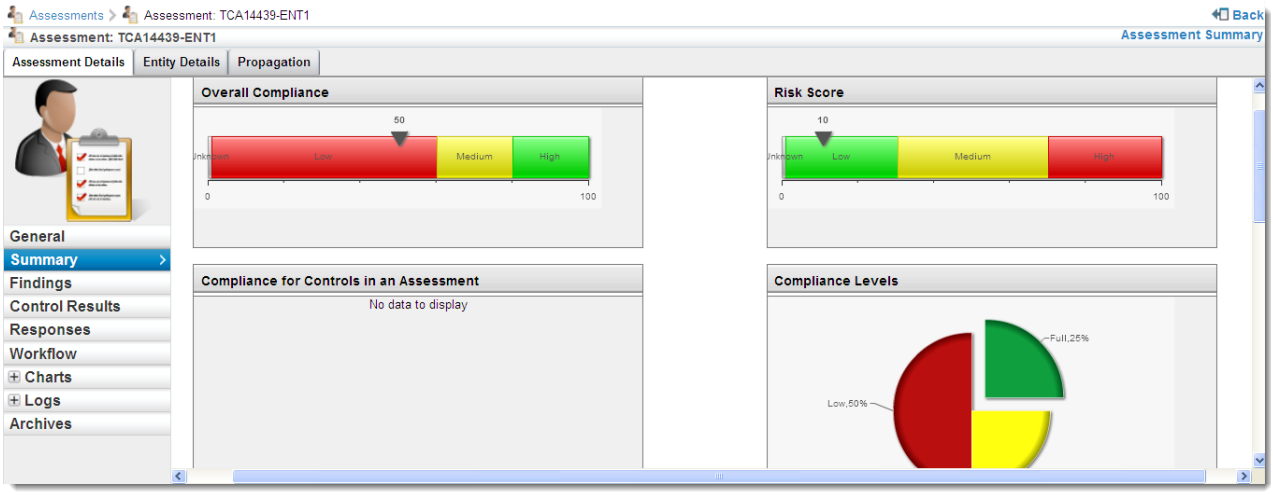
1. The same control as that which is being compensated cannot be added as a compensating control to itself.
2. A compensating control that is identical to one already present for a given control should not be able to be added.
3. A compensating control should not be able to compensate a control that itself is compensated.

About Compliance and Simple Risk Scoring

The compliance and simple risk scores for an entity show the status of the entity against compliance controls in Risk Assessment and Control Assessment programs.

Assessment, Control, and Subcontrol Compliance Scores

The **Summary** tab of the **Assessment Details** window includes charts that indicate overall compliance and risk scores. The**Control Results** tab provides detailed scores for each subcontrol in the assessment.



The compliance score shows an entity's overall compliance score. By default, the score is on a scale of 0-100, where 0 is not compliant and 100 is fully compliant. The control score shows the entity's average weighted subcontrol score (percentage scale 0-100). The subcontrol weight is proportional to the total weight of all the subcontrols. Risk Score is calculated as Risk x Weight x Criticality.

The scoring mechanism can be customized. For more information, contact Technical Support.

Risk Scoring

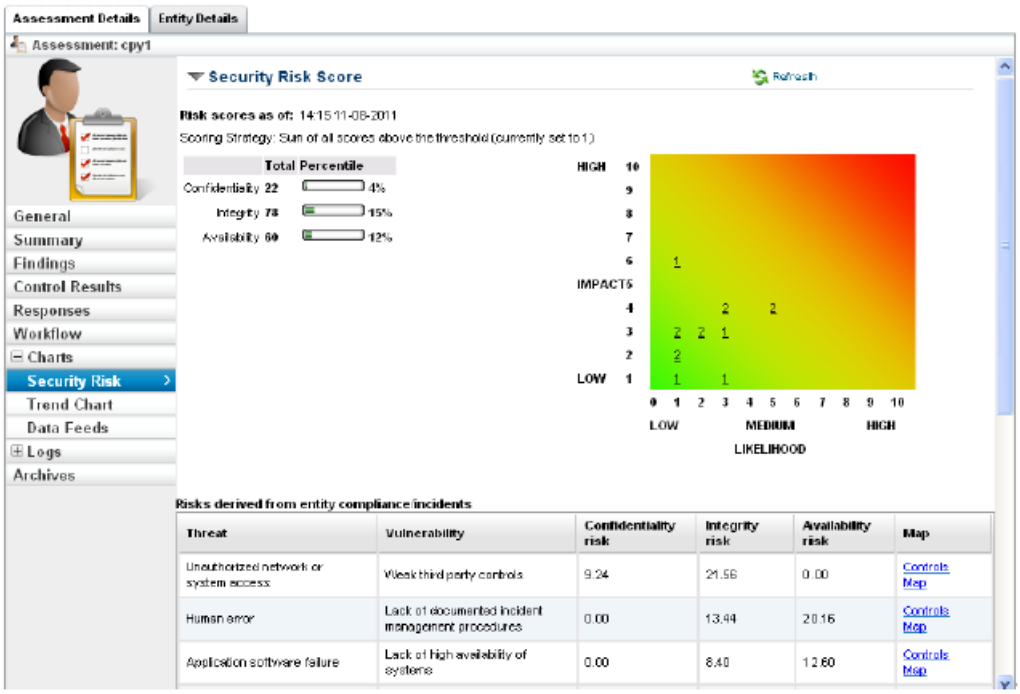
Risk scores are not normalized, but you are always able to use the current risk score to compare across entities.

For example, if entity A has a score of 150 and entity B has a score of 300, that means that entity B is twice as risky as entity A. Converting the numbers to percentages would not help in terms of comparison across entities, because the numbers are simply relative to each other whether it is a percentage or not.

Do not confuse the simple risk score (sometimes called just "risk score") with the total inherent or total risk score; the total scores may be different from the simple risk score.

Security Risk Score

Security risk score is derived from exposure and likelihood of risk and asset's criticality. In the assessment details, the security risk page of the charts tab displays the security risk score for an entity.



Configure the following settings in .properties file to display the security risk score:

1. Set the following property to enable the security risk score:

   com..risk.security.enabled=true

2. Specify an integer value in the following property to calculate the desired total percentile results for confidentiality, integrity and availability.

   com..risk.high.risk=

   The total percentile is calculated as the percentage of confidentiality, integrity, or availability divided by the integer value specified in the com..risk.high.riskproperty.

   [(confidentiality or integrity or availability)/com..risk.high.risk=]*100

   Where confidentiality, integrity and availability values are derived by aggregating the confidentiality risk, integrity risk and availability risk scores of risk(s) that are associated with an assessment.

When you finish configuring the properties, it is recommended to reload the server configuration within the **Commands** tab of **Administration** > **Server Administration** menu to reflect the changes.

Example:

If an assessment has three risks, with each risk having the confidentiality risks (5, 6, and 7), integrity risks (8, 9, and 10) and availability risks scores (11, 12, and 13), and com..risk.high.risk=300. In this case, the confidentiality is calculated by adding each risk's confidentiality risk score as:

5+6+7=18

and the total percentile value is calculated as:

(18/300)*100 = 6

Configuring Subcontrol Scoring

Resolver normalizes subcontrol, questionnaire question, and check scores on a scale of 0 - 10.

For a manual subcontrol, configure the check scoring by setting the question choice using the following method for each type of answer:

- **Radio button answers** : The highest choice score of all answers is normalized to 10, all the other answers choice scores are scaled using the same factor.
- **Check box answers**: The sum of all scores is normalized to 10, all other choices are scaled accordingly. The total score is the sum of all the user's selections.

For an automated subcontrol with extended subcontrols, the compliance score is also normalized between 0-10 by the connectors or as defined by server-side scripts. See the connector documentation for details on modifying the compliance score.

To customize compliance score settings for default content, copy the default content to your organization content folder. Settings are now modifiable.

Configuring Control Scoring

For the control score, Resolver shows the weighted average score of the subcontrols. The RiskVision solution can calculate the score as follows:

Sum (SC score * SC weight)
total weight

Where SC score is the subcontrol's normalized compliance score, **SC weight** is the value that you assigned to the subcontrol, and **total weight** is sum of all the subcontrol weights.

In questionnaire questions and for manual subcontrols, you can specify a weight for each question.

The score calculation for each question does not consider weight.

The score per question = {selected choice score} /Max of {all choice scores}

The weight factor is used when calculation the average score for a questionnaire.

The score per questionnaire = Sum {question score} * [{question weight} / Sum{question weight}]