Oracle Risk Management Cloud

Implementing Risk Management

20D
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>i</td>
</tr>
<tr>
<td>1 Risk Management Cloud Service</td>
<td>1</td>
</tr>
<tr>
<td>Overview of Oracle Risk Management Cloud Implementation</td>
<td>1</td>
</tr>
<tr>
<td>Multiple-Language Support in Risk Management</td>
<td>2</td>
</tr>
<tr>
<td>2 Jobs and Scheduling</td>
<td>5</td>
</tr>
<tr>
<td>Overview of Jobs</td>
<td>5</td>
</tr>
<tr>
<td>Predefined Risk Management Jobs</td>
<td>5</td>
</tr>
<tr>
<td>View Job Details</td>
<td>6</td>
</tr>
<tr>
<td>Manage Export Jobs</td>
<td>7</td>
</tr>
<tr>
<td>Cancel or Purge Jobs</td>
<td>8</td>
</tr>
<tr>
<td>Modify Schedules</td>
<td>8</td>
</tr>
<tr>
<td>3 Perspective Management</td>
<td>11</td>
</tr>
<tr>
<td>Perspectives</td>
<td>11</td>
</tr>
<tr>
<td>Create or Edit a Perspective Hierarchy</td>
<td>11</td>
</tr>
<tr>
<td>Manage Perspective Mappings</td>
<td>12</td>
</tr>
<tr>
<td>Perspective Status</td>
<td>12</td>
</tr>
</tbody>
</table>
4 Configuration and Administration

Overview of Risk Management Configuration and Administration 15
Data Migration 15
Import Template Options 17
Import Template Data Requirements 18
Set Email Alerts 19
Manage Lookups 20
Performance Configuration for Advanced Controls 22
Synchronize Data 23
Global Users 24
Configure Global Users 24
Purge Advanced Controls Results 26
Set Options for Financial Reporting Compliance Objects 27
Specify Assessment Activity Types 28
Assessment Activity Types 29
Edit Assessment Responses 30
Configure Flexfield Segments 30
Preface

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

Using Oracle 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 the Oracle Help Center to find guides and videos.

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

You can also read about it instead.

Additional Resources

• Community: Use Oracle Cloud Customer Connect to get information from experts at Oracle, the partner community, and other users.

• 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>boldface</td>
<td>Boldface type indicates user interface elements, navigation paths, or values you enter or select.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates file, folder, and directory names, code examples, commands, and URLs.</td>
</tr>
<tr>
<td>&gt;</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 run as modules of Oracle Risk Management Cloud Service. To begin using these modules, ensure that the Risk Management offering is selected in Functional Setup Manager (see the Using Functional Setup Manager guide). Then, to prepare Risk Management for use, set up and manage:

Jobs and Scheduling

You can schedule background tasks and monitor their results. Such tasks include, for example, evaluating models or advanced controls; synchronizing transaction, user, or role data; purging records; or exporting or importing 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. Predefined jobs called Security Synchronization, Report Synchronization, and Notification perform key background tasks. They run, however, only after you schedule them to run. As a setup task, determine and implement the schedules appropriate for your environment.

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.

Security

In Risk Management applications, you grant access to functionality by assigning job roles (and through them, duty roles and privileges). You grant access to data by appointing users who can work with individual records at owner, editor, and viewer levels. For more on security configuration, see Oracle Risk Management Cloud: Securing Oracle Risk Management.

Configuration and Administration

You can set features that configure Risk Management for use and routine maintenance. Some features apply generally. These include using a data-migration utility to upload operational or perspective data, determining whether users receive email alerts of tasks that require their attention, and editing values users can select in list-of-values fields throughout the applications.
Other features apply to Advanced Controls. You can set performance options, and purge older results of control analysis. You can also synchronize data and manage global users, operations that refresh transaction and user data that models and controls analyze.

Still others apply to Financial Reporting Compliance. You can select features and assessment activities available for processes, risks, and controls, and you can edit assessment responses.

Multiple-Language Support in Risk Management

Risk Management can store much of the text users enter in multiple languages. In general, you can save multiple values, one for each language, for any text attribute that could contain words. Examples include text you might enter in a Name or Description field. Each user would then see values in the language he or she chooses to work in.

There are exceptions. Some attributes store or return only a single value no matter what language a user chooses to work in. They include:

- System-generated values, such as IDs.
- Values that aren't text, such as numbers.
- Values, like codes, that contain letters that don't form words.
- Lists of values.
- Attachments (URLs or file names).
- Names of filters created for models in Advanced Controls, and values they search for. If a filter searches for values of an attribute that can be translated, it returns only the value in the “source language.” This is the language in which a user worked while creating the model that contains the filter. A Source Language column on the models page identifies the source language for each model.

Here's how Risk Management works with languages:

- Each user can choose a language, and can change that language at any time. One way to do this is to select a language while signing in to Oracle Cloud. Another way is to navigate to Settings and Actions > Set Preferences > Language, and then select either a default language or a language to be used in the current session.
- A user creates a record. As he enters its text-attribute values, he uses the language he's chosen to work in. Initially, all users with access to the record see the values in the language the creator chose.
- Another user, working in another language, edits the record to translate its text-attribute values. Now, users working in this second language see the translated values, but users working in any other language see the values in the original language.
- Users working in other languages open the original record and translate its text-attribute values into their languages. Once again, a user working in any of these languages sees the values in that language, while users working in languages for which no translations have been created see values in the original language.

Here's an example:

- Fred uses English. As he creates a new risk, he enters "This is my risk's name" in the Name field.
- Barry uses French. He changes the name of the risk to "C'est le nom de mon risque." Other French users see the French name, but users of all other languages see the English name.
- Fred, still working in English, sees "This is my risk's name." But he changes his language to French, and then sees "C'est le nom de mon risque."
• Maria uses Spanish. She opens the risk and sees "This is my risk’s name." She changes that value to "Este es el nombre de mi riesgo." All Spanish users see that; all French users continue to see "C’est le nom de mon risque"; users in all other languages still see "This is my risk’s name."

Here’s a recommendation: If you’re responsible for creating a record, prepare or review translations it will need before you make it visible to reviewers, approvers, managers, directors, auditors, and others. To do that, temporarily set your language to each of the translation languages. If you’re multilingual you may do this on your own, or you may collaborate with colleagues who are fluent in your translation languages.

Related Topics
• Best Practices for Transaction Model Development
2 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 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 from that page. In such cases, click the Back button to return to the page you started from.

Predefined Risk Management Jobs

Several predefined jobs perform background tasks related to security, notifications, and reporting.

- Security Synchronization: This job finds users who are no longer eligible to work with records for which they're authorized as owners, editors, or viewers. They may have lost eligibility because their role assignments changed. These users are marked as ineligible and lose access to the records for which they're no longer eligible. Note that ineligible users continue to have access until the job has run.

  When the Security Synchronization job runs, it also launches three other jobs. Each of these, however, is considered a separate job. Runs of these jobs have distinct entries in the Monitor Jobs page:

  - Result Worklist Synchronization updates Advanced Controls worklists to match current security definitions.
  - Financial Reporting Compliance Worklist Synchronization completes the same task in Financial Reporting Compliance.
  - Notification sends "bell" notifications to users of Advanced Controls and Financial Reporting Compliance when tasks require their attention. It may also send email alerts, but only if these have been enabled in the Manage Configuration Options page of the Setup and Administration work area.

- Report Synchronization: This job updates data in subject areas that support analyses run in Oracle Transaction Business Intelligence (OTBI). It handles Financial Reporting Compliance data, as well as Advanced Controls data concerning access and transaction controls and their results. However, it doesn't update data concerning model results in Access Controls.
Use the Scheduling page to set schedules for these jobs, or use its Run Now feature to run them on demand. (Unless you do one or the other, they don't run at all.)

- Your ideal schedule for the Security Synchronization job should reflect the frequency of changes to roles and user assignments in your environment.
- Because the Security Synchronization job launches the two worklist-synchronization jobs, you don't do anything to schedule or run them. Their runs are dependent on the schedule you set for Security Synchronization, and they don't appear in the Scheduling page.
- Although the Security Synchronization job also launches the Notification job, you can create a separate schedule for it. If you do, schedule it to run frequently enough (typically daily) to capture actions that generate new bell and email notifications.
- Schedule the Report Synchronization job to run at a frequency (typically daily) that makes current data available to users who view OTBI analyses. Note, though, that one subject area, called Advanced Access Models Real Time, has its own synchronization job, which must be run manually.

An additional predefined job, Access Certification Synchronization, performs background tasks that support Access Certification. These include:

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

Unlike the other jobs, you don't need to schedule Access Certification Synchronization. It begins running when you create your initial certification, and then runs once a day. You aren't expected to modify this schedule.

**Related Topics**

- Set Email Alerts
- Synchronize Access Model Result Data for OTBI Reporting

**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 don't 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.
- The Security Synchronization job displays counts of users who are authorized as owners, editors, or viewers of object records, but whose eligibility to work with those records has changed. It displays distinct counts for the types of object users can be authorized to work with, such as Risk in Financial Reporting Compliance or Incident in Advanced Controls. For each object, a New count is the number of users who have become ineligible for their authorizations, and a Fixed count is the number of users whose eligibility has been restored. For a given run of the job, counts include only users whose eligibility has been lost or restored since the previous run of the job.
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 module.
- Use a Data Migration utility to export templates containing perspective data from Advanced Controls, 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. As you do, a message presents a job ID. Note the ID, then close the message. You can initiate exports from:
   - Any of the pages for managing models, advanced controls, or global conditions in the Advanced Controls work area.
   - The Data Migration page in the Setup and Administration work area.
   - The reporting work areas for Financial Reporting Compliance or Advanced Controls.
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.
3 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, for use in sorting and filtering them in lists of records.

- In the Financial Reporting Compliance module, you may assign perspective values to processes, risks, controls, and assessments.
- In the Advanced Controls 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.

In Financial Reporting Compliance, perspectives also play a part in determining how assessments are distributed to the people who work on them. For any given process, risk, or control, you can initiate duplicate assessments, one for each perspective value assigned to the object. For each of the duplicates, you can then select a distinct set of assessors, reviewers, approvers, and viewers. Each set would assess the object from the point of view of whatever interest its perspective value 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. Open the Perspectives work area. 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 map it to the types of object users can assign its values to. Until you do, the perspective hierarchy isn’t available for use.

Manage Perspective Mappings

Placing a perspective hierarchy in use is a two-phase process. First, you create the perspective hierarchy. (You use the Perspectives work area to do so.) Second, you map the hierarchy to objects. 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 Financial Reporting Compliance or Advanced Controls. Then select Edit.
3. In a new page for the component you 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, 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, you can modify the setting of the Required option as you want.
   - After operational data exists, 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.
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's 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.
4 Configuration and Administration

Overview of Risk Management Configuration and Administration

In the Risk Management Setup and Administration work area, you can set features that configure Risk Management for use and routine maintenance. Some features are common to Financial Reporting Compliance and Advanced Controls:

- You can migrate operational and perspective data.
- You can enable users to receive email alerts of tasks that require their attention. (However, even if you disable email alerts, users receive "bell notifications" of these tasks.)
- You can modify lookups, which store values displayed in Risk Management lists of values.

Other features are specific to Advanced Controls:

- Models and controls are subject to limits that improve performance by reducing the number of records involved in data-intensive operations. You can modify those limits.
- You can synchronize data. This operation updates transaction and audit data records in Advanced Controls with fresh data from your Oracle Cloud data source.
- You can manage global users. A global user ID is a single identifier that correlates to potentially varying IDs a person may have in business-application accounts.
- You can purge incidents and data sets generated by controls.

Still other features are specific to Financial Reporting Compliance:

- You can determine features available to each of the Process, Risk, and Control objects, by selecting from standard sets of features.
- You can select assessment activity types for each object, and edit guidance text and an activity question for each activity.
- You can edit responses that assessors may select as they complete assessments.

In the Cloud Setup and Maintenance work area, you can configure "segments" for Risk Management flexfields. Each segment is, in effect, a user-defined field that appears in the record of a Financial Reporting Compliance or Advanced Controls object. Collectively, they enrich object records by adding details unique to your requirements.

Data Migration

A Data Migration utility uploads operational data for Financial Reporting Compliance, or perspective data only for Advanced Controls. 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 records you’re authorized to work with as an owner or editor.
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, 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.
  - In a Perspective worksheet, name and assign type codes to your perspectives.
  - 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 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>
</tbody>
</table>
• When you finish entering data into the template, save it in the .xml file format.

### Set Email Alerts

A Notification job sends notifications to users when tasks require their attention.

- Each time the job runs, it sends "bell notifications." A user would click the bell icon in the global header to see his or her bell notifications. You don't have to do anything to set these up.

- The job may also send email alerts each time it runs, but this requires that you configure a setting in the Manage Configuration Options page of the Setup and Administration work area. Users would then receive email messages in addition to bell notifications.

### Worklists

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, worklists apply only to incident results returned by controls. For a given user, a worklist is the set of all pending incidents generated by a control for which the user is a result investigator. Records of the user's worklists appear on the Worklists page of the Results work area, regardless of whether the Notification job has run.

Each time the Notification job runs, it sends alerts concerning new pending incidents. Each recipient is informed of controls that have generated new incidents the recipient is authorized to own or edit. ("New" incidents are those generated after the last time the recipient was alerted.)

- Bell notifications are distinct: each informs its recipient of a single control that has generated at least one new incident.
- Email alerts are consolidated: each lists every control that has generated at least one new incident for which the recipient is authorized.

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. The Worklists page of the work area for each object lists the user's worklists for that object.

Risk Management sends a bell notification each time a user has a task to complete in Financial Reporting Compliance. If you enable email alerts, Risk Management sends an email message as well.
Other Notifications

Another type of 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, a notification announces the creation or edit of an advanced control the user is authorized to work with. In Financial Reporting Compliance, a notification is a record of a task that involves the recipient indirectly. For example, she may oversee the action of those who are assigned to complete the task. Again, Risk Management sends bell notifications of these events, and also sends email messages if you enable email alerts.

Notifications in Access Certification

Access Certification works somewhat differently. It doesn't generate worklists or notifications in the sense defined above. It does, however, send bell notifications to notify users of approaching or passed deadlines, or of tasks to be completed. Providing that email alerts have been enabled centrally for all Oracle Cloud applications, Access Certification always sends email alerts. Disabling email alerts at the Risk Management level has no effect on Access Certification.

Enable Email Alerts

To enable email alerts in Advanced Controls and Financial Reporting Compliance:

1. Select the Manage Configuration Options tab in the Setup and Administration work area.
2. In the Email Alerts region, select Edit.
3. Select the Enable check box, and click Save.

Use the Scheduling page to create a schedule for the Notification job. You have two options:

- Set a schedule for the Security Synchronization job. When that job runs, it also launches the Notification job.
- Set a schedule for the Notification job directly.

Or, you can run either job on demand from the Scheduling page.

Related Topics

- Predefined Risk Management Jobs

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: Open the Perspectives work area, 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.

You can’t edit predefined lookups. You can edit lookups you have created. To edit a lookup you have defined:

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.
Performance Configuration for Advanced Controls

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 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 records that change infrequently, such as setup records.

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 Advanced Controls Configurations tab in the Setup and Administration work area.
2. In the Transaction and Audit 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 you want the large data set that can be expected for your time span.
   - Enter the cutoff date for the synchronization of audit events.
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. Select Save.

Synchronize Data

To ensure transaction and audit 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 and audit 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.

| Note: | If you use Advanced Financial Controls in a test environment, and you perform a production-to-test update, you must perform a graph rebuild in the test environment. |

Select the Advanced Controls Configurations tab in the Setup and Administration work area. In its Transaction and Audit Performance Configuration region, you can view the date and time data was most recently synchronized. You can also select among these options:

- Run, 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, 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.
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. 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 separation-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. 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.

**Note:** A global user’s first-name, last-name, and email-address values typically come from that user’s Oracle person record. If a user has no person record, or if the appropriate values are missing from a user’s person record, all three values appear in Risk Management as the word “unknown” followed by the user name.

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:

- Select the Global User Configuration tab in the Setup and Administration work area.
- In the Advanced Controls work area, select the Models tab. In the Actions menu on the Models page, select Global User Configuration.
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.)

Purge Advanced Controls Results

Records of Advanced Controls 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.
- 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 Purge Results tab in the Setup and Administration work area.
2. 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.
3. Optionally enter values in these fields:
   ◦ Result Type: Select Incident or Data set. If you make no selection, you 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.
4. Click Run Now.

Set Options for Financial Reporting Compliance Objects

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.

**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 Manage Configuration Options tab.
2. In a Search Results region, expand the 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 module.
  • Select Show or Hide. Show is the default.
• 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. Hide is 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. Hide is 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 in Financial Reporting Compliance. Ultimately, each type defines what assessors are to determine as they complete assessments. You can also edit text associated with each activity.

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

1. In the Setup and Administration work area, select the Manage Configuration Options tab.
2. In a Search Results region, expand the 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.

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>
<tr>
<td>Type</td>
<td>Description</td>
<td>Available for Assessment Of</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<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>

### Edit Assessment Responses

While completing an assessment in Financial Reporting Compliance, an assessor selects a response to an assessment question. The response determines whether an object passes or fails the assessment.

To a limited extent, you can edit these responses. Each 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.

### Configure Flexfield Segments

Descriptive **flexfields** are fields your company can use to store details unique to its requirements. Risk Management provides a single descriptive flexfield for each of the Process, Risk, Control, Issue, and Assessment objects in Financial Reporting Compliance, and the Control and Incident Result objects in Advanced Controls.

Before you can use flexfields, however, your company must define "segments" for each of them. Each segment accepts a piece of information you want to record about an object. Segments appear as fields in an Additional Information region of the pages to view, create, or edit objects.

To configure segments, use the Manage Descriptive Flexfields task in the Cloud Setup and Maintenance work area. In its Module search field, search for the value "Risks and Controls Top" to produce a complete list of the Risk Management flexfields available for you to use. Then select any one of them, and select Actions > Edit to open a page in which you can add, edit, or remove segments.
For detailed information on configuring flexfield segments, see the Flexfields chapter of a guide titled Configuring and Extending Applications. Note, however, that there are three types of flexfield: key, extensive, and descriptive. Risk Management uses only descriptive flexfields. As you review information about flexfields in the Configuring and Extending Applications guide, you can ignore information about key and extensive flexfields.
**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. 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. For most business objects, this is your Oracle Cloud instance. However, an Internal data source corresponds to the Advanced Controls 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.

**flexfield**
A user-defined field consisting of segments that store details unique to your company's requirements. Of three flexfield types, only descriptive flexfields are available in Risk Management. Extensible and key flexfields aren't available.

**global user**
An identifier assigned to each user of business applications subject to models and controls created in Advanced Controls. It correlates to potentially varying identifiers each person may have for business-application accounts. Global user IDs apply only to Advanced Controls, 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.

**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, objects include models, advanced controls, and incidents. These can serve as filtering values.