

# Oracle Fusion Cloud Risk Management

---

## **Implementing Risk Management**

26A





# Contents

<b>Get Help</b>	<b>i</b>
<hr/>	
<b>1 Introduction</b>	<b>1</b>
Implementation Overview	1
Opt In to Risk Management	2
Multiple-Language Support	2
<b>2 Jobs and Scheduling</b>	<b>5</b>
Overview of Jobs	5
Predefined Jobs	5
View Job Details	6
Manage Export Jobs	8
Cancel or Purge Jobs	9
Manage Job Schedules	9
<b>3 Perspective Management</b>	<b>11</b>
Perspectives	11
Create or Edit a Perspective Hierarchy	11
Manage Perspective Mappings	12
Perspective Status	13
<b>4 Configuration and Administration</b>	<b>15</b>
Overview of Configuration and Administration	15
Configure Common Elements	15
Set Up and Maintain Data Sources	18
Configure Advanced Controls	26
Set Up Advanced Access Requests	33
Migrate Data in Financial Reporting Compliance	34
Configure Financial Reporting Compliance	37
Activate the Enhanced Worksheet for Access Certifications	39


---

<b>5 Audit</b>	<b>41</b>
Audit Objects	41
Set Up Auditing	41
Run Audit Reports	42

# Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

## Get Help in the Applications

Some application pages have help icons  to give you access to contextual help. 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. If the page has contextual help, help icons will appear.

## Get Training

Increase your knowledge of Oracle Cloud by taking courses at [Oracle University](#).

## Join Our Community

Use [Cloud Customer Connect](#) to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, suggest [ideas](#) for product enhancements, and watch events.

## Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to [oracle\\_fusion\\_applications\\_help\\_ww\\_grp@oracle.com](mailto:oracle_fusion_applications_help_ww_grp@oracle.com).

Thanks for helping us improve our user assistance!



# 1 Introduction

## Implementation Overview

Oracle Fusion Cloud Risk Management is a set of complementary applications that document and assess your company's risk-control matrix; run models and controls that detect policy violations in transactions and in access grants to users; and certify role assignments.

To begin using these applications, opt in to the Risk Management offering in Oracle Fusion Functional Setup Manager. Then set up and manage the following.

### Jobs and Scheduling

You can schedule background tasks and monitor their results. 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 existing risk and control framework. Or you may import access and transaction models created by Oracle to ensure best practices.

Predefined jobs perform key background tasks related to security, notifications, and reporting. 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 records of 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

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 varying authorization levels. For more on security configuration, see *Oracle Fusion Cloud Risk Management: Securing Risk Management*.

### Configuration and Administration

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

Some features apply generally. You can determine whether users receive notifications, email alerts, or both when tasks require their attention. You can edit the values available for selection in list-of-values fields. You can configure flexfield segments; each segment is, in effect, a field that captures information unique to your organization's requirements.

Other features apply specifically to Oracle Fusion Cloud Advanced Controls, the application that runs models and controls to detect policy violations. You can set performance options, establish a uniform currency for amount attributes in transaction analysis, and purge old control-analysis results. You can synchronize data and manage global users; these operations refresh transaction and user data analyzed by models and controls. You can establish connections to data sources other than the default Oracle Cloud data source.

Still other features apply specifically to Oracle Fusion Cloud Financial Reporting Compliance, the application that documents your risk-control matrix. You can select assessment activities available for each of the Process, Risk, and

Control objects. (For each object, you can't change these selections after you create or import object records.) You can review assessment-response definitions. You can also use a data-migration utility to upload operational and perspective data.

In Oracle Fusion Cloud Access Certifications, the application for certifying role assignments, you can activate an enhanced version of the certifier worksheet, the page in which certifiers record their judgments of whether role assignments are justified.

## Audit

You can use the Oracle Cloud audit framework to track changes to records your organization creates in Oracle Risk Management. Most, but not all, auditable records apply to Oracle Advanced Controls.

## Opt In to Risk Management

To begin, opt in to Risk Management. To do so, you must have the Application Implementation Consultant job role.

1. Click Navigator > My Enterprise > Offerings.
2. In the Offerings page, scroll to the Risk Management offering and select it.
3. Click the Opt In Features button.
4. In an Opt In: Risk Management page, select the Enable checkbox in the Risk Management row.
5. Select among "functional areas," which are available in rows beneath the Risk Management row.
  - o Ensure that two of them, Application Extensions and Users and Security, are selected.
  - o Select Recommendation Engine if you want to use the Oracle Risk and Security Snapshot Report application. (This application requires other setup steps as well. See *Set Up Risk and Security Snapshot Report*.)
  - o Don't select the Risk Management Algorithms option. It's intended for future use.
6. Click the Done button. Back in the Offerings page for Risk Management, ensure that the Status field reads Enabled.

For more information on using the Offerings pages, see the "Offering Configuration" chapter in the Using Functional Setup Manager guide.

Also, add your Risk Management subscription to your environment family in Oracle Cloud Console. (See *Managing Environment Families*.)

## Multiple-Language Support

Oracle Fusion Cloud 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 transaction models, and the 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 to work 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 Fusion Cloud. Another way is to navigate to Settings and Actions > Set Preferences > Language. 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. But 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.
- Henri 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.



## 2 Jobs and Scheduling

### Overview of Jobs

Jobs are requests to perform background tasks like synchronizing data, evaluating models or controls, exporting results, or generating reports. You run or schedule a job on the page it applies to, but 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 Done icon to return to the page you started from.

### Predefined 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 for, 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 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 Security Synchronization** updates worklists in Oracle Fusion Cloud Advanced Controls to match current security definitions.
- **Result Summary Update** prepares access-control-incident data for presentation in the Results by Control and User page and the Results by Control, User, and Role page.
- Each of three notification jobs applies to the product included in its name: Advanced Controls Notifications, Financial Reporting Compliance Notifications, and Access Certification Notifications. These jobs may send notifications, email alerts, or both to users when tasks require their attention. (For each object to which notices apply, you can turn each type of notice on or off. To do that, use a Settings for Email Alerts and Notifications page, located in the Setup and Administration work area. See [Activate Alerts](#).)
- **Report Synchronization:** This job updates data in subject areas that support analyses run in Oracle Transaction Business Intelligence (OTBI). It handles Oracle Fusion Cloud Financial Reporting Compliance data, as well as Oracle Advanced Controls data concerning access and transaction controls and their results.

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. (See [Manage Job Schedules](#).)

- 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 worklist-synchronization, result-update, and notification 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.
- 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 two subject areas, Advanced Access Models Real Time and Advanced Financial Models Real Time, use a distinct synchronization job that must be run manually. (See [Synchronize Model Result Data for OTBI Reporting](#).)

One more predefined job, Access Certification Synchronization, performs background tasks that support Oracle Fusion Cloud Access Certifications. These include:

- Ensure the validity of owner assignments to certifications. If any is invalid, replace it with an All Eligible Owners value.
- 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're not expected to modify this schedule.

Two more predefined jobs support Advanced Access Requests, in which users may request role assignments, or review or approve those requests. Both jobs are scheduled by default to run daily. Although that's recommended, you can use the Scheduling page to modify the schedules.

- Advanced Access Request Analysis runs all active access controls to uncover violations in all requests that have accumulated since the job's previous run.

Schedule the Global User Synchronization job to run before the Advanced Access Request Analysis job. It ensures that new users are correctly accounted for in access requests. (See [Configure Global Users](#).)

- Access Request Notifications sends email alerts if you've activated them in the Settings for Email Alerts and Notifications page.

## View Job Details

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

Typically a job's status is updated 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 then to Canceled when the application completes the operation.

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

- The completed-with-errors status applies when a job evaluates multiple controls, and some run successfully but others fail. For access controls, the Messages panel in the record of the job run reports the controls that have failed and invalid access points in those controls.

- The completed-with-warnings 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: job ID, name, status, type, and submission date, as well as the user who's run the job.
- Sort the list of jobs by start date (the default), job ID number, name, or submission date. Select any 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. It doesn't appear for jobs at any status other than Started.
- Refresh the content of the page. You can click a refresh icon, or select an Auto refresh checkbox to cause the page to refresh automatically every 10 seconds.

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.
- The Transaction Data Source Synchronization job displays new, updated, and total values for each business object affected by the job. Or, if there were no new or updated records, it displays a message saying so. When updates do occur, the job also returns counts of underlying associations among business objects. You can drill into details of a data-synchronization job while it's running. That lets you see whether any data has been synchronized for each business object, and the status and record counts for each at any given moment.

This job also provides a report in XLSX format. In the report, a Record Counts tab gives the counts of synchronized records for each business object. A Messages tab documents warnings and errors; it also identifies business objects and attributes that are used in audit models or controls, but are not enabled for auditing. To view the report, click the download icon in the record of the job run.

- 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 job to import user-defined business objects displays new, updated, and total 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, click the status to open a child Summary page that presents record counts or messages.

If an incident control 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 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, and 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. For each object, a New count is the number of users who have become ineligible for their authorizations. 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.

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 export:
  - Models, advanced controls, or global conditions from the pages to manage them in Oracle Fusion Cloud Advanced Controls. Export files are in JSON format.
  - Results returned by models or advanced controls, from the pages that display those results. Export files are in XLSX format.
  - Files to create imported business objects, from the Select Business Objects page opened from the page to create a transaction model. (You would export these files to edit the objects.) Export files are in XML format.
  - Templates containing data from Oracle Fusion Cloud Financial Reporting compliance, for use by its Data Migration Utility. Export files are in XML format.
  - Reports from either application, from the Advanced Controls Reports or Financial Compliance Reports work area. Export files are in XLSX or PDF format.
  - User Assignment Groups, from the Risk Management Data Security work area. Export files are in JSON format.
2. In the Monitor Jobs page, locate the row displaying the job ID you noted. When its status is Completed, click the download icon.
3. A file-download window opens. In it, navigate to the folder in which you want to save the file and click the Save button.

## Cancel or Purge Jobs

You can cancel any job you've run or scheduled. Generally, you can't cancel other users' jobs, but there are exceptions: Anyone can cancel a job to synchronize transaction data, analyze models, or analyze controls, no matter who ran the job.

**Note:** There's a special case: If you're assigned the ESS Administrator role, you can cancel any job run by anyone.

You can also purge job records. To complete either a cancellation or a purge:

1. In the Monitor Jobs page, identify the jobs you want to cancel or purge. To be canceled, jobs must be at the Queued or Started status. To be purged, jobs must be at the Completed, Failed, or Canceled status. Click the check boxes in the rows for the jobs you've identified.
2. Click the Cancel button or the Purge button, whichever is appropriate for the jobs you've checked.
3. Respond to a message that asks you to confirm the cancellation or purge.

When you cancel a job, its status changes first to Cancel Requested, and then to Canceled when the application completes the operation. When you purge a job, its record disappears from the Monitor Jobs page.

## Manage Job Schedules

Use a Scheduling page to set, modify, or discontinue schedules on which jobs run.

- Some jobs are listed by default in the Scheduling page. In general, these are jobs that apply broadly, such as those related to security synchronization, notifications, or transaction data synchronization. You can create schedules for these jobs in the Scheduling page.
- In other cases, you create a schedule in the page that a job applies to. For example, you set a schedule to run advanced controls from the Controls page of the Advanced Controls work area. Once the schedule for one of these jobs is set, a record of it appears in the Scheduling page, where you can review or work with it.

No matter whether you're setting or changing a schedule:

1. Select the Scheduling tab in the Setup and Administration work area.
2. Select the row that represents a schedule, then click the Edit icon.
3. In a Schedule Parameters dialog box, do either of the following:
  - Enter values that determine when the schedule starts, how regularly the job runs, and when (if at all) the schedule expires. Then 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. Its row is removed from the Scheduling page if it's one of the jobs originally scheduled in another page.

**Note:** You can modify the schedules of the Security Synchronization and Report Synchronization jobs, but you can't cancel them. You're expected not to modify the schedule for the predefined Access Certification Synchronization job.

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 object records, for use in sorting and filtering them in lists of records.

- In Oracle Fusion Cloud Financial Reporting Compliance, you may assign perspective values to processes, risks, controls, and assessments.
- In Oracle Fusion Cloud Advanced Controls, you may assign perspective values to models, advanced controls, and incidents.
- You can't assign perspective values to any component of Oracle Fusion Cloud Access Certifications.

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 Oracle 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) in the General panel. 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 Hierarchy panel to create any number of perspective values. Each requires a name and a status (Active or Inactive). 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. Under Perspective Items, 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.

It's recommended that you create no more than five hierarchical levels below the root level. Although you can create values at lower levels, they would never be used. That's because you can associate object records with perspective values only down to the fifth subordinate level.

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

5. Typically as you edit a hierarchy, select any value in the Perspective Hierarchy panel to view information about it in the Item Details panel. Select tabs in this panel to view general configuration details, or to identify 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

To use a perspective hierarchy, you create it (you use the Perspectives work area to do so), then map it to objects. Until you map a hierarchy to an object, it's not available for use with instances of that object.

To perform the perspective-to-object mappings:

1. Open the Module Perspectives page. In the Setup and Administration work area, select the Module Perspectives tab.
2. Click the Financial Reporting Compliance row or the Advanced Controls row. 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.
  - If you selected the Financial Reporting Compliance row in step 2, you can map perspective hierarchies to the Process, Risk, and Control objects. If you selected the Advanced Controls row, 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 save an instance of the object only if 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 panel 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

You assign Active or Inactive status to perspective values, perspective hierarchies, and mappings of hierarchies to objects. Changes in these status values have 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 become inactive 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 panel 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 Configuration and Administration

In the Setup and Administration work area, you can set features that configure Oracle Fusion Cloud Risk Management for use and routine maintenance. Some features are common to its applications:

- You can activate or deactivate email alerts and notifications that inform users of tasks requiring their attention.
- You can modify lookups, which store values displayed in lists of values.

Other features are specific to Oracle Fusion Cloud 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.
- For certain business objects, you can set up the conversion of monetary amounts to a single currency.
- You can synchronize data. This operation updates transaction and audit data records with fresh data from your Oracle Cloud data source.
- You can purge results generated by controls.
- You're connected by default to a native Oracle Cloud data source, which provides data from Oracle Fusion ERP, SCM, HCM, and CX applications for analysis by models, controls, and access-certification campaigns. You can also connect to, or import data from, other data sources.
- 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, particularly accounts in multiple data sources.

Still other features are specific to Oracle Fusion Cloud Financial Reporting Compliance:

- You can migrate operational data.
- You can select assessment activity types for each of the Process, Risk, and Control objects. For each activity type, you can edit guidance text and an activity question.
- You can review responses that assessors may select as they complete assessments.

In Oracle Fusion Cloud Access Certifications, you can activate an enhanced version of the worksheet in which certifiers record their judgments of whether role assignments are justified.

In Oracle Fusion Functional Setup Manager, you can configure flexfield "segments." Each segment is, in effect, a user-defined field that appears in the record of an object. Collectively, they enrich object records by adding details unique to your requirements.

## Configure Common Elements

### Activate Alerts

Users may receive notifications, email alerts, or both when tasks or events require their attention.

- Notifications are available from the Notifications icon in the global header. (It looks like a bell.)

- Email alerts are messages sent to recipients' email addresses.

These notices report tasks or events concerning "objects." In most cases, an object is a class of items you can create or edit, for example Risk or Incident. Failed jobs and ineligible security assignments are also objects for which notices are sent.

By default, both types of notice are active for all objects to which notices apply. But you can deactivate or reactivate either notice type for each object individually. Having done that, you can turn either notice type off for all objects, or turn your individualized settings on again.

To modify notice activations:

1. Select the Settings for Email Alerts and Notifications tab in the Setup and Administration work area.
2. Click the Edit button.
3. In the Object-Level Settings panel, you can select settings that apply individually to objects:
  - Select one or more objects for which you want to do one of the following: activate both notice types, activate only one type or the other, or deactivate both types. (Click their checkboxes to select them.) To aid in making your selection, you can filter objects by business area (product), object, or current activation setting.
  - Expand the **Update Settings** list and select the activation value you want: **Email and notification**, **Email only**, **Notification only**, or **No email or notification**. Your selection appears in the Settings column for each object in the set.
  - As needed, select other sets of objects and, for each set, select another value from the Update Settings list.
4. In the Global Settings panel, you can select activation settings that apply to all objects:
  - Select either of the **Suppress emails** or **Suppress notifications** checkboxes to prevent its type of notice from being sent. Or select both to stop any notices from being sent.
  - Clear either checkbox to resume sending its type of notice. Or clear both.

When selected, the Suppress options override, but don't change, the settings that apply to individual objects in the Object-Level Settings panel.

5. Click the Save button.

Predefined jobs run to determine when alerts and notifications are sent. You can modify their default schedules. For more on this, see [Manage Job Schedules](#).

## Manage Lookups

Lists of values in Oracle Fusion Cloud 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 Lookups page: Select the Lookups tab in the Setup and Administration work area.
3. Click Show Filters. In the Meaning field of the Filters panel, enter the value you noted. Click Search. The Lookups page then includes 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:

Page	Lookup Type
Create Process or Edit Process	GRCM_PROCESS_TYPE
Create Risk or Edit Risk	GRCM_RISK_TYPE
Create Control or Edit Control	GRCM_CONTROL_TYPE
Create Issue or Edit Issue	GRCM_ISSUE_TYPE

## Create and Edit Lookups

To create a lookup:

1. In the Lookups page, click the Create Lookup icon. A Create Lookup page opens.
2. In the Lookup Type field, enter the lookup-type value you've 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. The combination of lookup code and meaning must be unique.
5. In the Status field, accept the default value, Active, or select Inactive.
6. Optionally, describe the lookup in the Description field.
7. Select Save and Close.

You can't edit predefined lookups. You can edit lookups you've created. To edit a lookup you've defined:

1. In the Lookups page, search for the lookup you want to edit: Filter for any combination of type, meaning, description, and status values, and click the Search button.
2. Click the row for the lookup you want to edit, then click the Edit Lookup icon.
3. An Edit Lookup page opens. Modify any of the status, meaning, and description values. (The lookup type and lookup code are presented as read-only values; you can't edit them.)

4. Select Save and Close.

## Configure Flexfield Segments

Your company can use descriptive flexfields to store details unique to its requirements. One flexfield applies to each object; you define "segments" of each object's flexfield to capture discrete values.

In Oracle Fusion Cloud Financial Reporting Compliance, a flexfield is available for each of the Process, Risk, Analysis, Evaluation, Treatment Plan, Event, Consequence, Control, Issue, Remediation Plan, and Assessment objects. In Oracle Fusion Cloud Advanced Controls, a flexfield is available for each of the Control and Incident Result objects.

For each object's flexfield, you can create up to 40 text-string segments, 20 numeric segments, and 10 date segments, for a total of 70 segments. Each segment accepts a piece of information you want to record about an object. Segments appear as fields in an Additional Information panel of the pages to view, create, or edit objects.

You can create global or context segments. Broadly, a global segment is a piece of information that becomes part of an object record under any circumstance. A context segment is a piece of information that applies only under circumstances you define as you configure the flexfield.

To define segments, use the Manage Descriptive Flexfields task in Oracle Fusion Functional Setup Manager. In its Module search field, search for the value "Risks and Controls Top." From the resulting list of flexfields, select one, and select Actions > Edit to open a page in which you can add, edit, or remove segments.

For detailed information on defining flexfield segments, see the Flexfields chapter of Oracle Fusion Cloud Applications: Configuring and Extending Applications. But note: Although there are three types of flexfield, Risk Management uses only one of them, descriptive. As you read about flexfields, ignore information about two other types, key and extensive.

## Set Up and Maintain Data Sources

### Overview of Data Sources

Models, controls, and access certifications can analyze data from multiple data sources. Among them, an Oracle Cloud data source supplies access and transaction data from Oracle Fusion ERP, SCM, HCM, and CX applications. It's native to the Advanced Controls and Access Certifications applications, so you don't have to do anything to set it up.

You can also analyze data from the following "synchronized" data sources, but to do so you must set up connections to them.

- An EPM-ARCS data source provides access and transaction data from Oracle Enterprise Performance Management Account Reconciliation.
- Up to three EPM-FCCS data sources provide access and transaction data from "pods" in Oracle Enterprise Performance Financial Consolidation and Close.
- An OCI data source supplies access data from Oracle Cloud Infrastructure.

Each synchronized data source has its own setup procedure. Once data sources are set up, you can schedule jobs that refresh the data they provide and you can perform other maintenance tasks.

You can also import role-assignment data for analysis by access models and controls. The imports are from applications, such as Workday and Salesforce, that aren't among the synchronized data sources to which you can set up connections.

## Prerequisites for Data Sources

You may need to complete some preparatory steps to activate data sources or to enable the import of role-assignment data.

To set up a connection to an EPM-ARCS, EPM-FCCS, or OCI data source:

- If you haven't done so already, activate permission groups for the Risk Administrator, Advanced Access Controls Analyst, and Access Certification Administrator predefined roles, and for related custom roles if you have any. See the *Required Security Update* topic.
- The Advanced Controls Administrator duty role requires two privileges that support synchronized data sources. They're already added to the predefined role, but if you use a custom version of this role, you need to add the privileges to your version. The privileges are:
  - Manage Additional Advanced Control Data Sources (GTG\_MANAGE\_ADDITIONAL\_RISK\_MANAGEMENT\_DATA\_SOURCES\_PRIV)
  - View Additional Advanced Control Data Sources (GTG\_VIEW\_ADDITIONAL\_RISK\_MANAGEMENT\_DATA\_SOURCES\_PRIV)

See the *Copy or Edit Risk Management Roles in the Security Console* topic.

Two privileges are required for users to import role-assignment data, but they're not included in any predefined role. So you need to add the privileges to a custom role and assign it to appropriate users. The privileges are:

- Export Access Point Data (GTG\_EXPORT\_ACCESS\_POINT\_DATA\_PRIV)
- Import Access Point Data (GTG\_IMPORT\_ACCESS\_POINT\_DATA\_PRIV)

The custom role can be a job role based on a copy of the predefined Advanced Access Controls Analyst role. Or it can be a duty role based on a copy of the predefined Advanced Controls Administrator duty role, and added to the role hierarchies of custom job roles.

## Set Up EPM Data Sources

If you want Risk Management to evaluate data from EPM Account Reconciliation, you must set up an EPM-ARCS data source. If you want Risk Management to evaluate data from up to three EPM Financial Consolidation and Close pods, you need to set up a distinct EPM-FCCS data source for each of them. Setup involves establishing a connection to an EPM server and running synchronization jobs that refresh EPM data in Risk Management.

One step in connecting to an EPM server is to provide authentication details, and those details depend on which of two authentication protocols you use. Each applies to an EPM instance deployed as a cloud service in Oracle Cloud Infrastructure (OCI); on-premises deployments aren't supported.

- An Open Authorization 2.0 (OAuth2) protocol is recommended for production, but you can use it only if your EPM deployment integrates EPM with Oracle Identity Cloud Service (IDCS).
- A basic authorization protocol is required for a "classic" EPM deployment (one without IDCS integration). Even if your EPM deployment qualifies for the OAuth2 protocol, you may use the basic protocol instead.

In either case, you'll use a setup page to provide authentication details for the data source. Before you begin the setup procedure, you should determine what these values are. You may need to consult with your EPM system administrator.

If you use the basic protocol, authentication details include the following four values:

- **API Credentials > User Name:** The name for a user account in the data source you're setting up, either EPM-ARCS or an EPM-FCCS pod. This user must have the Service Administrator role. Risk Management uses this account to connect to EPM to fetch data for analysis.
- **API Credentials > Secret Key:** The password paired to the User Name. This password may be subject to expiration. If so, update it when it expires, then rerun the setup procedure, entering the new password value as you do.
- **Authorization > Protocol Type:** The correct protocol type is **Basic authentication**.
- **Authorization > Host:** The https URL of the server for the data source you're setting up, either EPM-ARCS or an EPM-FCCS pod.

If you use the OAuth2 protocol, provide the following values.

- **API Credentials > API Key:** The client ID for the REST client application registered in the IDCS system.
- **Authorization > Protocol Type:** The correct protocol type is **Open authorization 2.0**. It's the default value.
- **Authorization > Authorization Scope:** The authorization scope for the EPM instance.
- **Authorization > Host:** The https URL of the server for the data source you're setting up, either EPM-ARCS or an EPM-FCCS pod.
- **Authorization > Token URL:** The token URL for the IDCS instance paired with the EPM-ARCS instance or EPM-FCCS pod you're setting up. For IDCS this value is the base URL, with the following value added: **/oauth2/v1/token**
- **Authorization > Grant Type:** The correct grant type is **JWTAssertion**. It's the default value.
- Ignore any other fields in the API Credentials and Authorization sections of the setup page.

If you use the OAuth2 protocol, you must also use an Assertion section of the setup page to specify two values, a Client Assertion and a User Assertion. You can, but typically shouldn't, supply these assertion values directly. Instead, you can supply values in the following five fields, from which the application generates the assertions.

- **Assertion > User Name:** The name for a user account in the data source you're setting up, either EPM-ARCS or an EPM-FCCS pod. This user must have the Service Administrator role. Risk Management uses this account to connect to EPM to fetch data for analysis.
- **Assertion > Key Alias:** The alias for the public certificate imported into IDCS.
- **Assertion > Audience List:** The audience list value for generating OAuth2 assertions. For IDCS this value is **https://identity.oraclecloud.com/**
- **Assertion > Public Certificate:** The public certificate value imported into IDCS for validating OAuth2 assertions. (You can import this value. See step 3 below.)
- **Assertion > Private Key:** The private key value for generating OAuth2 assertions. (You can import this value. See step 3 below.)

More about these assertions:

- The application saves the two assertion values, but not the other values, in the Fusion credential store. The assertion values eventually expire. By default, they remain in force for one year. To create new assertions, you would rerun the setup procedure, and would reenter all of the required values to do so. The application doesn't save them because they're considered to be sensitive data.
- You would supply the assertion values directly, in **Client Assertion** and **User Assertion** fields, only if you want to change the default behavior of the assertions, for example by designating a shorter time until expiration. But

you would have to create them. You can use a tool called OpenSSL to do so. However, this would require you to have an in-depth understanding of OpenSSL and assertions.

- If you supply the two assertions, leave the other five fields blank. If you supply values in the other five fields, leave the two assertion fields blank.

Complete these steps to set up an EPM-ARCS or EPM-FCCS data source:

1. Navigate to Risk Management > Setup and Administration > Advanced Controls Configuration.
2. In the **Non-Fusion Data Sources** panel, locate the row for the EPM-ARCS data source, or one of three rows (numbered 1 through 3) for EPM-FCCS pods. Initially, each of these rows displays a **Not set up** sync status. Click the **Edit Credentials** icon.
3. An Enter Authentication Details page opens. In it, the **Authorization > Protocol Type** field defaults to the value **Open authorization 2.0**. Accept that value if you use the OAuth2 protocol; if not, select **Basic authentication**. The page presents fields appropriate for the protocol you've selected. In either case, enter the authentication details you've determined are correct for the data source you're setting up.

If you've selected the OAuth2 protocol, you have options about how to provide the Public Certificate and Private Key values.

- You can enter them manually.
  - You can import them, one at a time. Click the **Upload** button above the field for either value. In a file-upload dialog, navigate to the corresponding file your organization has generated for the X509 public certificate or private key, and upload the file. Then repeat for the other value. The application reads the content of each file, performs the necessary formatting, and inserts the value in the Enter Authentication Details page.
4. Click the **Test Connection** button. When a message confirms that your authentication details are valid, click the **Update** button.
  5. The focus returns to the Advanced Controls Configuration page. In the row for the data source you're setting up, there are now two sync-status fields, one for access analysis and the other for transaction analysis. The value of each is **Not started**.

In that row, expand the **Actions** menu. In it, select the **Run Access Sync** option to prepare for access analysis, or the **Run Transaction Sync** option to prepare for transaction analysis.

6. A message displays a job number. Make a note of the number and close the message. Click the **Go back** icon and, in the **Monitor Jobs** page, locate the row for your job number to track the progress of the job.
7. When the job has finished running, click the Advanced Controls Configuration tab. In the row for the data source you're setting up, the sync-status value for the job you ran is now **Completed**.
8. You can stop at this point. If you intend to perform both access and transaction analysis, however, you need to run the second synchronization job. To do so, repeat steps 5 to 7, but select the Actions menu option for the job you haven't yet run.

Two fields in the data-source row show the most recent dates on which access synchronization succeeded and was attempted. Two more fields provide the same information for transaction synchronization. (For each sync job, the successful and attempted dates are initially the same, but they may differ if a later job run results in errors.)

**Note:** For optimal performance, transaction-data synchronization operates on EPM records created or updated on or after a cutoff date. It's the same as the cutoff date for transaction synchronization in the Oracle Cloud data source, which is set in the **Transaction and Audit Performance Configuration** panel of the Advanced Controls Configuration page.

## Set Up the OCI Data Source

You must set up an OCI data source if you want Risk Management to evaluate access data from Oracle Cloud Infrastructure. Setup involves establishing a connection to an OCI server and running a synchronization job that refreshes OCI data in Risk Management.

One step in connecting to an OCI server is to use a setup page to provide authentication-detail values specific to your organization. Before you begin the setup procedure, you should determine what these values are. They include:

- **API Credentials > API Key:** The client ID set up for an OAuth2 client in an Oracle Identity Cloud Service (IDCS) instance integrated with the OCI deployment.
- **API Credentials > Secret Key:** The secret key paired with the client ID for the OAuth2 client in IDCS.
- **Authorization Protocol Type:** The correct protocol type is **Open authorization 2.0**. It's the default value and can't be changed.
- **Authorization > Authorization Scope:** The authorization scope for the OCI instance.
- **Authorization > Token URL:** The https URL of the OCI server, with the following value added: **/oauth2/v1/token**
- **Authorization > Grant Type:** The correct grant type is **client\_credentials**. It's the default value and can't be changed.
- **Authorization > Host:** The https URL of the OCI server, with the following value added: **/admin/v1**
- Ignore any other fields in the API Credentials and Authorization sections of the setup page.

Complete the following steps to set up the OCI data source for which you want to perform Risk Management analysis.

1. Navigate to Risk Management > Setup and Administration > Advanced Controls Configuration.
2. In the **Non-Fusion data sources** panel, locate the row for the OCI data source. Initially, it displays a **Not set up** sync status. Click the **Edit Credentials** icon.
3. An Enter Authorization Details page opens. In it, the **Authorization > Protocol Type** field defaults to the value **Open authorization 2.0**. Accept that value and enter the authentication details you've determined are correct for your OCI data source.
4. Click the **Test Connection** button. When a message confirms that your authentication details are valid, click the Update button.
5. The focus returns to the Advanced Controls Configuration page. In the row for the OCI data source, the sync-status field now reads **Not started**. In that row, expand the **Actions** menu. In it, select the **Run Access Sync** option.
6. A message displays a job number. Make a note of the number and close the message. Click the **Go back** icon and, in the **Monitor Jobs** page, locate the row for your job number to track the progress of the job.
7. When the job has finished running, click the **Advanced Controls Configuration** tab. In the OCI row, the sync-status value for the job you ran is now **Completed**.

Two fields in the OCI row show when access synchronization succeeded and was attempted most recently. (The successful and attempted dates are initially the same, but they may differ if a later job run results in errors.)

## Maintain Synchronized Data Sources

You can determine which data source provides default business objects in the page to create access models. You can also schedule synchronization jobs and set other data-source options. To take these actions, navigate to Setup and Administration > Advanced Controls Configuration.

### Select Default Access Business Objects

In Advanced Controls, an access model consists of filters. They select users assigned one or more roles whose authorizations create a potential for fraud or significant error. Each filter designates a business object, which provides data to be evaluated by the filter. Each data source has its own set of three business objects for access analysis, and the objects for one of these data sources are available by default in the page to create an access model. To use business objects from another data source, a user would need to select them while creating models.

Initially, the Oracle Cloud business objects are the defaults. But the objects for any other data source you've set up can be designated as the defaults. If you select the objects for another data source, you can change back to the Oracle Cloud objects.

1. In the **Default access business objects** panel of the Advanced Controls Configuration page, click the **Edit default access business objects** icon.
2. Expand the **Default from** list. It displays entries for the Oracle Cloud data source and any other data sources set up in your environment. Select the one you want.
3. Click **Save**.

### Schedule Synchronization

You're expected to run the sync jobs regularly.

- For each of the EPM-ARCS and EPM-FCCS data sources, two distinct sync jobs update access and transaction data, capturing role assignments to new users, changes in role assignments to new users, and new transactions.
- The OCI data source doesn't support transaction analysis, so for it, a single sync job captures new and changed role assignments.

You can schedule these jobs to run automatically. The recommended frequency is once per day.

1. In the **Non-Fusion data sources** panel of the Advanced Controls Configuration page, expand the **Actions** menu in the row for a data source.
2. In the Actions menu, click the **Schedule Access Sync** or **Schedule Transaction Sync** option if you're working with an EPM data source, or only the **Schedule Access Sync** option if you're working with the OCI data source.
3. Enter values that set the name of the schedule, its start date and time, the intervals at which the job should run, and an end date (if any).
4. Click **Save**.
5. For any of the EPM data sources, if you've set up both access and transaction analysis, repeat these steps, but select the menu option for the schedule you haven't yet set.

You can instead click the **Run Access Sync** option or (for the EPM data sources) the **Run Transaction Sync** option in the Actions menu. This runs the sync job you select immediately, but doesn't affect the schedule if you've set one. The job runs again when its schedule next determines that it should.

## Set Other Data Source Options

From the Actions menu you open in the row for a data source, you can also complete these actions:

- Change the name of the data source. Click the **Edit Non-Fusion data sources** option. The row expands, and the **Data Source Name** field becomes editable. Enter a new name, then click the **Save** button.
- Inactivate the data source, or reactivate it. Click the **Edit Non-Fusion data sources** option; in the expanded row, an **Active** check box is present. Clear it to deactivate the data source, or select it to reactivate the data source. Then click the **Save** button.

Note, though, that before you inactivate a data source, you must first delete all models, controls, result records, and other objects that use data from the data source. (These other objects include, for example, entitlements and global conditions.)

Note also that near the top of the **Non-Fusion data sources** panel, you can click an **Active** button to display the rows for data sources that are active or have not yet been set up. You can click an **Inactive** button to display the rows for data sources that were inactivated after having been set up.

- Edit or view authorization details:

Click the **Edit Credentials** option to open a version of the Enter Authorization Details page in which fields are editable. Modify your setup configuration, then click **Update** to save changes and exit the page. After making changes, run the sync jobs.

Be aware, though, that you can't change some settings. For an EPM data source, for instance, you can't edit the Host value.

Click the **View Credentials** menu option to open a read-only version of the page, view your setup configuration, and click **Cancel** to exit the page.

- Click the **Refresh** option to update the row with the most recent values.

## Import Role-Assignment Data

You can import role-assignment data for analysis by access models and controls, and by access certifications. The imports are from applications, such as Workday and Salesforce, that aren't among the synchronized data sources to which you can set up connections. Data from these applications form a data source called **Imported**.

One way to import (or update) access data is via import files. (A second way to import data is via a REST API.) To use import files, complete three tasks:

- Export a template from Advanced Controls. The template is an Excel worksheet. For the first import, the template is blank. For subsequent imports, the template contains data from the previous import.
- For your first import, enter records of role assignments in applications you want models and controls to analyze. For subsequent imports, edit the existing records, typically by adding or removing role-assignment records.
- Import the template back into Advanced Controls.

## Export the Template

You export the template from a Select Business Objects page, which becomes available when you're in the process of creating or editing an access model. Although you download the template in the context of a specific model, other models may analyze the data you'll use the template to import.

1. Navigate to Risk Management > Advanced Controls > Models. Then do either of the following:
  - Select Actions > Create Access Model. In the Create Access Model page, enter a name for the model.
  - Select the record of an access model, then select Actions > Edit.
2. Click Add in the Model Objects panel of the create- or edit-model page. The Select Business Objects page opens.
3. Click the Export Access Data icon in the Select Business Objects page. A message presents a job ID. Note the ID, then close the message.
4. Click the Monitor Jobs button. In the Monitor Jobs page, locate the row displaying the job ID you noted. Monitor the job status until it reaches Completed.
5. Once the job is complete, click a file-download icon that appears in the job's row. In a distinct save-as dialog, navigate to the folder in which you want to save the template, and click Save.
6. Click Back in the Monitor Jobs page to return to the Select Business Objects page. If your only intention was to export the data template, click the Back icon to return to the create- or edit-model page, then click the Cancel button. You may instead finish work on a model you're creating or editing.

## Populate the Template

The template is an Excel worksheet in which each row is a record of the assignment of a role to a user in an application. It may include records of assignments in any number of applications.

Each record must include the following required values:

- User Name: The name with which the user logs on to an application.
- First Name: The user's given name.
- Last Name: The user's surname.
- Email: The user's email address.
- Access Point ID: The internal name for a role assigned to the user.
- Access Point Name: The display name for the role identified by the Access Point ID.
- Access Point Type: The only valid value is **Role**.
- Application Name: The name of the application in which the role exists. Be sure to adopt a consistent name value for each application.

Each record may also include these optional values:

- Access Point Description: A description of the access the role provides.
- Business Process: The name of a business process in which a user assigned the role would work.

Each time you import data, you replace all data from the previous import. So as you edit an import template, be sure to retain all records containing data you don't want to change.

## Import the Template

Once the template is updated, you use the Select Business Objects page to import it.

1. Open the page: Repeat steps 1 and 2 in the **Export the Template** procedure. This time, click the Import Access Data icon.
2. An Import Access Data dialog opens. Click its Browse button. Navigate to your edited template file, and select it. The File field of the Import Access Data dialog then displays the file name.
3. Click the OK button. Once again, a message presents a job ID. Note the ID, then close the message.
4. As before, click the Monitor Jobs button to track the progress of the job in the Monitor Jobs page. When it's complete, click Back to return to the Select Business Objects page. There you can either cancel or continue working on the model you opened to get to the Select Business Objects page.

## Configure Advanced Controls

### Optimize Performance

You may modify settings that improve performance in the Oracle Cloud data source by reducing the number of records involved in data-intensive operations.

#### 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. If the result set includes one record of a user with an access conflict, it must include all records involving that user. So when the result set reaches its nominal limit, analysis may continue until records are complete for all users already included in the return set. However, the model-analysis job adds no records for users not already included in the result set.

On the other hand, model results may fall short of the limit. This can happen if global users are configured so 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

Each business object used in a transaction model or control belongs to a category. A Transaction object contains records that pertain to actual transactions, which are created or updated frequently and in large volume. Objects in Operational Master Data and Configuration Setup Data categories contain 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 Master Data or Configuration Setup Data 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 close automatically if they're related to records no longer subject to synchronization after you reset the cutoff date.

## Audit Performance Configuration

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. Data-synchronization runs include audit business objects 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 Configuration tab in the Setup and Administration work area.
2. In the **Transaction and Audit Performance Configuration** panel:
  - o Click the **Actions** menu. Then select its **Edit Transaction and Audit Performance Configuration** option.
  - o Enter or modify the cutoff date that applies to transaction data, audit events, or both.
  - o Click the **Save** button.
3. In the **Access Performance Configuration** panel:
  - o Click the **Edit Access Performance Configuration** icon.
  - o The **Result Record Limit per Model** field displays the value 5,000 by default. Accept that value or enter a smaller number. The value can't exceed 5,000.
  - o By default an **Allow override at the access model level** option is turned off. This prevents users from overriding the record limit. Click its toggle switch to turn it on, enabling users to see all possible results from the models they run. You can click it again to turn it back off.
  - o Click the **Save** button.

## Set Up Currency Conversion

If your organization transacts in multiple currencies, your Oracle Cloud transaction models, controls, and results can use amounts converted to a single currency. You select the currency to which other currencies are to be converted, as well as a conversion rate.

This currency-conversion feature is disabled by default. Enable it only if at least one transaction model or control uses a currency-conversion attribute, either in a risk-logic filter or a result-attribute selection. The business objects that offer these attributes are identified in a Business Objects Supporting Currency Conversion field as you enable the conversion feature.

Each of these business objects includes pairs of attributes that report monetary values. In each pair, the first attribute reports an original value, and the second reports the value to which the first is converted. The attributes in a pair have identical names, except that the second one contains the word "Converted." For example, Amount and Amount

Converted constitute one of the pairs in the Payables Invoice business object. Each business object also includes a Conversion Currency attribute, which identifies the currency to which amounts or prices are converted.

To set up the currency-conversion feature:

1. Select the Advanced Controls Configuration tab in the Setup and Administration work area.
2. In the Currency Configuration panel, click the **Edit Currency Conversion** icon.
3. Click the **Currency Conversion** toggle switch to turn conversion on.
4. In a **To Currency** field, select the currency to which you want other currencies to be converted. US Dollar is the default. You can type in the field to search for matching currencies.
5. In a **Rate Type** field, select the exchange rate you want to use. You can select among values that are enabled in the Rate Types page of the Currency Rates Manager. The default is the value selected as default in the Rate Types page.  
(The Currency Rates Manager is available at My Enterprise > Setup and Maintenance. Search for the Manage Conversion Rate Types task.)
6. Select **Save**.

If you want to disable currency conversion, click the Currency Conversion toggle switch once again. However, you must first delete models and controls that use the currency-conversion attributes.

## Schedule or Run Data Synchronization

To ensure transaction and audit models and controls evaluate current data, run the Transaction Data Source Synchronization job. It's a process that uploads data from your Oracle Cloud data source. If you set up currency conversion, the job also calculates currency conversions. (The job doesn't update data for sources other than Oracle Cloud; those data sources have their own sync jobs.)

You can run a standard synchronization or a graph rebuild. Before you can do either, however, you must synchronize global users at least once. (See [Configure Global Users](#).)

- 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 recreates the Risk Management graph. This is a mathematical construct that describes relationships between attributes of your setup and transaction records. It's used to accelerate transaction model and control analyses. A graph rebuild recreates the graph from scratch, based on current data in your applications. It doesn't change your models or controls. It doesn't change your incidents, except in the way a standard synchronization would: it updates the status of incidents that refer to application setups or transactions that have changed from the previous synchronization.

A graph rebuild usually takes longer than a standard synchronization, because the latter updates the graph, rather than rebuilding it from scratch. Moreover, a graph rebuild is rarely needed. As a result, it's recommended that you rebuild the graph only when Oracle directs you to do so.

**Note:** If you run transaction models and 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 Configuration tab in the Setup and Administration work area. In the Advanced Controls Configuration page, a **Transaction and Audit Performance Configuration** panel displays the date and time of the most recent data synchronization. In this panel, expand the **Actions** menu to 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 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.

You have two other options for running a standard synchronization:

- Select the Run Transaction Synchronization quick action from the Risk Management springboard. (Depending on the number of quick actions available to you, you may need to select a Show More option on the springboard.)
- Run or schedule the Transaction Data Source Synchronization job from the Scheduling page of the Setup and Administration work area, where it's also listed.

#### *Related Topics*

- [Synchronize Transaction Data](#)

## Global Users

A global user ID is assigned to each person who uses business applications subject to models and controls. An individual's global user ID correlates to potentially varying IDs that person may have for business-application accounts.

The global user ID ensures that each person is recognized properly by access models and controls, and by transaction models and controls that incorporate the User business object. In particular, the global-user ID serves as a single identifier for each user who has accounts in multiple data sources. For another example, the global user ID would serve as a single identifier for an individual who marries, then changes her surname.

You determine how to formulate global users. To do so, you select one or more attributes that can identify users uniquely. For example, the default attribute is Email. In an environment in which each user has a single, distinct email address, you might use only that attribute.

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

- **Global user:** The last record with identifying-attribute values that apply to a given person. The user name for this record serves 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 as the word "unknown" followed by the user name.

## Configure Global Users

You can select the attributes that define 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, use either of two paths to 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 or more identifying attributes that define users uniquely in your environment. The Email attribute is selected by default. If you want to use that attribute and no other, you don't need to select attributes. (You do, however, need to run or schedule the synchronization job.)

If you use two or more attributes, they have an AND relationship. 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.

In addition to Email, attributes include First Name, Last Name, and User Name. Select identifying attributes whose values are most likely to be distinguishing and least likely to change over time in your environment.

To select attributes:

1. In the Identifying Attributes panel, 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. As needed, remove attributes: select them in the Selected field and click the Remove Selected Items button to move them to the Available field.
4. 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'd subsequently need to rerun models and controls to replace model results and control incidents.

## Run or Schedule the Synchronization Job

Once you've 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.
- You can also schedule the job, or run it on demand, from the Scheduling page: Select the Scheduling tab in the Setup and Administration work area.

**Note:** A job called Advanced Access Request Analysis supports Advanced Access Requests, a self-service workflow for requesting and assigning ERP roles. If you use that feature, schedule the Global Synchronization job to run before the Advanced Access Request Analysis job. This ensures that new users are correctly accounted for in access requests.

## Review Global Users and Related Users

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

Suppose, for example, you were to select Email 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.
- In a Count column, view the number of data sources in which each user has business-application accounts. You can select a **Show users with count value greater than one** checkbox to filter the list so that it shows only users active in multiple data sources.
- In a Data Source column, view the name of the data source in which each user has business-application accounts. If the Count value is greater than one, the Data Source value is **Multiple**.
- When a Count value is greater than one, click it to open a Related Global Users page. It displays the global-user record and related-user records for the person whose Count value has been selected, and it identifies the data source for each record.

## Purge Advanced-Control Results

Records of incident or data set results generated by advanced controls remain even after they're used. You can purge results generated before a date that you specify. However, you must be an owner of a control to purge its results.

## 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.
- 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, Control Inactive, Assigned, Accepted, Remediate, and Resolved.
  - Control Name: Select one or more controls whose results are to be purged. The list of controls you can choose from is filtered by the control type and, if any, the result type you selected.

4. Click Run Now.

## Set Up Advanced Access Requests

### Modify Security for Advanced Access Requests

Advanced Access Requests implements a self-service workflow for requesting and assigning ERP roles. For a majority of users to make requests, you need to edit and assign a custom job role.

A user assigned a predefined job role called Access Request Security Administrator (ORA\_GTG\_ACCESS\_REQUEST\_SECURITY\_ADMINISTRATOR\_JOB) has full rights to request roles and to review or approve role requests. However, very few users would be request approvers.

On the other hand, virtually any user might request a role, or be selected to review a role request. A duty role called Access Provisioning Requests and Review (ORA\_GTG\_ACCESS\_PROVISIONING\_REQUESTS\_AND\_REVIEW\_DUTY) enables such users to make and review requests. By default this role isn't included in any assignable role; it's up to you to decide what roles to add it to. The recommendation is, add it to a custom job role that's based on a role meant to be assigned widely, such as Employee (ORA\_PER\_EMPLOYEE\_ABSTRACT).

In addition, a privilege called View Access Requests (GTG\_VIEW\_ACCESS\_REQUESTS\_PRIV) provides view-only rights to the Access Request Approvals work area. Add it to a custom job role assigned to your auditors.

#### *Related Topics*

- [Copy or Edit Risk Management Roles in the Security Console](#)

### Advanced Access Request Jobs

Two jobs support Advanced Access Requests. Both are scheduled to run daily. Although that's recommended, you can use the Scheduling page in Setup and Administration to modify the schedules.

- Advanced Access Request Analysis runs all active access controls (if any exist) to uncover violations in all requests that have accumulated since the job's previous run.

Schedule the Global User Synchronization job to run before the Advanced Access Request Analysis job. It ensures that new users are correctly accounted for in access requests. (See [Global Users](#).)

- Access Request Notifications sends email alerts and notifications if you've activated them in the Settings for Email Alerts and Notifications page. (See [Activate Alerts](#).)

### Activate Security Briefings for Advanced Access Requests

For each role request, a security briefing can display data that provides useful information for determining whether the request should be approved. AI-generated summaries describe access granted by the role. Information about the request includes its data-security definition and the number of access-control violations the assignment would generate. Counts of users assigned the role provide context for the request.

Security briefings are disabled by default. They become available in the Access Request Reviews and Access Request Approvals work areas if you set a profile option:

1. In the Navigator, select My Enterprise > Setup and Maintenance. Expand the Task panel tab, then click Search.
2. Search for and select **Manage Administrator Profile Values**.
3. The Search area of the Manage Administrator Profile Values page includes a Profile Option Code field. In it, enter **ORA\_GTG\_ADVANCED\_ACCESS\_REQUEST\_GENAI\_ENABLED**. Click the Search button.
4. A record of that profile value appears. In the row for the Site profile level, select **Yes** in the Profile Value field. Click the **Save** button.
5. Click Save and Close.

**Note:** The Advanced Certifications application may also display security briefings, but only if a distinct profile option is set. This feature runs independently in the two applications, so you can choose to run it in only one or the other, or in both. (See *Activate the Enhanced Worksheet for Access Certifications*.)

## Migrate Data in Financial Reporting Compliance

### Use the Data Migration Tool

A Data Migration tool uploads operational data for Oracle Fusion Cloud 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.

You can use Data Migration to load an initial set of data or to update data in a single instance. Or you can 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

### Generate a Template

To generate a Data Migration template:

1. In the Data Migration page, click the **Create Import Template** button.
2. 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.

3. 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. 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.

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.
- 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, 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 **Import Data File** button.
2. In an Import File dialog, browse for and select your template file.
3. Click **Import**.
4. 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.

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 and issues.
- 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. Note that each perspective hierarchy can have a maximum of five hierarchical levels.

In the worksheet, 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.

## 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'd 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 can 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.

- 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 checkbox 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:

Activity Code	Activity Description
ASSESS_RISK	Risk assessment
AUDIT	Audit
AUDIT_TEST	Audit test
DESIGN_ASSESS	Design assessment
DOC_UPDATE	Documentation update
CERTIFY	Certification
OPERATING_ASSESS	Operating assessment

- When you finish entering data into the template, save it in the XML file format.

## Configure Financial Reporting Compliance

### Specify Assessment Activity Types

You can specify the activity types users can select as they create assessment templates or initiate impromptu assessments. Each type defines what assessors determine as they complete assessments. You can 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 Configuration Options tab.

2. In a Configure Module Objects panel, 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.

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.

## Assessment Activity Types

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

Type	Description	Available for Assessment Of
Certification	Is the information in this assessment of an object accurate and complete?	Process, risk, control
Audit Test	Does a risk, control, or process meet audit guidelines?	Process, risk, control
Operational Assessment	Does a control or process operate effectively and as designed?	Process, control

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

## Review Assessment-Response Codes

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

Each response consists of a "response code" and a "response name." The former is an internal value, and the latter is the text a user actually sees while assessing an object. You can review the codes that correspond to the response names in an Assessment Results page. To open it, click the Assessment Results tab in the Setup and Administration work area. However, the page is read-only. You can't modify the response codes, names, or their relationships to one another.

## Activate the Enhanced Worksheet for Access Certifications

Oracle Fusion Cloud Access Certifications enables your organization to perform reviews that determine whether roles are assigned properly to users. You can activate an enhanced certifier worksheet for use with this application, and you can enable it to display security briefings.

The certifier worksheet is a pivotal tool. Any number of certifiers may be involved in a certification project, each using a certifier worksheet to record judgments about a set of role assignments included in the project. Users known as owners and role managers supervise the certifiers, reviewing their worksheets in the process.

By default, however, the application provides an original worksheet. The enhanced worksheet offers an updated, cleaner design; improved filtering, search, and sort capability; and better performance when certifications involve large numbers of role assignments.

Security briefings display data that informs certification decisions: AI-generated summaries describe access granted by a role. Information about the assignment of that role to a user includes its data-security definition and the number of its access-control violations. Counts of other users assigned the role provide context for the role assignment.

You have the option of activating only the enhanced worksheet, or activating both features. You can't activate the security briefings if you continue to use the original worksheet. To activate these features, set profile values:

1. In the Navigator, select My Enterprise > Setup and Maintenance. Expand the Task panel tab, then click Search.
2. Search for and select **Manage Administrator Profile Values**.

3. To activate the enhanced worksheet, locate the Profile Option Code field in the Search area of the Manage Administrator Profile Values page. In it, enter **ORA\_GTR\_ACERT\_ENHANCED\_WORKSHEET\_ENABLED**. Click the Search button.
4. A record of that profile value appears. In the row for the Site profile level, select **Yes** in the Profile Value field. Click the **Save** button.
5. To activate security briefings, repeat steps 3 and 4, but search for and select the **ORA\_GTR\_ACERT\_GENAI\_ENABLED** profile value.
6. Click **Save and Close**.

Two issues may have an impact:

- For the enhanced worksheet to be available to users, updates are required for the Access Certification Manager predefined job role and any custom job roles based on it. The updates incorporate security features introduced in release 24C. If you've already updated the roles, you don't have to update them again. If you haven't, however, you can do so in any subsequent release. See [Required Security Update](#).
- The Advanced Access Requests application may also display security briefings, but only if a distinct profile option is set. This feature runs independently in the two applications, so you can choose to run it in only one or the other, or in both. See [Activate Security Briefings for Advanced Access Requests](#).

# 5 Audit

## Audit Objects

You can use the Oracle Cloud audit framework to track changes to records your organization creates in Oracle Fusion Cloud Risk Management.

You're strongly encouraged to use this feature. In part, it supports tasks you may need to complete regularly. External auditors may require you, for instance, to justify changes to controls that have occurred over an audit period. Audit reports can identify those controls and help you to justify the changes.

Internally, auditing helps you to control edits that have significant effects. For example, global user IDs differentiate users whose role assignments are analyzed by access models and controls. One implementation task is to select values that distinguish one global user from another. At any point after, a user may modify those values, but if so, all access model results and control incidents are purged. So are results and incidents for transaction models and controls that incorporate the User business object. The audit capability enables you to monitor significant changes such as this one.

The following are the objects, and the attributes of those objects, you can use the audit framework to track.

- Advanced controls: Control name, description, status, priority, flexfields, result investigator, perspectives, result perspectives, and related records.
- Entitlements: Entitlement name, description, status, and access point name.
- Global conditions: Name, filter name, attribute, condition, and value.
- Global users: First name, last name, middle name, user name, global user ID, email, hire date, status, and job.
- User-defined access points: User-defined access point ID, name, and description.
- User groups: New groups, deleted groups, and members who have been added to groups, removed from them, or are no longer eligible for them.
- Business object security: User name, Access by product or business object.

**Note:** You can also create transaction models that use audit data to uncover risk revealed by changes to data over time. For more on that audit capability, see [Create Models That Support Audit](#).

## Set Up Auditing

Enable auditing for attributes you want to track. To do this, you must be a user with rights to Oracle Fusion Functional Setup Manager.

1. In the Navigator, select My Enterprise > Setup and Maintenance. Expand the Task panel tab, then click Search.
2. Search for and select **Manage Audit Policies**.
3. In the Manage Audit Policies page, locate the row for Oracle Fusion Applications. In its Audit Level field, ensure that Auditing is selected.
4. Click the Configure Business Object Attributes button in that row.
5. In a Configure Business Object Attributes page, select Risks and Controls in the Product field.

6. An Objects section presents a hierarchical list of business objects. Select the checkboxes for those that contain attributes you want to track.

Each object you can audit belongs to a hierarchy. (Often the immediate child of the root object is an object with the same name as the root.) Click the checkbox not only of the parent object, but also each child object that has attributes you want to track.

You can select a child object without selecting its parent, but that can cause audit reports to exclude data relating to the parent. For example, you may select only the User Group Members child object in the User Assignment Groups hierarchy. A report meant to show user-group deletions would then show the members of groups that had been deleted, but wouldn't identify the groups themselves. It's recommended that whenever you select a child object, you also select its parents.

7. In an Audited Attributes section, click Create (a plus icon). In a Select and Add Audit Attributes dialog, click the checkbox for each attribute you want to track. Then click OK.

You select attributes of child objects one object at a time. Having finished with one child object, you select another (step 5), select Audited Attributes > Create, and make new selections. All the attributes you select from all child objects are audited. You don't have to select objects from all objects.

8. When you complete your selections, click Save and Close.

For example, suppose you want to track changes to advanced controls. Once you've opened the Configure Business Objects Attributes page, you'll find that the Advanced Controls object has four hierarchical subordinates. Immediately below, a child object is also called Advanced Controls. Beneath it, there are three more nodes, titled Perspective, Result Perspective, and Related Records.

You'd typically select all attributes for child objects that apply to your implementation, and all their parents. For example, Related Records attributes come into play only if you relate advanced controls to processes, risks, or controls. If so, you'd select Related Records attributes. If not, you wouldn't.

## Run Audit Reports

Audit reports capture changes made after auditing is enabled.

By default, each record in a report shows the following:

- The date and time a change was made.
- The user who made the change.
- The event (whether an item is inserted, deleted, or updated).
- The type of business object affected by the change.
- A description (the name of the item that's been changed).

To run a report:

1. Select Navigator > Tools > Audit Reports. This is available to you if you're assigned a role with the View Audit History privilege (FND\_VIEW\_AUDIT\_HISTORY\_PRIV).
2. In a Search area, select Risks and Controls in the Product field. In a Date field, define the period you want the report to cover, such as "Before" and the current date. You can also set other search criteria. For example:
  - If you select a value in the Business Object Type field, you limit the report results to records of changes to that object (for example, advanced controls). However, you also activate checkboxes that enable you to refine the information each record presents.

- You can use an Event Type field to have the report return records of all changes, or only of inserts, updates, or deletions.
- 3. Click the Search button. A Search Results area displays the change records you've searched for.
- 4. If your search criteria included a Business Object Type value, click any of three checkboxes to expand the information each record displays.

In particular, a Show Attribute Details option adds columns that identify the attribute that has changed in each record and display the old and new values of that attribute. When you click the Show Attribute Details checkbox, a field appears. In it, you may do either of the following:

- Select the value All Attributes. The report then displays the attribute, old value, and new value for every record your search criteria identified.
- Search for and select a single attribute. The report then filters records returned by your search criteria to include only those involving the attribute you select. It displays the attribute, old value, and new value for each of those records.

Click the related-topic link for more information on audit reporting.

#### *Related Topics*

- [Audit Reports](#)

