# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>i</td>
</tr>
<tr>
<td><strong>1 Risk Management Cloud Service</strong></td>
<td>1</td>
</tr>
<tr>
<td>Overview of Oracle Risk Management Cloud Implementation</td>
<td>1</td>
</tr>
<tr>
<td><strong>2 Perspective Management</strong></td>
<td>3</td>
</tr>
<tr>
<td>Perspectives</td>
<td>3</td>
</tr>
<tr>
<td>Create or Edit a Perspective Hierarchy</td>
<td>3</td>
</tr>
<tr>
<td>Perspective Status</td>
<td>4</td>
</tr>
<tr>
<td><strong>3 Module Management</strong></td>
<td>7</td>
</tr>
<tr>
<td>Overview of Modules</td>
<td>7</td>
</tr>
<tr>
<td>Set Module Options</td>
<td>7</td>
</tr>
<tr>
<td>Specify Assessment Activity Types</td>
<td>8</td>
</tr>
<tr>
<td>Assessment Activity Types</td>
<td>9</td>
</tr>
<tr>
<td>Manage Module Perspectives</td>
<td>10</td>
</tr>
<tr>
<td>Data Migration</td>
<td>11</td>
</tr>
<tr>
<td>Import Template Options</td>
<td>12</td>
</tr>
<tr>
<td>Import Template Data Requirements</td>
<td>13</td>
</tr>
<tr>
<td><strong>4 Risk Management Administration</strong></td>
<td>15</td>
</tr>
<tr>
<td>Overview of Risk Management Administration</td>
<td>15</td>
</tr>
<tr>
<td>Set Email Alerts</td>
<td>15</td>
</tr>
<tr>
<td>Performance Configuration for Advanced Controls Management</td>
<td>16</td>
</tr>
<tr>
<td>Purge Advanced Controls Management Results</td>
<td>17</td>
</tr>
<tr>
<td>Data Sources</td>
<td>18</td>
</tr>
<tr>
<td>Synchronize Data</td>
<td>19</td>
</tr>
<tr>
<td>Global Users</td>
<td>19</td>
</tr>
<tr>
<td>Configure Global Users</td>
<td>20</td>
</tr>
<tr>
<td>Manage Lookups</td>
<td>21</td>
</tr>
<tr>
<td>Can I edit assessment responses?</td>
<td>23</td>
</tr>
</tbody>
</table>
## Jobs and Scheduling

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Jobs</td>
<td>25</td>
</tr>
<tr>
<td>Predefined Risk Management Jobs</td>
<td>25</td>
</tr>
<tr>
<td>View Job Details</td>
<td>26</td>
</tr>
<tr>
<td>Manage Export Jobs</td>
<td>27</td>
</tr>
<tr>
<td>Cancel or Purge Jobs</td>
<td>27</td>
</tr>
<tr>
<td>Modify Schedules</td>
<td>28</td>
</tr>
</tbody>
</table>
Preface

This preface introduces information sources that can help you use the application.

Using Oracle Applications

Using Applications Help

Use help icons to access help in the application. If you don’t see any help icons on your page, click your user image or name in the global header and select Show Help Icons. Not all pages have help icons. You can also access Oracle Applications Help.

Watch: This video tutorial shows you how to find help and use help features.

You can also read Using Applications Help.

Additional Resources

- **Community:** Use Oracle Cloud Customer Connect to get information from experts at Oracle, the partner community, and other users.
- **Guides and Videos:** Go to the Oracle Help Center to find guides and videos.
- **Training:** Take courses on Oracle Cloud from Oracle University.

Conventions

The following table explains the text conventions used in this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates user interface elements, navigation paths, or values you enter or select.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates file, folder, and directory names, code examples, commands, and URLs.</td>
</tr>
<tr>
<td><strong>&gt;</strong></td>
<td>Greater than symbol separates elements in a navigation path.</td>
</tr>
</tbody>
</table>

Documentation Accessibility

For information about Oracle’s commitment to accessibility, visit the Oracle Accessibility Program website.

Videos included in this guide are provided as a media alternative for text-based help topics also available in this guide.
Contacting Oracle

Access to Oracle Support
Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit My Oracle Support or visit Accessible Oracle Support if you are hearing impaired.

Comments and Suggestions
Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: oracle_fusion_applications_help_ww_grp@oracle.com.
1 Risk Management Cloud Service

Overview of Oracle Risk Management Cloud Implementation

Oracle Financial Reporting Compliance and Oracle Advanced Controls Management run as modules of Oracle Risk Management Cloud Service. To prepare Risk Management for use, set up and manage:

Perspectives

A perspective is a set of related values. Users can associate individual perspective values with individual objects, such as risks or controls. Perspectives can serve as filtering values in reports or in the pages in which users manage objects. They also play an important role in securing Risk Management.

Security

Job roles consist of duty roles and privileges, which define functional access. Roles are associated with data security policies, which define data access. Predefined data security policies map to predefined roles, but you’re expected to use those predefined elements to create your own roles and policies. You must create these elements if you want to incorporate perspectives into your security structure. (For more on security configuration, see Oracle Risk Management Cloud: Securing Oracle Risk Management.)

Modules

A module is an independent set of objects that relate to one another in a way that defines a governance, risk, and compliance environment. Financial Reporting Compliance and Advanced Controls Management are modules of Risk Management, and each requires configuration:

- As you set up Financial Reporting Compliance, you may select features available for each object in the module.
- To set up either module, you select perspectives whose values may be assigned to each object in the module. You may also use a data-migration utility to upload operational or perspective data.

Administration

You can set features that configure Risk Management for use and routine maintenance.

Some of these apply generally. You can, for example, edit the values users can select in list-of-values fields throughout the application.
Other features are module-specific:

- In Advanced Controls Management, you can set performance options. Or you can purge older results of Advanced Controls Management analysis.

  Administration features for Advanced Controls Management also include data synchronization and global user management. Synchronize data and global users regularly as you use Advanced Controls Management, typically in coordination with the running of models or advanced controls.

- In Financial Reporting Compliance, you can edit assessment responses.

**Jobs and Scheduling**

You can schedule and manage background tasks such as the export or import of operational data. As an implementation task, you may import your risk and control framework for use with Financial Reporting Compliance. Or you may import delivered content, a set of models created by Oracle for use with Advanced Controls Management.
2 Perspective Management

Perspectives

A perspective is a set of related, hierarchically organized values. The root value (the one all others are related to) may be organization, region, regulatory code, or any other concept you determine to be meaningful. You assign individual perspective values to individual Risk Management object records, establishing a context in which these object records exist.

- In the Financial Reporting Compliance module, you may assign perspective values to processes, risks, and controls.
- In the Advanced Controls Management module, you may assign perspective values to models, advanced controls, and incidents.
- You don't assign perspective values to any component of Access Certification.

For example, an Organization perspective might contain values that map the structure of your company. Divisions might be immediate children of the organization; each division might be the parent of a set of business units; and so on. This would enable the company to associate individual risks, controls, or other objects with the divisions, units, or other corporate entities they apply to.

Perspectives and Security

Job roles consist of duty roles and privileges that define functional access. Data security policies define sets of data. Roles map to data security policies, so that a user assigned a role can apply its functionality to data defined by a mapped policy.

As you configure a data security policy, you may assign perspective values to it. If so, it would grant access only to data concerning objects associated with the same perspective values. (This security restriction, however, doesn't apply to Access Certification.)

To use the Organization example, a user might be assigned a job role associated with a single data security policy. That policy might specify the Organization perspective value for a particular business unit. The user would have access only to data records assigned that value, which therefore pertain to the business unit it represents.

Create or Edit a Perspective Hierarchy

To create or edit a perspective hierarchy, name it and set other high-level details, create or modify perspective values, then define their hierarchical relationships.

1. Select Perspectives under Risk Management Tools. Then either:
   - Select the create action.
   - Click the row representing a hierarchy and select the edit action.

2. As you create a hierarchy, enter a name, select a type, and set a status (Active or Inactive). You may also create a description. As you edit a hierarchy, you can modify the status or description, but you can't edit the name or type.

   You may select a given type value for any number of hierarchies. However, all values for a given type must be unique. Hierarchies of a given type may not share values. A given value may be used in more than one hierarchy only if the hierarchies are of different types.
3. Use the Perspective section to create any number of perspective values. For each, a name and a status (Active or Inactive) are required. You may add a description or attach documents.

The first value you create is the root node. You can’t move it from that position. Its name may match the name of the perspective hierarchy, but it doesn’t have to.

4. Also in the Perspective section, adjust the relative positions of all but the root node to define hierarchical relationships. A parent node is situated above and to the left of a child node. Nodes are peers if they’re indented equally. A child node is situated below and to the right of its parent.

For ease of working with a large hierarchy, you may select among view options that expand or collapse either all nodes, or all that descend from a node you have selected.

5. Typically as you edit a hierarchy, select any value in the Perspective section to view information about it in the Perspective Details section. The section provides general configuration details, and it identifies objects this value has been assigned to.

After you create a perspective hierarchy, you must associate it with the types of object users can assign its values to. Until you do, the perspective hierarchy isn’t available for use. Map hierarchies to object types in the Module Perspectives page, among the Setup and Administration tasks under Risk Management Tools.

Related Topics
- Manage Module Perspectives

Perspective Status

In the Perspectives work area, you assign Active or Inactive status to perspective hierarchies and to perspective values as you create or edit them. In the Module Perspectives page of the Setup and Administration work area, you assign Active or Inactive status to the mappings of hierarchies to object types. Changing the status of a value, hierarchy, or mapping from Active to Inactive has ramifications:

- Before you can inactivate an active perspective value, you must remove it from all instances of objects for which it’s selected. If the perspective value is the hierarchical parent of other values, you must also remove the child values from objects for which they’re selected.

When you inactivate a parent value, all its child values are inactivated automatically. If you add child values to an inactive parent, they’re inactive, and you can’t change their status. When you activate the parent value, the child values become active automatically.

- Before you can inactivate an active hierarchy, you must complete two tasks: Remove all its values from all instances of objects for which they’re selected. Also, inactivate its mappings to object types in the Module Perspectives page. While a hierarchy is inactive, you can’t reset these mappings to active, and the hierarchy isn’t available to be selected for new mappings.

- You can edit an inactive perspective hierarchy. Typically, Inactive is the preferred status for a hierarchy that is in development. All values you create for it are also inactive, and you can’t change their status until you activate the hierarchy itself.

- Before you can inactivate the mapping of a perspective hierarchy to an object type, you must remove all values of the hierarchy from all instances of the mapped object.

- A functional alternative to inactivating a hierarchy is to inactivate its mappings to all object types. Whether the hierarchy itself is inactive, or is active but has no mappings, its values are no longer available to be assigned to objects.
• In the Perspective Assignment region of pages to create or edit objects, a hierarchy is no longer presented in the Perspective list field if it’s inactive or if its mapping to the object type is inactive. An inactivated value is no longer presented for selection in its hierarchy.

• A data security policy, which defines users’ access to data records, may contain filters that specify perspective values. If you inactivate a perspective value cited in one of these filters, the policy isn’t updated. Because the policy attempts to select records on the basis of a criterion that effectively no longer exists, it may not provide appropriate data access to some users. This is true no matter which is inactive: the value itself, its hierarchy, or the hierarchy mapping to an object type affected by the policy. To restore the policy’s effectiveness in providing access, edit it either to delete filters specifying inactive perspective values, or to replace them with filters specifying active perspective values.

Related Topics

• Manage Module Perspectives
Module Management

Overview of Modules

A module is a set of objects that define a governance, risk, and compliance environment. The objects in a given module relate to one another, but they’re independent of objects in other modules.

- In Advanced Controls Management, objects include Model, Advanced Control, and Incident. Users can create models that define risk, develop controls from those models, and run controls to identify incidents (records of transactions or access assignments that violate controls).
- In Financial Reporting Compliance, objects include Process, Risk, and Control (as well as dependent objects such as Issue, Remediation Plan, Event, or Consequence). Users can define business processes, identify risks that may affect those processes, and create controls to address those risks.

The following configuration options apply only to the Financial Reporting Compliance module:

- Determine features available to each of the Process, Risk, and Control objects, by selecting from standard sets of features.
- Select assessment activity types for each object.

The following configuration options apply to both Financial Reporting Compliance and Advanced Controls Management:

- Select perspectives whose values may be assigned to each object in the module.
- Use a data-migration utility to upload operational and perspective data (for Financial Reporting Compliance) or perspective data only (for Advanced Controls Management).

To work with modules, select Risk Management Tools in the home page. Among its options, select Setup and Administration.

Set Module Options

You can select the features available for each of the Process, Risk, and Control objects in Financial Reporting Compliance. The array of features depends on the object you’re configuring. (These options don’t apply to the Advanced Controls Management module.)

Note: Once you enter operational data for an object within a module, you can’t change the configuration you establish for that object. For example, you may hide the Event and Consequence features for the Risk object. Once you create a risk, you can no longer expose the Event and Consequence features.

To select an object to configure:

1. In the Setup and Administration work area, select the Configure Module Objects tab.
2. Expand a Financial Reporting Compliance entry.
3. In the expanded list, select an object: Process, Risk, or Control.
4. Select Edit.
Result
This option determines whether a Result tab appears in the management page for a process, risk, or control in Financial Reporting Compliance. If so, a Results page can display incidents generated in the Advanced Controls Management module, and assigned there to other modules.

- Select Show (the default) or Hide.
- This option applies to processes, risks, and controls.

Event
This option determines whether the Event region is available in the pages to create, edit, and manage risks. If so, users can define distinct sets of circumstances under which a risk may manifest itself. If events are hidden, consequences are also hidden.

- Select Show or Hide (the default).
- This option applies only to risks.

Consequence
This option determines whether consequences are displayed with related events in the Events region of the pages to create, edit, and manage risks. If so, users can define the expected impact of each event.

- Select Show or Hide (the default).
- This option applies only to risks.

Treatment
This option determines the tools available in the Risks page for users to alleviate risks.

- Select:
  - Hide and Default: Related-control stratification is available. Treatments and treatment plans are hidden. This is the default setting.
  - Show: Treatment, treatment plans, and control stratification are available.

- This option applies only to risks.

Specify Assessment Activity Types
You can specify the activity types available for users to select as they create assessment templates or set up impromptu assessments. Ultimately, each type defines what assessors are to determine as they complete assessments. You can also edit text associated with each activity. (These tasks don’t apply to the Advanced Controls Management module.)

Select an Object
To select an object whose activity types you want to specify:

1. In the Setup and Administration work area, select the Configure Module Objects tab.
2. Expand a Financial Reporting Compliance entry.
3. In the expanded list, select an object: Process, Risk, or Control.
4. Select Edit.

Select Activities

All assessment activities for all three objects are available by default.

- Clear the Include option for each activity type you don’t want to make available for the object you’re configuring.
- Ensure that the Include option remains selected for the activity types you do want to make available.

**Note:** Once you enter operational data for an object, you can’t modify the set of assessment activities available for that object. For example, you may deselect the Documentation Update activity for the Process object. Once you create a process, you can’t restore that activity.

Edit Activity Text

Each activity type includes the following components:

- Guidance text: A broad statement of purpose an assessor may consult while completing an assessment of the object you’re configuring.
- Activity question: A question (or statement) to which an assessor must respond while completing an assessment. The response determines, in effect, whether an instance of the object passes or fails the assessment.
- Response details: Possible answers to the activity question.

Click the row for each included activity to display its guidance text, activity question, and response details.

You can edit the guidance text and activity question, either before or after operational data exists. Prior guidance text and activity questions continue to apply to assessments undertaken before the edits are made. New guidance text and activity questions apply to assessments begun after the edits are made.

To edit response details, navigate to the Assessment Results page.

**Related Topics**

- Can I edit assessment responses

Assessment Activity Types

An activity type defines the scope of an assessment. Each activity type applies to assessments of particular objects. Types include:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Available for Assessment Of</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certify</td>
<td>Is the information in this assessment of an object accurate and complete?</td>
<td>Process, risk, control</td>
</tr>
<tr>
<td>Audit Test</td>
<td>Does a risk, control, or process meet audit guidelines?</td>
<td>Process, risk, control</td>
</tr>
<tr>
<td>Operational Assessment</td>
<td>Does a control or process operate effectively and as designed?</td>
<td>Process, control</td>
</tr>
</tbody>
</table>
Manage Module Perspectives

Placing a perspective hierarchy in use is a two-phase process. First, you create the perspective hierarchy. (You use the Perspectives work area under Risk Management Tools to do so.) Second, you map the hierarchy to objects that exist in a module. Until you map a perspective hierarchy to an object, it isn’t available for use with instances of that object.

To complete the second phase:

1. Open the Module Perspectives page. In the Setup and Administration work area, select the Module Perspectives tab.
2. Click the row for the module in which you want to map perspectives to objects. Then select Edit.
3. In a new page for the module you have selected, click Create. Or, select the row for an existing mapping and click Edit.
4. As you create a mapping, select a perspective hierarchy in the Name field. Select the object you want to map to it in the Associated Object field.
   - In Financial Reporting Compliance, you can map perspective hierarchies to the Process, Risk, and Control objects. In Advanced Controls Management, you can map perspective hierarchies to the Model, Control, and Result (Incident) objects.
   - Once you save a mapping, the fields in which you enter your hierarchy and object selections become read-only. You can’t edit these values.
   - You can’t map more than 15 perspective hierarchies to each type of object.
5. As you create or edit a mapping, specify whether a perspective is required. If so, a user can’t save an instance of the object unless a value for the perspective is selected.
   - Before operational data exists in a module, you can modify the setting of the Required option as you want.
   - After operational data exists in the module, you can change a required perspective to optional, but you can’t change an optional perspective to required.
6. As you create or edit a mapping, select a status, Active or Inactive.
   - Before you select Inactive status as you edit an active mapping, you must remove all values of the perspective hierarchy from all instances of the mapped object.
   - When you inactivate a mapping, the hierarchy is no longer presented in the Perspective list field of the Perspective Assignment region in pages to create or edit the mapped object.
   - The perspective hierarchy with an inactive mapping doesn’t count toward the 15-hierarchy limit for an object type.

### Table: Types of Assessments

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Available for Assessment Of</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design Review</td>
<td>Is a control or process designed effectively and does it meet its guidelines?</td>
<td>Process, control</td>
</tr>
<tr>
<td>Documentation Update</td>
<td>Does a process have required documentation?</td>
<td>Process</td>
</tr>
<tr>
<td>Assess Risk</td>
<td>Is a risk appropriately documented, is its analysis current, is its evaluation accurate, and are controls related to it?</td>
<td>Risk</td>
</tr>
</tbody>
</table>
Data Migration

A Data Migration utility uploads operational data for Financial Reporting Compliance, or perspective data only for Advanced Controls Management. You may use it to load an initial set of data, or to update data, in a single instance. Or you may use it to migrate data from one instance to another, for example from a development environment to a test environment.

Note: The Data Migration utility enables you to upload or download only data to which your roles and their related data security policies give you rights.

To use Data Migration, select the Data Migration tab in the Setup and Administration work area. The procedure involves:

- Generating a template
- Updating the template with operational or perspective data
- Running an import process

For Financial Reporting Compliance, operational data includes object and perspective specifications, transactions against the objects (for example, issues or assessments), and how these items relate to one another.

Generate a Template

To generate a Data Migration template:

1. In the Data Migration page, click the row representing the module into which you want to upload data.
2. Click the Create Import Template button.
3. In a Create Import Template dialog, select a data option:
   - Without Data creates a blank template. This is appropriate in either of two cases: You plan to upload data into an environment in which no operational data exists yet. Or, your upload data has no relationships to data already existing in your target environment.
   - With Data - All Objects or With Data - Perspectives Only creates a template containing all of your operational data or only your perspective data. Use one of these options if you plan to upload data that defines new associations to existing data, or sets new values for perspectives that already exist. These options also apply if your upload data includes some records with associations to existing data, and other records with no associations.
4. Click OK. A message presents an identifying number. Make a note of it, then close the message. Retrieve the template from the record of the job in the Monitor Jobs page.

Update the Template

The template is an Excel workbook organized into tabbed worksheets.

- For Financial Reporting Compliance, use any of the worksheets in the template. A given worksheet may hold information pertinent to a type of object or to perspectives, or may define object-to-object, object-to-perspective, or object-to-transaction associations.
• For Advanced Controls Management, use only the worksheets that contain perspective data: Perspective, Perspective Item, and Perspective Hierarchy. No other worksheets should contain any data.

If you’re working with a blank template, add new records to it.

If you’re working with a template populated with existing data:

• Identify and retain records of existing objects that are to be associated with new records.
• Delete all other existing records.
• Add records of new objects, perspectives, or transactions.
• For Financial Reporting Compliance, use association tabs to define relationships between new and existing records. Remove rows that define relationships of existing records to one another.
• The template may contain both new records with associations to existing records and new records with no associations to existing data.
• Except to define new associations, you can’t modify the record of an existing object. For example, for Financial Reporting Compliance you can’t edit the row for an existing risk to modify its description.

When you finish editing the template, save it in .xml format.

Import the Template

To import an updated template:

1. In the Data Migration page, click the row representing the module into which you want to upload data.
2. Click Import Data File.
3. In an Import File dialog, browse for and select your template file.
4. Click Import.
5. Navigate to the Monitor Jobs page to check on the status of the import job.

Related Topics

• Manage Export Jobs

Import Template Options

The Data Migration template is an Excel workbook organized into tabbed worksheets. Each tab is devoted to a particular type of data.

For the Financial Reporting Compliance module, you can import:

• Object data. In distinct worksheets, supply data that defines processes, risks, controls, test plans, and risk models.
• Transaction data. In distinct worksheets, supply data that defines assessments, issues, and attachments.
• Perspective data.
  o In a Perspective worksheet, name and assign type codes to your perspectives.
  o In a Perspective Item worksheet, define values for all your perspectives. (You select a type code for each value in this worksheet. It must match the type code for the perspective that the value belongs to. The code for the perspective is set in the Perspective worksheet.) A perspective item name can’t exceed 50 characters.
In a Perspective Hierarchy worksheet, define relationships. Each row defines a parent/child relationship between two values from the Perspective Item worksheet. Each row also relates its pair of values to a hierarchy defined in the Perspective worksheet. Specifically:

- In a PERSP_ITEM_NAME column, enter the name of a value that's the parent of another value.
- In a CHILD_NAME column, enter the name of a value that's the child of the value in the PERSP_ITEM_NAME column.
- In a TREE_NAME column, enter the name of the perspective hierarchy both values belong to.
- In a ROOT column, enter Y if the PERSP_ITEM_NAME column contains the root value of the hierarchy, or N if it doesn’t.

Association data. Distinct worksheets define how processes relate to risks; how risks relate to controls; how perspective values relate to processes, risks, or controls; and how issues relate to the items they’re raised against.

In each case, the worksheet title specifies the two associated items. For example, a Risk Control worksheet defines how individual risks relate to individual controls. To define an association, you match the ID for one item with the ID for another. These IDs are established in the worksheets that define the items.

For the Advanced Controls Management module, you can import perspective data only.

**Import Template Data Requirements**

As you enter data into an import template, keep the following in mind:

- The first column of each worksheet contains ID values. Each must be a number that’s unique within its worksheet.
  
  These values apply only within the template; they’re not imported into the Risk Management database. Use them to establish relationships between objects. For example, you create an ID for a control in the Control tab, and an ID for a risk in the Risk tab. Then you specify those IDs in a row of the Risk Control tab to relate the risk to the control.

- Never enter or modify values in SYSTEM_ID or REVISION_NUMBER columns. For new data, these values should be blank. For existing data, these are system-generated. Any modifications prevent records from being recognized when they’re imported, and so generate errors.

- In each worksheet, some information is required, and some not. If a column contains required data, its header says so. In some cases, though, optional information is highly desirable. For example, on the Control tab, Description isn’t required. Typically, however, the description of a control defines what it does to mitigate a risk, and so you would want to provide one.

- In general, columns (other than those that display ID values) correspond to fields in the user interface. For example, the Control tab contains an ASSERTION_CODE column. It may contain values you would enter in the Assertions field of the page to create or edit a control. If you’re uncertain of appropriate content for a column, review user documentation for the field or page it represents.

- For a STATE_CODE column, blank equals APPROVED. Enter a value in this column only to select a state other than APPROVED.

- The value in a NAME column can’t exceed 150 characters.

- In text columns, don’t use these characters: ampersand (&), apostrophe (‘), hash (#), less than (<), greater than (>), asterisk (*), or equals (=). Also, don’t use the Enter key to create a line break.

- If a column corresponds to a check box on the user interface, enter Y for selected or N for cleared.
• Some worksheets contain an ACTIVITY_CODE column. Values represent activities you can complete in an assessment. Enter only the following codes:

<table>
<thead>
<tr>
<th>Activity Code</th>
<th>Activity Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASSESS_RISK</td>
<td>Risk assessment</td>
</tr>
<tr>
<td>AUDIT</td>
<td>Audit</td>
</tr>
<tr>
<td>AUDIT_TEST</td>
<td>Audit test</td>
</tr>
<tr>
<td>DESIGN_ASSESS</td>
<td>Design assessment</td>
</tr>
<tr>
<td>DOC_UPDATE</td>
<td>Documentation update</td>
</tr>
<tr>
<td>CERTIFY</td>
<td>Certification</td>
</tr>
<tr>
<td>OPERATING_ASSESS</td>
<td>Operating assessment</td>
</tr>
</tbody>
</table>

• When you finish entering data into the template, save it in the .xml file format.
Overview of Risk Management Administration

You can set features that configure Risk Management for use and routine maintenance.

- Among application-configuration tasks, you can perform general maintenance and setup. You can also manage global users and data sources, and synchronize data.
- You can modify lookups, which store values displayed in Risk Management lists of values.
- You can edit the text a user may select as responses to Financial Reporting Compliance assessment questions.

To set these options, select Risk Management Tools in the home page. Among its options, select Setup and Administration. Tabs in the Setup and Administration work area open pages in which you can configure administration features.

Set Email Alerts

You can set Risk Management to send email messages to users when new worklists or notifications contain tasks that require their attention.

- A worklist is a record of a task that requires its recipient to act. It’s also a link to the page on which he or she can complete the action.

  For Advanced Controls Management, a worklist is a record of incidents generated by a control for which the user is a result investigator. Each worklist encompasses all pending incidents generated by that control. If any incident on an existing worklist remains pending, and the control generates new incidents, these are added to the existing worklist. Risk Management sends an email alert only when a new worklist is created, not when new incidents are added to an existing worklist. A new worklist is created only if a control generates incidents after all earlier incidents for that control have been resolved.

  For Financial Reporting Compliance, the worklist displays a name for the task, a description, and the name of the object the task applies to. The task description is a brief statement of the action the recipient is intended to take. "Draft" indicates work that the user has begun but not yet completed. For example, he may have saved an object, but not submitted it for review. Other task descriptions, such as "Review" or "Complete Assessment," are self-explanatory.

- A notification is a record of a task that doesn’t require action, even though the recipient has an interest in the task. In Advanced Controls Management, a notification announces the creation or edit of an advanced control to which the user’s roles give access. In Financial Reporting Compliance, a notification is a record of a task that involves the recipient indirectly. For example, she may oversee the actions of those who are assigned to complete the task.

Access Certification works somewhat differently. It doesn’t generate worklists or notifications in the sense defined above. It can, however, send email messages that directly notify users of approaching or passed deadlines, or of tasks to be completed. You would need to enable email alerts for this feature to be active.

To enable email alerts:

1. Select the Application Configurations tab in the Setup and Administration work area.
2. Within Application Configurations, ensure that the General Maintenance tab is selected.
3. In the Email Alerts region, select the Enable check box.
4. Click Test Connection to ensure that Risk Management communicates with your email server.
5. Set a schedule on which alerts are generated: Enter or select a start date, and set the number of hours between one transmission of alerts and the next.

You can also click Run Now to send unscheduled alerts immediately. Doing so has no effect on the schedule you create.

Performance Configuration for Advanced Controls Management

You may modify settings that improve performance by reducing the number of records involved in data-intensive operations. These settings apply to the Advanced Controls Management module.

Access Performance Configuration

By default, the number of records an access model can return is limited to 5,000. You can set this value lower, but not higher. This limit applies only to results returned by access models. It doesn't apply to incidents generated by access controls.

A model may return records slightly in excess of the limit. Once a record of a user with an access conflict is included in the result set, all records involving that user must be included. So when the limit is reached, analysis may continue until records are complete for all users already included in the return set. Once the limit is reached, however, no records are added for users not already included in the return set.

On the other hand, model results may fall short of the limit if global users are configured in such a way that individual global user IDs are associated with more than one actual user.

Also by default, users can't override the limit as they run models. You may, however, select an option that permits users to override the limit on a model-by-model basis.

Transaction Performance Configuration

In Advanced Financial Controls, each business object belongs to a category. A Transaction object contains records that pertain to actual transactions. These are expected to be created or updated frequently and in large volume. An Operational object or a Configuration object consists of master-data or setup records that change infrequently.

For Transaction business objects, data synchronization operates on records created or updated on or after a cutoff date you specify. This date is required; data-synchronization jobs fail if no date is set. This cutoff date has no effect on Operational or Configuration business objects. For them, a synchronization job encompasses all records, no matter when they were created or updated.

The cutoff date for Transaction-object data forms one boundary for a time period during which data is selected. It’s static, but the other boundary, the current date, is dynamic. As time passes, the period grows longer, and so the amount of data available for synchronization grows larger. Reset the cutoff date periodically, so that you maintain a time period short enough to produce an amount of data that doesn’t impact performance negatively. Typically, the outside limit is two years’ worth of Transaction-object data. Note that incidents are automatically closed if they're related to records no longer subject to synchronization after you reset the cutoff date.
Audit Performance Configuration

In Advanced Financial Controls, Audit business objects store data intended for use in models and controls that perform change tracking. Such an object stores not only the most recently set value for a given field, but also the prior value. Audit business objects are included in data-synchronization runs along with other business-object types. However, records in Audit business objects aren’t synchronized if they’re older than a cutoff date you specify. This date is required, and is distinct from the cutoff date you set for the synchronization of Transaction business objects.

You should periodically reset the Audit cutoff date, like the Transaction cutoff date, to maintain a time period short enough to produce an amount of data that doesn’t impact performance negatively.

How to Set Performance Values

To set these values:

1. Select the Application Configurations tab in the Setup and Administration work area.
2. Within Application Configurations, ensure that the General Maintenance tab is selected.
3. In the Access Performance Configuration region:
   - The Result Record Limit Per Model field displays, by default, the value 5,000. Accept that value or enter a smaller number. The value can’t exceed 5,000.
   - A Record limit for access model analysis option is selected by default. It prevents the record limit from being overridden. You may select the Record limit for access analysis with ability to override at the access model level option instead. This allows a person who runs a model to have it return all possible results.
4. In the Transaction Performance Configuration region, enter the cutoff date for the synchronization of Transaction business objects. If you enter a date two years or more before the current date, also respond to a message asking you to confirm that you want the large data set that can be expected for your time span.
5. In the Audit Performance Configuration region, enter the cutoff date for the synchronization of audit events.

Purge Advanced Controls Management Results

Records of Advanced Controls Management incident or data set results remain even after they’re used. For example, incidents remain after they have reached an end status. You can purge incident or data set results generated before a date that you specify.

Consequences of a Purge Job

Note the following:

- When an incident is purged, all change history associated with the incident is also purged.
- Although an incident may be purged, the risk it represents may continue to exist in a business application. If so, the next run of advanced controls will regenerate the incident. However, any status or comments assigned to the incident before it was purged are lost.
- If other jobs, such as control analysis or data synchronization, are running, a purge job runs only after those jobs are completed. If a purge job includes a result that a user is actively viewing, that result is purged only after the user navigates away from it.
• Pending incidents appear in worklists. If you purge pending incidents, the worklists that listed them continue to exist, but lead nowhere. To prevent this, close the worklists before purging the incidents. To close worklists, you can:
  ◦ Identify pending incidents among those you intend to purge, and resolve them to a status at which they’re no longer pending.
  ◦ Inactivate controls that have generated pending incidents you intend to purge. To inactivate a control, edit it to set its status to Inactive.
• Reports generated before a purge continue to show records of purged incidents, even though those incidents no longer exist in Advanced Controls Management.
• An incident control may cite a user-defined object created from a data set control. If the incident control has generated incidents, and you purge the data set results, the incidents remain open. If you rerun the incident control without first rerunning the data set control, the incidents close, because the data to support them no longer exists. If you rerun the data set control, then rerun the incident control:
  ◦ The new data set may include data that had existed before the purge. Corresponding incidents are regenerated at the Assigned status, but without comments or audit history.
  ◦ The data set may include new data. From this data, new incidents may be generated, at the Assigned status.

How to Purge Results
To purge results:

1. Select the Application Configurations tab in the Setup and Administration work area.
2. Within Application Configurations, ensure that the General Maintenance tab is selected.
3. Enter values in these fields:
   ◦ Control Type: Select the type of control whose results you want to purge. You can select Access, Transaction, or Both.
   ◦ Created on or Before Date: Select a date. Risk Management purges results generated on or before that date.
4. Optionally enter values in these fields:
   ◦ Result Type: Select Incident or Data set, or select All to purge both types of result.
   ◦ Incident Status: Select All, Closed, or Closed and Inactive. If you select All, you purge incidents at every status: Closed, Inactive, Assigned, Accepted, Remediation, and Resolved.
   ◦ Control Name: Select one or more controls whose results are to be purged.
5. Click Run Now.

Data Sources
In Advanced Controls Management, a model or control consists of filters, and each filter cites a business object. Each business object is associated with a data source, which ultimately supplies data to be analyzed. There are several types:
• The Oracle Cloud instance subject to risk analysis by models and controls is the data source for most business objects.
• A data source called Internal captures data configured within Advanced Controls Management. For example, it supplies data to an Access Entitlement business object used by Advanced Access Controls.
• A data source called Imported Business Object applies to business objects imported in .xml files.
The Oracle Cloud data source must be connected to Risk Management, but this connection is already configured and you can’t change it. You can, however, view its details. You can also synchronize data. That is, you can update records in Advanced Controls Management with fresh data from the Oracle Cloud data source. To complete these tasks, select the Application Configurations tab in the Setup and Administration work area. Within Application Configurations, select the Data Sources tab.

Synchronize Data

To ensure transaction models and controls evaluate current data, run synchronization, a process that copies data from your Oracle Cloud data source to Risk Management.

- A standard synchronization updates data for business objects used in existing transaction models and controls. It imports records that have been newly added, and updates those that have changed, since the previous synchronization. It has no effect on records that haven’t changed.
- A graph rebuild deletes all data for your data source and replaces it with current data for existing models and controls. This typically takes longer than a standard synchronization, and it may have a significant effect on existing incidents, model results, and worklists. As a result, it isn’t to be performed lightly.

To run either job, select the Application Configurations tab in the Setup and Administration work area. Within Application Configurations, select the Data Sources tab.

Locate the row representing the data source you want to synchronize. In that row, click a button to display a menu of actions. Then select one of them:

- Synchronize Transaction, to run a standard synchronization once, immediately. A message displays a number; make a note of it.
  
  Check the status of the synchronization job in the Monitor Jobs page: Select the Monitor Jobs tab in the Setup and Administration work area. Review information in the row for the job whose number you noted.

- Schedule Synchronize, to create a schedule on which any number of standard synchronization operations run automatically. Enter values that set the name of the schedule, its start date and time, how regularly synchronization should occur, and an end date (if any). Then click the Schedule button.
  
  To track scheduled synchronization runs, navigate to the Scheduling page: Select the Scheduling tab in the Setup and Administration work area.

  - Rebuild Graph to perform a graph rebuild.

Related Topics

- Synchronize Data for an Individual Model
- View Job Details

Global Users

Risk Management assigns a global user ID to each person who uses business applications subject to models and controls created in Advanced Controls Management. An individual’s global user ID correlates to potentially varying IDs that person may have for business-application accounts.
For example, the global user ID would serve as a single identifier for an individual who marries, then changes her surname.

The use of the global user ID ensures that each person is recognized properly during segregation-of-duties analysis performed by Advanced Access Controls. In addition, models and controls created in Advanced Financial Controls may incorporate a User business object. The global user ID ensures that these models and controls account for people correctly.

You determine how global users are formulated. To do so, you select up to five attributes that can identify users uniquely. For example, one of the attributes is Email Address. In an environment in which each user is known to have a single, distinct email address, you might select only that attribute.

You then run a synchronization job, which identifies the following for each person:

- **Global user:** The first record with identifying-attribute values that apply to a given person. Risk Management adopts the user name for this record as that person’s global user name. The global user name, first name, and last name values for this record may be displayed in model results and incidents concerning the user.

- **Related users:** All other records with the same identifying-attribute values as those that generated a global user. Risk Management assigns related users the same global user name as that of the global user to which they’re related.

### Configure Global Users

You can select the attributes Risk Management uses to create global users. You can then either run the synchronization job that generates global users or schedule the job to run regularly. Having run the job, you can review the users it creates to evaluate whether you selected the best combination of attributes for deriving global users.

To complete any of these tasks, navigate to the Global User Configuration page:

- In Risk Management Tools, select the Application Configurations tab in the Setup and Administration work area. Within Application Configurations, select the Global User Configuration tab.
- In Advanced Controls Management, open the Related Links panel tab in either the Models or Controls page. Then select the Global User Configuration link.

### Select Attributes

Select one to five identifying attributes that, in combination, define users uniquely in your environment.

The attributes you select have an AND relationship. That is, two records are related only if values for all identifying attributes match. If the values for any attribute don’t match, the records constitute distinct global users.

Select identifying attributes whose values are most likely to be distinguishing and least likely to change over time in your environment.

**Note:** In your Oracle Cloud data source, every user has a unique user name. Therefore, the simplest way to configure global users is to select User Name as the only identifying attribute.

To select attributes:

1. In the Identifying Attributes region, select the attributes you want in the Available field. To select one, click it. To select a continuous set, click the first one, hold down the Shift key, and click the last one. To select a discontinuous set, hold down the Ctrl key as you click attributes.
2. Click the Move Selected Items button to move the attributes to the Selected field.
3. When you’re satisfied with your selections, click Save.
Modify Attributes
At any time, you can modify the selection of identifying attributes that define your global users. You may move attributes from the Selected field to the Available field, move new attributes from the Available field to the Selected field, or both.

Doing so, however, has a significant effect: When you save the new configuration, all existing global users are purged. So are access model results and control incidents. So are results and incidents for transaction models and controls that incorporate the User business object. New global users are created according to your new configuration when you run global-user synchronization. You would subsequently need to rerun models and controls to replace model results and control incidents.

Run or Schedule the Synchronization Job
Once you have saved a set of identifying attributes, or as you add, modify, or inactivate users in your business applications, run a synchronization job. Expand the Actions menu, then select either of these options:

- **Run**, to run a global-user synchronization once, immediately. A message displays a number; make a note of it.
  
  Check the status of the job in the Monitor Jobs page: Select the Monitor Jobs tab in the Setup and Administration work area. Review information in the row for the job whose number you noted.

- **Schedule**, to create a schedule on which global-user synchronization jobs run automatically. Enter values that set the name of the schedule, its start date and time, how regularly synchronization should occur, and an end date (if any). Then click the Schedule button.
  
  To track scheduled synchronization runs, navigate to the Scheduling page: Select the Scheduling tab in the Setup and Administration work area.

Review Global Users and Related Users
A Global Users grid displays records of the global and related users generated by the identifying attributes you have selected. Review these to determine whether your attributes identify each person uniquely.

Suppose, for example, you were to select Email Address as the only identifying attribute. As you review records in the grid, you may discover two global users, both displaying a single email address but each with its own user name. If your company expects unique email addresses, this person may have arranged for a second, "ghost" account to be created for himself. This may indicate suspect activity that requires investigation.

As you work with the grid, you can:

- **Use View options to select or reorder the columns on display, or sort their contents.**
- **Use query-by-example fields at the heads of the columns to filter records.**
- **Select a Show Where Related Users Exist option to determine which global users have related users. This is actually a filter that returns records in which the global user names match. (Risk Management assigns the same global user name to a global user and all its related users.)**

Manage Lookups
Lists of values in Risk Management pages are stored as "lookups." You can add values to some delivered lookups.
Each list of values has its own lookup table. An entry within a lookup table consists of these elements:

- A "lookup type" identifies the table in which a lookup value exists. In effect, it distinguishes lookup values belonging to one LOV from those belonging to others.
- Within a given lookup type, each entry correlates a "lookup code" to a "meaning." The code is an internal value. The meaning is the text that actually appears in an LOV.
- Each entry may also have a description.

Determine Lookup Type

To create a lookup value, first determine its lookup type:

1. Identify one value in the LOV in which the lookup is to appear. For example, if you’re creating a new perspective type:
   - Navigate to the Create Perspective Hierarchy page: Select Perspectives under Risk Management Tools, then select the Create action.
   - Expand the Type field in the Create Perspective Hierarchy page. Note one of its values, such as Major Process.
2. Open the Lookup Tables page: Select the Lookup Tables tab in the Setup and Administration work area.
3. In the Meaning field of the Search panel, enter the value you noted. Click the search button. The Search Results panel then presents one row that displays the lookup type to which you want to add. In the perspective type example, this value is GRCM_PERSPECTIVE_TYPE.

However, each of the following pages contains a Type field with no predefined values. For those fields, this method of determining a lookup type wouldn’t work. On each of the following pages, the correct lookup type for the Type field is:

<table>
<thead>
<tr>
<th>Page</th>
<th>Lookup Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Process or Edit Process</td>
<td>GRCM_PROCESS_TYPE</td>
</tr>
<tr>
<td>Create Risk or Edit Risk</td>
<td>GRCM_RISK_TYPE</td>
</tr>
<tr>
<td>Create Control or Edit Control</td>
<td>GRCM_CONTROL_TYPE</td>
</tr>
<tr>
<td>Create Issue or Edit Issue</td>
<td>GRCM_ISSUE_TYPE</td>
</tr>
</tbody>
</table>

Create and Edit Lookups

To create a lookup:

1. In the Manage Lookups page, select the Create Lookup action. A Create Lookup page opens.
2. In the Lookup Type field, enter the lookup-type value you have just identified.
3. Enter a code in the Lookup Code field. A code should consist of 30 or fewer characters. Use upper-case for alphabetic characters. Fill the space between words with an underscore.
4. In the Meaning field, enter text that’s actually to be presented in an LOV.
5. Optionally, describe the lookup in the Description field.
6. Select Save and Close.
To edit a lookup:

1. In the Manage Lookups page, search for the lookup you want to edit: In the Search panel, enter any combination of type, meaning, and description values, and click the Search button.
2. In the Search Results panel, click the row for the lookup you want to edit, then select the Edit Lookup action.
3. An Edit Lookup page opens. Modify the meaning or description value. (The lookup type and lookup code are presented as read-only values; you can’t edit them.)
4. Select Save and Close.

Can I edit assessment responses?

Yes, but only to a limited extent. Each response to an assessment activity question consists of a "response code" and a "response name." The latter is the text a user actually sees while assessing an object. Responses are listed in the Assessment Results page. To open it, click the Assessment Results tab in the Setup and Administration work area.

In that page, you:

- Can edit the response names.
- Can’t edit the response codes.
- Can’t add new responses or delete existing responses.

A response may apply to multiple questions for multiple assessment activities. For example, an assessor may select a NO OPINION response while completing the Risk Audit activity or any of the Operational Assessment, Design Review, and Audit Test activities for the Control or Process object. If you edit the name value for a response in one context, you edit it in all contexts.
5 Jobs and Scheduling

Overview of Jobs

Jobs are individual requests to synchronize data, evaluate models or advanced controls, export results, generate reports, or perform other background tasks. You run or schedule a job on the page to which the job applies, but you manage it in the Monitor Jobs page. You can:

- See the current status of a job and review job results.
- Manage files created by export jobs.
- Cancel some jobs.
- Purge job history.

Monitor Jobs is the landing page for the Setup and Administration work area in Risk Management Tools. In some cases, you can also reach it from pages in which you run jobs. For example, users run advanced controls from the Controls page in the Advanced Controls work area, and the Monitor Jobs page is available in a Related Links panel tab on that page. In such cases, click the Back button to return to the page from which you started.

Predefined Risk Management Jobs

Two predefined jobs run the first time you start Risk Management, and at scheduled intervals thereafter:

- Security Synchronization: Risk Management roles, and their assignment to users, are managed in the Security Console. The Security Synchronization job enables Risk Management to recognize changes made in that application. As role and data security policy definitions change, the job updates worklists so that users do not have access to worklists they’re no longer entitled to see, and do have access to worklists they’re newly entitled to see. The first time the job runs, it also maps predefined roles to predefined data security policies.


By default, these jobs run once a week, on Sundays. It’s anticipated you will modify the default schedules:

- Your ideal schedule for the Security Synchronization job should reflect the frequency of changes to roles, user assignments, and data security policies in your environment.
- Schedule the Report Synchronization job to run at a frequency (typically daily) that makes current data available to users who view Transaction Business Intelligence Enterprise analyses and reports.

Use the Scheduling page to modify the schedules for these jobs, or use its Run Now feature to run them on demand. Because these jobs must run regularly for Risk Management to function properly, you can’t cancel their schedules.

A third predefined job, Access Certification Synchronization, performs background tasks that support the Access Certification features of Advanced Access Controls. These include:

- Ensure the validity of administrator assignments to certifications. If any is invalid, replace it with an All Eligible Administrators value.
- Send notifications of certifications that are approaching their due dates or are past due.
• Update reporting tables with changes to administrator, owner, or certifier assignments.
• Update active continuous certifications with new assignments of scoped roles.

The job begins running only when you create your initial certification. At that point it runs once a day. You aren’t expected to modify this schedule.

View Job Details

By default, the Monitor Jobs page lists jobs submitted by any user in the last twenty-four hours. Each row provides summary information about a job: an identifying number as well as the job name and status.

Typically a job’s status updates automatically as the job progresses, from Queued to Started to either Completed or Failed. However, you may cancel a job. If you do, its status changes to Cancel Requested and ultimately to Canceled.

Some jobs may end in a Job completed with warnings status or a Job completed with errors status.

• The completed-with-warnings status applies when a job evaluates multiple controls, and some are invalid. The valid controls return results properly, while the invalid controls return warnings.
• The completed-with-errors status applies when elements of a synchronization job fail, but do not impact other elements of the job. For example, the job may fail for one business object, but synchronize data properly for all others.

Note: Job polling may take up to one minute. It’s therefore possible for a job to reach its end state up to a minute before the Monitor Jobs page displays its final status.

In the Monitor Jobs page, you can:

• Select filtering criteria that return a set of jobs other than those you see by default. Select the Show Filters link to set filtering options.
• Sort the list of jobs by job ID number, name, or submission date. Select one of these options in the Sort By field.
• Select the Expand icon in the row for any job to view additional details about it. These include the user name of the person who submitted the job, its type, and dates on which the job was submitted, started, and ended. Click the Collapse icon to close the expanded view.
• View the percentage completion of jobs at the Started status. This statistic appears beneath the status. To refresh it, click the refresh icon. This statistic doesn’t appear for jobs at other statuses.

You can also view information about a job’s run. Hover over the job’s status. If an underscore appears, additional information is available. In that case, click the status to open a Summary page presenting the additional data.

• A job at the Failed or Canceled status opens a display of messages explaining the failure or cancellation.
• A global-user synchronization job, the Report Synchronization job, or an import job displays the numbers of new and updated records processed by the job. The global-user synchronization job also displays a count of total processed records.

A transaction data synchronization job displays new, updated, and total values for each business object affected by the job, as well as counts of underlying associations among business objects. A job to import user-defined business objects displays these values for each imported object included in the job.

• Some jobs display a count of records processed by the job. These include model-analysis jobs; mass-edit jobs; and jobs to import or export models, controls, or global conditions.
• A control-analysis job presents the number of newly generated incidents and the number of updated incidents.
A job to analyze multiple controls is actually a set of distinct analyses, one of each control. When you click the status of a multiple-control analysis job, its Summary page serves as a child Monitor Jobs page, listing each control distinctly. For each control, it reports status and, if that status is Started, percentage completion. For each control that’s reached Completed or Failed status, you can click the status to open a child Summary page that presents record counts or messages.

If an incident control (or a model) calls user-defined objects, its Summary page displays elements hierarchically. The incident control is at the top of the hierarchy. Beneath it are data set controls that provide data to user-defined objects called by the incident control. Once again, each displays status, and you can click the status of each to view its results.

- A purge job shows the count of purged records.
- An Access Certification scoping job provides the number of job roles selected by scoping filters. The Access Certification Synchronization job shows the numbers of administrators, owners, and auditors added to or removed from certifications. The Synchronization job also shows the number of active continuous certifications, as well as the number of new assignments of roles to users since the previous run.

## Manage Export Jobs

Although you initiate an export job in the page to manage the type of data you’re exporting, you complete the job in the Monitor Jobs page.

You can:

- Export models, advanced controls, or global conditions in the Advanced Controls Management module.
- Export templates containing perspective data from Advanced Controls Management, or perspective and other operational data from Financial Reporting Compliance. A template serves as a vehicle for the import of new perspective or operational data.
- Export reports from either module.

To export data:

1. Initiate an export from the page for managing models or advanced controls, or from the Data Migration page. Or run a report from any of the reporting work areas for Financial Reporting Compliance or Advanced Controls Management. As you do, a message presents a job ID. Note the ID, then close the message.
2. In the Monitor Jobs page, locate the row displaying the job ID you noted. When its status is Completed, click the download icon. This icon appears only in the rows for export jobs.
3. A file-download window offers you options to open or save the export file. Select the Save option and, in a distinct save-as dialog, navigate to the folder in which you want to save the file. The download file is saved in .xml format.

## Cancel or Purge Jobs

If a job is at the Queued or Started status, you can cancel it. If a job is at any status other than Queued or Started, you can purge its record.

To complete either task:

1. In the Monitor Jobs page, select the check boxes in the rows for any number of jobs you want to cancel or purge.
2. Click the Cancel button or the Purge button. Note, however, that each button is active only if all the jobs you have selected are at a status appropriate for the action you’re taking.

3. Respond to a message that asks you to confirm the cancellation or purge.

The status of a canceled job changes first to Cancel Requested and ultimately to Canceled. The record of a purged job disappears from the Monitor Jobs page.

Modify Schedules

You may schedule a job to run. You create the schedule in the page the job applies to. For example, you can use the Financial Compliance Reports pages to schedule a report to be run. However, any schedule created anywhere is listed for review in the Scheduling page.

You can modify or discontinue a schedule you have created:

1. Select the Scheduling tab in the Setup and Administration work area.
2. Select the row that represents a schedule, then click the Edit option.
3. In a Schedule Parameter dialog box, do either of the following:
   - Enter new values in fields, and make new selections among radio buttons, to define a new schedule. Click the Reschedule button. The new schedule is then in force.
   - Click the Cancel Schedule button. The job is no longer scheduled to be run, and its row is removed from the Scheduling page.

**Note:** You can modify, but you can’t cancel, the schedule for either of two predefined jobs: Security Synchronization and Report Synchronization. If you use Access Certification, you should not modify the schedule for its predefined job, Access Certification Synchronization.

In addition to scheduling jobs, you can run them on demand. From the Scheduling page, click the row representing a job schedule, and click Run Now. This runs the job immediately, but doesn’t affect the schedule. The job runs again when its schedule next determines that it should.
Glossary

**assessment**
The review of a process, risk, or control to determine that it’s correct when created or remains appropriate over time. A batch assessment applies to many objects and is relatively complex. An impromptu assessment applies to a single object and is relatively simple.

**business object**
A set of related fields in a data source subject to models and controls created in Advanced Controls Management. While creating a model, a user selects one or more business objects that supply data for evaluation.

**data source**
The supplier of data to business objects cited in models and controls created in Advanced Controls Management. For most business objects, this is your Oracle Cloud instance. However, an Internal data source corresponds to the Advanced Controls Management instance in which you’re working, and supplies data to business objects such as User and Access Entitlement. Imported Business Object is a data source name that applies to business objects imported in .xml files.

**data synchronization**
A process to copy transaction data from a business application to Advanced Financial Controls, for analysis by models and controls. A standard synchronization involves only records that have been newly created or updated since the previous synchronization. Data synchronization doesn’t apply to Advanced Access Controls.

**global user**
An identifier assigned to each user of business applications subject to models and controls created in Advanced Controls Management. It correlates to potentially varying identifiers each person may have for business-application accounts. Global user IDs apply only to Advanced Controls Management, not to Financial Reporting Compliance.

**graph rebuild**
A form of data synchronization that deletes all data for a given data source and replaces it with current data required by existing models and controls.

**module**
A set of Risk Management objects that relate to one another, but are independent of objects in other modules. Financial Reporting Compliance and Advanced Controls Management are considered modules of Risk Management.

**panel tab**
A tab that provides supplemental information or functionality for the page. Each panel tab is on the right side of the page, has an icon as the tab label, and slides out when you open the tab.

**perspective hierarchy**
A set of related, hierarchically organized values. You assign perspective values to Risk Management objects to define a context they exist in. In Financial Reporting Compliance, these objects include processes, risks, and controls. In Advanced
Controls Management, objects include models, advanced controls, and incidents. These can serve as filtering values, but also play an important part in securing Risk Management Cloud.