Oracle Fusion Cloud Risk Management

Securing Risk Management

24B

Oracle Fusion Cloud Risk Management
Securing Risk Management

24B

F92715-01

Author: David Christie

Contents

Get Help i

1 Introduction 1
Security Overview 1
Predefined Security Jobs 2

2 Users 3
Prepare an Implementation User 3
Prepare for and Manage Application Users 3

3 Functional Security 5
Roles Overview 5
Security Visualizations 6
Generate a Visualization 6
Options for Viewing a Visualization Graph 7
Visualization Table Display Options 8
Create Risk Management Roles in the Security Console 9
Copy or Edit Risk Management Roles in the Security Console 12
Compare Roles 13
Simulate Navigator Menus in the Security Console 14
Analytics for Roles 15
Configure the Security Console 15

4 Data Security 19
Data Security Overview 19
Select Users or Groups for Records 19
Manage User Assignment Groups 20
Export and Import User Assignment Groups 22
Use the Mass Edit Security Assignment Tool 22
Secure Business Objects 24

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

Use help icons to access help in the application. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons.

Get Support

You can get support at *My Oracle Support*. For accessible support, visit *Oracle Accessibility Learning and Support*.

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.

Learn About Accessibility

For information about Oracle's commitment to accessibility, visit the *Oracle Accessibility Program*. Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

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*.

Thanks for helping us improve our user assistance!

1 Introduction

Security Overview

In Oracle Fusion Cloud Risk Management, 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 each record as you create or edit that record.

Roles in Oracle Risk Management

A job role conceptually represents a job that a user performs in an organization. It typically provides broader functional access than a duty role, which represents one or more tasks included within a job.

Even so, either role type may define function security policies, role hierarchies, or both. A function security policy grants privileges to complete specific tasks. A role hierarchy is a set of subordinate roles; the parent role inherits functional access from them.

A job role provides broad enough access for assignment to a user. You can assign job roles directly to users, but you can't assign duty roles. A user is granted duty roles only indirectly, as elements in the hierarchy of a job role.

You can assign predefined job roles to users, or you can create and manage both job and duty roles. You'd use Oracle Applications Security, also known as the Security Console, to create your own roles.

Data Security in Oracle Risk Management

To have access to data records, a user must first be "eligible" and then "authorized." To be eligible for records of an object, a user must be assigned a role that grants privileges to work with that type of object. To be authorized for a record, an eligible user must be appointed as its owner, editor, or viewer. A user has access only to records for which he or she's authorized.

The eligible user who creates a record is authorized automatically as its owner, and that person may select other eligible users as owners, editors, or viewers.

- An owner can modify the details of a record, including its security configuration (the selection of users who can work with the record, and the level of their access).
- An editor can't change the security configuration, but can modify other details.
- A viewer can see record details, but can't change them.

If you assign predefined roles to users, owners may select them for records at any of the three levels. An owner can authorize less access for a record than a user's role allows. For example, an owner may select a user as a viewer of a transaction model. If so, that user can't edit the model, even if he or she remains eligible to be authorized as an editor or owner of other models.

Owners may also assign data-security rights that are specific to individual applications. For example, a user may have a role that grants rights to review or approve records in Oracle Fusion Cloud Financial Reporting Compliance. But those rights would apply only to records whose owners have authorized the user as a reviewer or approver.

Owners may authorize individual users for records, or may select user assignment groups. Each group is a set of users with an authorization for a type of object. Assigning groups to records is typically the more efficient approach to managing security: As users move into and out of positions in your organization, they can be added to or removed from

user assignment groups. This effectively grants or rescinds their access to records the groups are associated with. You create groups in a Risk Management Data Security work area.

Business Object Security

Within Oracle Fusion Cloud Advanced Controls, transaction models and controls define risks, then uncover transactions displaying those risks. Business objects provide business-application data for models and controls to analyze. As a further element of data security, you can select the business objects each user has access to. You make these selections in the Risk Management Data Security work area.

Related Topics

- Manage User Assignment Groups
- Secure Business Objects

Predefined Security Jobs

Three security jobs work together to update users' data access and worklists as their eligibility for data records changes over time.

A Security Synchronization 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.

The Security Synchronization job launches other jobs. Among them:

- 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.

These jobs are separate from Security Synchronization, and the Monitor Jobs page includes separate entries for their runs.

Use the Scheduling page to set or modify the schedule on which the Security Synchronization job runs, or use its Run Now feature to run the job on demand. Your ideal schedule should reflect the frequency of changes to roles and user assignments in your environment.

Because the Security Synchronization job launches the two result-update 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.

Related Topics

- Manage Job Schedules

2 Users

Prepare an Implementation User

The service activation mail from Oracle provides the service URLs, user name, and temporary password for the test or production environment. Use these credentials to create an implementation user whose responsibility is to set up Oracle Fusion Cloud Risk Management within each environment.

Setup involves:

- Configuring perspectives.
- Configuring security.
- Selecting assessment activities available to Process, Risk, and Control objects. Unlike other implementation tasks, this activity establishes some settings that can't be changed once application users create operational data.
- Setting administrative features that configure Oracle Risk Management for use and routine maintenance.
- Testing the implementation, in effect by using Oracle Risk Management features to ensure they return expected results.

> **Note:** You may use Oracle Risk Management as a tool to manage risk in other offerings, and so need to coordinate their implementations. They're likely to require distinct implementation users. Consult documentation for those other offerings for information about their requirements.

Create the implementation user in Oracle Fusion Cloud Human Capital Management (HCM), for example with Create User functionality available in a Manage Users work area. Doing so associates the implementation user with a person record, which is needed for the testing of an email notification feature.

> **Note:** It's possible to create user accounts in the Security Console. However, this doesn't create a person record and so is inappropriate. Use HCM, not the Security Console, to create the implementation user.

As you create the implementation user, you may assign these predefined job roles:

- Risk Administrator: This role enables the user to perform administrative setup, create perspectives, define user groups, configure business object security, and mass-edit security assignments.
- IT Security Manager: This role provides access to the Security Console, where the user can create roles.
- Oracle Risk Management job roles appropriate to use, and therefore test, the features you implement.

Prepare for and Manage Application Users

During implementation, you prepare your Oracle Fusion Applications Cloud service for application users. Tasks include determining whether:

- The creation of a person, user, or party record automatically creates a related user account.

- Roles are provisioned to users automatically or can be requested and, if so, creating role-provisioning rules.
- A user account is suspended automatically when the user has no roles, and reactivated automatically when roles are assigned.

During implementation, you can use the Create User task to create test application users. By default, this task creates a minimal person record and a user account. After implementation, you should use the Hire an Employee task to create application users. You can also import users. These tasks are available through HCM.

For detailed information on preparing for, creating, and managing application users, see Oracle Fusion Cloud ERP: Securing Cloud ERP.

You can set certain standards for user accounts in the General Administration page of the Security Console. These include the format of the user name (the value a user enters during sign-in to identify himself), and password format and policy.

3 Functional Security

Roles Overview

Oracle Fusion Cloud Risk Management provides seven predefined job roles:

- Access Certification Administrator. This role provides features of Oracle Fusion Cloud Access Certifications, and supporting setup and administration features.
- Access Request Security Administrator. This role provides features of Advanced Access Requests, which implements a workflow for requesting and assigning ERP roles. It's for assignment to request approvers, the only level of user who can approve or reject role requests.

  In addition, Access Provisioning Requests and Review is a duty role that enables users to request roles and review requests. It's not included in any assignable role, but you're expected to add it to one, for example a custom job role based on a widely assigned role such as Employee.
- Advanced Access Controls Analyst. This role provides Oracle Fusion Cloud Advanced Access Controls features, and supporting setup and administration features.
- Advanced Transaction Controls Analyst. This role provides Oracle Fusion Cloud Advanced Financial Controls features, and supporting setup and administration features.
- External Auditor. This role organizes activities for users responsible for enterprise auditing of advanced access and transaction controls, and of financial-reporting controls.
- Risk Activities Manager. This role provides Oracle Fusion Cloud Financial Reporting Compliance features, and supporting setup and administration features.
- Risk Administrator. This role grants access to all features in the Setup and Administration, Perspective, and Risk Management Data Security work areas. It's used by administrators, but is also typically the starting point for implementation job roles.

You can assign predefined job roles to users. To limit the access they provide, owners select users only for data records appropriate for them.

You may instead create your own job roles, but even if you do, you may choose to use predefined duty roles in their hierarchies. A common strategy is to copy a predefined job role that applies to a product area. You'd then remove duty roles from the copy, or potentially add duty roles to it, until you're left with what you want users to have.

You may also create duty roles, or copy predefined duty roles and edit the copies. However, you should rarely have occasion to do so. In most cases, the predefined duty roles should meet your needs.

How to Work with Roles

The remaining topics in this chapter apply to you if you intend to create, edit, or review roles. You configure roles, and may assign them to users, within Oracle Applications Security. Its Security Console enables you to:

- Create roles, either from scratch or by copying existing roles and editing the copies. As you create or edit job roles, you can also assign them to users.
- Visualize hierarchical relationships among users, roles, and privileges.
- Simulate Navigator menus available to roles or users.

- Compare versions of roles.

To open the Security Console, select Tools in the home page. Among its options, select Security Console. You must have the IT Security Manager role to do so.

Security Visualizations

A Security Console visualization graph consists of nodes that represent security items. These may be users, roles, privileges, or aggregate privileges. Arrows connect the nodes to define relationships among them.

You can trace paths from any item in a role hierarchy either toward users who are granted access or toward the privileges roles can grant.

You can select one of the following two views:

- Radial: Nodes form circular (or arc) patterns. The nodes in each circular pattern relate directly to a node at the center. That focal node represents the item you select to generate a visualization, or one you expand in the visualization.
- Layers: Nodes form a series of horizontal lines. The nodes in each line relate to one node in the previous line. This is the item you select to generate a visualization, or the one you expand in the visualization.

For example, a job role might consist of several duty roles. You might select the job role as the focus of a visualization (and set the Security Console to display paths leading toward privileges):

- The Radial view initially shows nodes representing the duty roles encircling a node representing the job role.
- The Layers view initially shows the duty-role nodes in a line after the job-role node.

You can then manipulate the image, for example, by expanding a node to display the items it consists of.

Alternatively, you can generate a visualization table that lists items related to an item you select. For example, a table may list the roles that descend from a role you select, or the privileges inherited by the selected role. You can export tabular data to an Excel file.

Related Topics

- Generate a Visualization
- Options for Viewing a Visualization Graph
- Visualization Table Display Options

Generate a Visualization

The Roles tab of the Security Console lets you generate a visualization. You can choose to view the details as a graph or as a table.

1. On the Security Console, click **Roles**.
2. Search for the security item on which you want to base the visualization.
    - In a Search field, select any combination of item types, for example, job role, duty role, privilege, or user.
    - In the adjacent field, enter at least three characters. The search returns the matching records.

- Select a record.
  Alternatively, click **Search** to load all the items in a Search Results column, and then select a record.

3. Select either **Show Graph** or **View as Table** button.

   Note: On the Administration page, you can determine the default view for a role.

4. In the **Expand Toward** list, select **Privileges** to trace paths from your selected item toward items lower in its role hierarchy. Or select **Users** to trace paths from your selected item toward items higher in its hierarchy.
5. If the Table view is active, select an item type in the Show list: Roles, Privileges, or Users. (The options available to you depend on your Expand Toward selection.) The table displays records of the item type you select. Note that an aggregate privilege is considered to be a role.

Options for Viewing a Visualization Graph

Within a visualization graph, you can select the Radial or Layers view. In either view, you can zoom in or out of the image. You can expand or collapse nodes, magnify them, or search for them.

You can also highlight nodes that represent types of security items.

1. To select a view, click Switch Layout in the Control Panel, which is a set of buttons on the visualization.
2. Select Radial or Layers.

Node Labels

You can enlarge or reduce a visualization, either by expanding or collapsing nodes or by zooming in or out of the image. As you do, the labels identifying nodes change:

- If the image is large, each node displays the name of the item it represents.
- If the image is small, symbols replace the names: U for user, R for role, S for predefined role, P for privilege, and A for aggregate privilege.
- If the image is smaller, the nodes are unlabeled.

Regardless of labeling, you can hover over a node to display the name and description of the user, role, or privilege it represents.

Nodes for each type of item are visually depicted such that item types are easily distinguished.

Expand or Collapse Nodes

To expand a node is to reveal roles, privileges, or users to which it connects. To collapse a node is to hide those items. To expand or collapse a node, select a node and right-click or just double-click on the node.

Using Control Panel Tools

Apart from the option to select the Radial or Layers view, the Control Panel contains these tools:

- Zoom In: Enlarge the image. You can also use the mouse wheel to zoom in.
- Zoom Out: Reduce the image. You can also use the mouse wheel to zoom out.
- Zoom to Fit: Center the image and size it so that it's as large as it can be while fitting entirely in its display window. (Nodes that you have expanded remain expanded.)

- Magnify: Activate a magnifying glass, then position it over nodes to enlarge them temporarily. You can use the mouse wheel to zoom in or out of the area covered by the magnifying glass. Click Magnify a second time to deactivate the magnifying glass.
- Search: Enter text to locate nodes whose names contain matching text. You can search only for nodes that the image is currently expanded to reveal.
- Control Panel: Hide or expose the Control Panel.

Using the Legend

A Legend lists the types of items currently on display. You can take the following actions:

- Hover over the entry for a particular item type to locate items of that type in the image. Items of all other types are grayed out.
- Click the entry for an item type to disable items of that type in the image. If an item of that type has child nodes, it's grayed out. If not, it disappears from the image. Click the entry a second time to restore disabled items.
- Hide or expose the Legend by clicking its button.

Using the Overview

On the image, click the plus sign to open the Overview, a thumbnail sketch of the visualization. Click any area of the thumbnail to focus the actual visualization on that area.

Alternatively, you can click the background of the visualization and move the entire image in any direction.

Refocusing the Image

You can select any node in a visualization as the focal point for a new visualization: Right-click a node, then select Set as Focus.

> **Note:** You can review role hierarchies using either a tabular or a graphical view. The default view depends on the setting of the **Enable default table view** option on the Administration tab.

Related Topics

- Visualization Table Display Options

Visualization Table Display Options

A visualization table contains records of roles, privileges, or users related to a security item you select.

The table displays records for only one type of item at a time:

- If you select a privilege as the focus of your visualization, select the Expand Toward Users option. Otherwise the table shows no results. Then use the Show option to list records of either roles or users who inherit the privilege.
- If you select a user as the focus of your visualization, select the Expand Toward Privileges option. Otherwise the table shows no results. Then use the Show option to list records of either roles or privileges assigned to the user.

- If you select any type of role or an aggregate privilege as the focus of your visualization, you can expand in either direction.
    - If you expand toward privileges, use the Show option to list records of either roles lower in hierarchy, or privileges related to your focus role.
    - If you expand toward users, use the Show option to list records of either roles higher in hierarchy, or users related to your focus role.

Tables are all-inclusive:

Table Name	What it displays
Roles	Records for all roles related directly or indirectly to your focus item. For each role, inheritance columns specify the name and code of a directly related role.
Privileges	Records for all privileges related directly or indirectly to your focus item. For each privilege, inheritance columns display the name and code of a role that directly owns the privilege.
Users	Records for all user assigned roles related directly or indirectly to your focus item. For each user, Assigned columns display the name and code of a role assigned directly to the user.

The table columns are search-enabled. Enter the search text in a column field to get the records matching your search text. You can export a table to Excel.

Create Risk Management Roles in the Security Console

You can use the Security Console to create Oracle Fusion Cloud Risk Management job or duty roles.

In many cases, an efficient method of creating a role is to copy an existing role, then edit the copy to meet your requirements. Typically, you'd create a role from scratch if no existing role is similar to the role you want to create.

To create a role from scratch, select the Roles tab in the Security Console, then click the Create Role button. Enter values in a series of role-creation pages, selecting Next or Back to navigate among them.

Provide Basic Information

On the Basic Information page:

1. In the Role Name field, create a display name, for example North America Risk Manager.
2. In the Role Code field, create an internal name for the role, such as GRC_NA_RISK_MGR_JOB.

> **Note:** Don't use "ORA_" as the beginning of a role code. This prefix is reserved for roles predefined by Oracle. You can't edit a role with the ORA_ prefix.

3. In the Role Category field, select a tag that identifies a purpose the role serves in common with other roles. Typically, a tag specifies a role type and an application the role applies to. For Oracle Risk Management, appropriate tags are "GRC - Job Roles" and "GRC - Duty Roles."
   If you select the duty-role category, you can't assign the role you're creating directly to users. To assign it, you'd include it in the hierarchy of a job role, then assign that role to users.
4. Optionally, describe the role in the Description field.

Add Function Security Policies

A function security policy selects a set of functional privileges; each permits use of a field or other user-interface feature. On a Function Security Policies page, you may define a policy for a duty role. The policy selects functional privileges to be inherited by other roles the duty role belongs to. Typically, you don't add function security policies directly to a job role.

As you define a policy, you can either add an individual privilege or copy all the privileges that belong to an existing role:

1. Select Add Function Security Policy.
2. In a Search field, select the Privileges value or role types in any combination, and enter at least three characters. The search returns items of the types you selected, whose names contain the characters you entered.
3. Select a privilege or role. If you select a privilege, click Add Privilege to Role. If you select a role, click Add Selected Privileges.

The Function Security Policies page lists all selected privileges. When appropriate, it also lists the role a privilege is inherited from. You can:

- Click a privilege to view details of the code resource that it secures.
- Delete a privilege. If, for example, you added the privileges associated with a role, but want to use only some of them, you must delete the rest. To delete a privilege, click its deletion icon (×).

Data Security Policies

Data security policies apply to Oracle Cloud applications other than Oracle Risk Management. If you're creating a Risk Management role, make no entries in the Data Security Policies page. Simply click Next to move to the next page.

Configure the Role Hierarchy

In a Role Hierarchy page, you link the role you're creating to other roles from which it's to inherit functional privileges.

- If you're creating a duty role, you can add duty roles to it. In effect, you're creating an expanded set of duties for incorporation into a job role.
- If you're creating a job role, you can add duty roles to it.

The page displays either a visualization table or a visualization graph with the role you're creating as its focus. Select the Show Graph button or View as Table button to select between them. However, you can add roles only when the visualization table is selected.

To add a role:

1. Ensure that View as Table is selected. Then click the Add Role option.
2. In a Search field, select a combination of role types, and enter at least three characters. The search returns items of the types you selected, whose names contain the characters you entered.
3. Select the role you want, and click Add Role Membership. You add not only the role you've selected, but also its entire hierarchy.

In the graph view, you can use the visualization Control Panel, Legend, and Overview tools to manipulate the nodes that define your role hierarchy.

Run Separation of Duties Analysis

On a Separation of Duties page, you can determine whether the hierarchy of the role you're creating includes separation of duties conflicts. These are pairs of roles that would allow an individual user to complete tasks that involve risk.

Note, however:

- Separation of duties conflicts are defined by provisioning rules. You would use the Separation of Duties page only if your organization uses Oracle Fusion Cloud Advanced Controls to create those provisioning rules.
- The Separation of Duties page is active only if your organization has set an ASE_SEGREGATION_OF_DUTIES_SETTING profile option to Yes in the Manage Administrator Profile Values page of Oracle Fusion Functional Setup Manager. (It would be appropriate for the option to be set to No if your organization doesn't use provisioning rules.)

If these two conditions are met, click the Analyze button. The Separation of Duties page then lists pairs of roles that provisioning rules define as conflicting. You'd be expected to return to the Role Hierarchy page to remove one role from each pair.

However, no validation is performed to confirm that you've done so. Be aware, therefore, that if you don't perform this role cleanup, you're creating a role that can't be assigned to any user without creating what your organization considers to be a separation of duties conflict.

Add Users

On a Users page, you can select users to whom you want to assign a job role you're creating. (You don't assign a duty role directly to users.)

When you add a user to a job role, he or she can access pages to which the role grants functional access. Data appears in data-secured pages, however, only when the user creates records (if the role grants that capability) or is selected for records by owners of those records.

To add a user:

1. Select Add Users.
2. In a Search field, select the value Users or types of role in any combination, and enter at least three characters. The search returns items of the types you selected, whose names contain the characters you entered.
3. Select a user or role. If you select a user, click Add User to Role. If you select a role, click Add Selected Users; this adds all its assigned users to the role you're creating.

The Users page lists all selected users. You can delete a user. You may, for example, have added all the users associated with a role. But you may intend to assign your new role only to some of them, and so must delete the rest. To delete a user, click its deletion icon (×).

Complete the Role

On a Summary and Impact Report page, review the selections you've made. Summary listings show the numbers of function security policies, roles, and users you've added and removed. An Impact listing shows the number of roles and users affected by your changes. Expand any of these listings to see names of policies, roles, or users included in its counts.

If you determine you want to make changes, navigate back to the appropriate page and do so. If you're satisfied with the role, select Save and Close.

Related Topics

- Work with Provisioning Rules

Copy or Edit Risk Management Roles in the Security Console

You can edit roles you've created from scratch. Or, you can copy any role, then edit the copy to create a new role.

> **Note:** You can't edit predefined roles. That's because your edits would be overwritten during each upgrade, when Oracle updates predefined roles to the specifications for the newer release. You can identify a predefined role by the ORA_ prefix in its role code. Or, a **Predefined role** box is checked in the Basic Information page for a role if it's shipped by Oracle.

Initiate a copy or an edit from the Roles tab of the Security Console. Do either of the following:

- Create a visualization graph and select any role in it. Right-click and select Copy Role or Edit Role.
- Generate a list of roles in the Search Results column of the Roles page. Select one of them, and click its menu icon. In the menu, select Copy Role or Edit Role.

If you're copying a role, you must also select one of two options:

- Copy top role: You copy only the role you've selected. The source role has links to roles in its hierarchy, and the copy inherits links to the original versions of those roles. If you select this option, subsequent changes to the inherited roles affect not only the source top role, but also your copy.
- Copy top role and inherited roles: You copy not only the role you've selected, but also all of the roles in its hierarchy. Your copy of the top role is connected to the new copies of subordinate roles. If you select this option, you insulate the copied role from changes to the original versions of the inherited roles.

Next, an editing train opens. Essentially, you follow the same process in editing a role as you would to create one. However, note the following:

- As is true for role creation, the Data Security Policies page in the Edit Role train has no application to Oracle Fusion Cloud Risk Management.
- By default, the name and code of a copied role match those of its source role, except that a prefix, suffix, or both are appended. In the Roles Administration page, you can configure the default prefix and suffix for each value.
- A copied job role can't inherit users from its source job role. You must select users for the copied role. (They may include users who belong to the source role.)
- The Role Hierarchy page displays all roles subordinate to a role you copied. Even so, you can add roles only to (or remove them from) the top role you copied.

To monitor the status of a role-copy job, select the Administration tab, and then the Role Status tab of the Administration page.

Compare Roles

You can compare any two roles to see the structural differences between them. As you compare roles, you can also add function security policies existing in the first role to the second role, providing that the second role isn't a predefined role.

For example, assume you've copied a role and edited the copy. You then upgrade to a new release. You can compare your edited role from the earlier release with the role as shipped in the later release. You may then decide whether to incorporate upgrade changes into your edited role. If the changes consist of new function security policies, you can upgrade your edited role by adding the new policies to it.

Select Roles for Comparison

1. Select the Roles tab in the Security Console.
2. Do any of the following:
    - Click the **Compare Roles** button.
    - Create a visualization graph, right-click one of its roles, and select the **Compare Roles** option.
    - Generate a list of roles in the Search Results column of the Roles page. Select one of them, and click its menu icon. In the menu, select **Compare Roles**.
3. Select roles for comparison:
    - If you began by clicking the **Compare Roles** button, select roles in both **First Role** and **Second Role** fields.
    - If you began by selecting a role in a visualization graph or the Search Results column, the **First Role** field displays the name of the role you selected. Select another role in the **Second Role** field.

    For either field, click the search icon, enter text, and select from a list of roles whose names contain that text.

Compare Roles

1. Select two roles for comparison.
2. Use the **Filter Criteria** field to filter for any combination of these artifacts in the two roles:
    - Function security policies
    - Inherited roles

    The data security policies option doesn't apply to Oracle Fusion Cloud Risk Management.
3. Use the **Show** field to determine whether the comparison returns:
    - All artifacts existing in each role
    - Those that exist only in one role, or only in the other role
    - Those that exist only in both roles
4. Click the **Compare** button.

You can export the results of a comparison to a spreadsheet. Select the **Export to Excel** option.

After you create the initial comparison, you can change the filter and show options. When you do, a new comparison is generated automatically.

Add Policies to a Role

1. Select two roles for comparison.
    - As the **First Role**, select a role policies already exist in.
    - As the **Second Role**, select the role you're adding the policies to. This must be a custom role. You can't modify a predefined role.
2. In the Filter Criteria field, select **Function security policies**. The **Data security policies** option doesn't apply, and the **Inherited roles** option is to be excluded for any application.
3. As a Show value, select **Only in first role**.
4. Click the **Compare** button.
5. Among the artifacts returned by the comparison, select those you want to copy.
6. An **Add to Second Role** option becomes active. Select it.

Simulate Navigator Menus in the Security Console

You can simulate Navigator menus available to roles or users. From a simulation, you can review the access inherent in a role or granted to a user. You can also determine how to alter that access to create roles.

Opening a Simulation

To open a simulated menu:

1. Select the Roles tab in the Security Console.
2. Create a visualization graph, or populate the Search Results column with a selection of roles or users.
3. In the visualization graph, right-click a role or user. Or, in the Search Results column, select a user or role and click its menu icon.
4. Select **Simulate Navigator**.

Working with the Simulation

In a Simulate Navigator page:

- Select **Show All** to view all the menu and task entries that may be included in a Navigator menu.
- Select **Show Access Granted** to view the menu and task entries actually assigned to the selected role or user.

In either view:

- A padlock icon indicates that a menu or task entry can be, but isn't currently, authorized for a role or user.
- An exclamation icon indicates an item that may be hidden from a user or role with the privilege for it, because it has been modified.

To plan how this authorization may be altered:

1. Click any menu item on the Simulate Navigator page.
2. Select either of the two options:

- **View Roles That Grant Access**: Lists roles that grant access to the menu item.
- **View Privileges Required for Menu**: Lists privileges required for access to the menu item. Lists privileges required for access to the task panel items.

Analytics for Roles

You can review statistics about the roles that exist in your Oracle Cloud instance.

On the Analytics page, click the Roles tab. Then view these analyses:

- Role Categories. Each role belongs to a category that defines some common purpose. Typically, a category contains a type of role configured for an application, for example, "Financials - Duty Roles."

  For each category, a Roles Category grid displays the number of:

  - Roles
  - Role memberships (roles belonging to other roles within the category)
  - Security policies created for those roles

  In addition, a Roles by Category pie chart compares the number of roles in each category with those in other categories.
- Roles in Category. Click a category in the Role Categories grid to list roles belonging to that category. For each role, the Roles in Category grid also shows the number of:

  - Role memberships
  - Security policies
  - Users assigned to the role
- Individual role statistics. Click the name of a role in the Roles in Category grid to list the security policies and users associated with the role. The page also presents collapsible diagrams of hierarchies to which the role belongs.

  Click Export to export data from this page to a spreadsheet.

Configure the Security Console

Before you start using the Security Console, ensure that you run the background processes that refresh security data. You can use the Security Console Administration pages to select the general options, role-oriented options, and track the status of role-copy jobs.

You can also select, edit, or add notification templates.

Run the Background Processes

Here are the background processes you must run:

- **Retrieve Latest LDAP Changes** - This process copies data from the LDAP directory to the Oracle Cloud Applications Security tables. Run this process once, before you start the implementation.
- **Import User and Role Application Security Data** - This process imports users, roles, privileges, and data security policies from the identity store, policy store, and Oracle Cloud Applications Security tables. Schedule it to run regularly to update those tables.

To run the **Retrieve Latest LDAP Changes** process:

1. In the Setup and Maintenance work area, go to the **Run User and Roles Synchronization Process** task in the Initial Users functional area.
2. If you want to be notified when this process ends select the corresponding option.
3. Click **Submit**.
4. Review the confirmation message and click **OK**.

To run the **Import User and Role Application Security Data** process:

1. Open the Scheduled Processes work area.
2. In the Search Results section of the Overview page, click **Schedule New Process**.
3. In the Schedule New Process dialog box, search for and select the **Import User and Role Application Security Data** process.
4. Click **OK**.
5. In the Process Details dialog box, click **Advanced**.
6. On the Schedule tab, set Run to **Using a schedule**.
7. Set **Frequency** to **Daily** and **Days Between Runs** to **1**.
8. Enter start and end dates and times. The start time should be after any daily run of the **Send Pending LDAP Requests** process completes.
9. Click **Submit**.
10. Click **OK** to close the confirmation message.

Configure the General Administration Options

1. On the Security Console, click **Administration**.
2. In the Certificate Preferences section, set the default number of days for which a certificate remains valid. Certificates establish keys for the encryption and decryption of data that Oracle Cloud applications exchange with other applications.
3. In the Synchronization Process Preferences section, specify the number of hours since the last run of the **Import User and Role Application Security Data** process. When you select the Roles tab, a warning message appears if the process hasn't been run in this period.

Configure the Role Administration Options

1. On the Security Console, click **Administration**.
2. On the Roles tab, specify the prefix and suffix that you want to add to the name and code of role copies. Each role has a Role Name (a display name) and a Role Code (an internal name). A role copy takes up the name and code of the source role, with this prefix or suffix (or both) added. The addition distinguishes the copy from its

source. By default, there is no prefix, the suffix for a role name is "Custom," and the suffix for a role code is "_CUSTOM."

3. In the **Graph Node Limit** field, set the maximum number of nodes a visualization graph can display. When a visualization graph contains a greater number of nodes, the visualizer recommends the table view.
4. Deselect **Enable default table view**, if you want the visualizations generated from the Roles tab to have the radial graph view.

View the Role Status

1. On the Security Console, click **Administration**.
2. On the Role Status tab, you can view records of jobs to copy roles. These jobs are initiated on the Roles page. Job status is updated automatically until a final status, typically Completed, is reached.
3. Click the **Delete** icon to delete the row representing a copy job.

4 Data Security

Data Security Overview

To secure data in Oracle Fusion Cloud Risk Management, owners of data records select users who can work with those records. Owners also set the level of access at which each user can work.

These security settings apply to records of:

- Processes, risks, controls, issues, remediation plans, assessments, and surveys.
- Models, advanced controls, and incident results.
- Certification projects.
- User assignment groups.

Also, you can complete these tasks in a Risk Management Data Security work area:

- Create user assignment groups. When an owner selects a group for a record, all members of the group are authorized to work with the record.
- Make mass edits to the assignments of users or groups to records.
- Select the business objects to which each user has access while working with transaction models and controls.

Select Users or Groups for Records

You must be the owner of a record to modify its data security. If so, you can select the users who work with it, and you can set their levels of access to it.

You may be the owner of a record either because you created it or because you've been added as an owner of it.

Depending on the type of object you're working with:

- Security configuration may occur as a step in a "guided process" as you create or edit a record.
- A Security Assignment button may appear in the page to view or edit a record. Clicking it opens a Security Assignment page. (The button isn't available while the record is being created, but appears immediately after its creator saves or submits it for the first time.)

In either case, you can select individuals or user groups. Typically, if you create groups and assign them to records, you'll have less to keep track of, and so security management will be easier.

To select individual users, click Add in a User Assignments panel. Search for and select a user in a Name field. Then make these selections:

- In an Authorized As field, select Owner, Editor, or Viewer. An owner can edit details of the record, including its security configuration. An editor can't modify the security configuration, but can modify other details. A viewer

can see record details, but can't change them. These are authorizations that apply in any Oracle Fusion Cloud Risk Management application. You must select one value for each user you add to a record.

You can select less access for a record than a user's role allows. For example, a user may be eligible to own, edit, or view records of an object. If you select that user as a viewer for a record, he can't edit it, even though he remains eligible to be selected at any level for other records of the object.

- In an Authorizations field, optionally select one or more authorizations specific to Oracle Fusion Cloud Financial Reporting Compliance or to Oracle Fusion Cloud Access Certifications. (This field doesn't apply to Oracle Fusion Cloud Advanced Controls or to user groups, and so doesn't appear as you secure their records.)

  The two types of authorization are distinct. For example, you may select a user as a viewer of a risk in Oracle Financial Reporting Compliance. You may also select her as an approver. If so, she can't edit the risk record itself, but she does have write access to the page in which the risk is either approved or rejected.

  While an Authorizations selection is optional for individual users, making no selection for any user would have an impact on functionality. For example, if you select no user as an approver or reviewer of a record, that record isn't subject to review or approval. For another example, it makes no sense to create a certification project if you select no users to manage and certify roles within it.

To select user groups, click Add in a Group Assignment panel. Search for and select one or more groups.

- Each group is granted a single authorization when it's created. As you select a group for a record, you can view its authorization, but you can't change it. You may assign multiple groups to a record, to combine authorizations. (See *Manage User Assignment Groups*.)
- A group is available to be selected for a record only if at least one of its members is eligible for that record. Groups with no eligible users are excluded.
- Over time, members may be added to or dropped from groups, or their role assignments may change. This may result in a group having been assigned to a record but no longer having members who are eligible for it. If so, a warning icon appears next to the group name.

In either the User Assignment or Group Assignment panel, you can filter lists by authorization. Use either of two methods:

- Click Show Filters, then click an authorization in either of two lists: "Authorized As" or "Ineligible User." The panel then displays users or groups either granted the authorization you selected, or ineligible for it. Also, an "Authorized As [authorization]" or an "Ineligible User [authorization]" button appears, and the filter remains in force until you select the delete icon for the button. Multiple filters have an AND relationship.
- Type an authorization in the Search by field, preceding it either by a plus sign or a minus sign. A plus sign with an authorization is equivalent to selecting that authorization in the Authorized As list. For example "+Owner" returns authorized owners, or groups each of which has at least one member eligible to be an owner. A minus sign with an authorization is equivalent to selecting that authorization in the Ineligible User list. For example, "-Owner" returns users who were authorized for the record as owners, but are no longer eligible for it.

See *Secure Records in Advanced Controls*, *Secure Records in Financial Reporting Compliance*, and *Secure the Certification* for user-authorization details specific to each application.

Manage User Assignment Groups

As they edit records, owners may select user assignment groups, assigning data rights to all members of each group at once.

Each group specifies an authorization. While selecting a group for a record, an owner can view the authorization it provides, but can't change that authorization.

For each group you create, you can select only one authorization (and an object it applies to). You may select one of the application-specific authorizations, such as reviewer or approver in Oracle Fusion Cloud Financial Reporting Compliance, or manager or certifier in Oracle Fusion Cloud Access Certifications. But to have access to records, a user must be authorized as an owner, editor, or viewer. So if you select any authorization other than those three for a group, its members are also automatically assigned the viewer authorization.

To combine multiple authorizations, you can create multiple groups. For example, you may create a group of risk approvers, and assign it to a risk record. Its members would have only view access to the risk record itself, but would be able to approve or reject it. You might want some or all of these users to be able to edit the risk as well. You'd create a second group, assign it the editor authorization for the risk object, assign users to it, and select it for the risk record. Users who belong to both groups would be able both to edit the risk record and to approve or reject the risk.

To create a user assignment group:

1. Use either of two methods to open a Create User Assignment Group page:
    - Select the Create User Assignment Group 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.)
    - Navigate to Risk Management > Risk Management Data Security. User Assignment Groups is the landing page for this work area. Then select Add.
2. In a Details panel:
    - Name the group.
    - Select an object. The group you're creating becomes available for selection by an owner working with a record of this object type.
    - Select an authorization. The authorizations available for selection are those appropriate for the object you've selected.
3. An Eligible Users panel displays a list of users whose roles make them eligible for the object and authorization you chose. Select among those users:
    - Optionally, search for users to select. Enter text in the search field; a list displays user names that contain text matching what you've typed. Select one of them, or click the Search button to select all the matches for your text string.
    - To select members individually, click check boxes next to their names. Then click Add Selected Users. You may select any number of times; for example, you may create one filter, select among the users it returns, then create another filter and select among the users it returns.
    - Instead, you can click an Add All Eligible Users option. (If you've selected any user check boxes, clear them first.) This selects all users from the full list; if you've filtered the list of users, this option ignores the filter.

    The user names you select move from the Eligible Users panel to the Members panel. If you have second thoughts, you can click the delete icon in the row for any user in the Members panel to return that user to the Eligible Users panel.
4. When you're satisfied with your Member selections, click Save and Close.

To edit an existing group:

- Search for it in the User Assignment Groups page. To make the search easier, click Show Filters, then create one or more filters based on predefined attributes, and click Search. For filters based on user information (such as Department or Location), a search returns groups with at least one member who meets the criteria you specify.

- Select the Edit icon in the record of the group you want to edit.
- You can't modify the object and authorization selections. Otherwise, follow the creation procedure to edit the group name or to add or delete members.

If you're an owner of the group, you can also authorize other users to work with it. Click the Security Assignment button (which appears only after the group has been saved for the first time), and authorize individual users or add groups for which the User Assignment Groups object is selected.

Export and Import User Assignment Groups

You can export user assignment groups from a source instance to a file, then import them from the file to a second instance.

Here are issues to be aware of before you undertake these tasks:

- When you export groups, security assignments configured for them aren't exported with them. A user who subsequently imports them automatically becomes their owner in the destination environment, and could configure additional security for them in that environment.
- The import job fails if the file contains a group whose name matches that of a group already existing in the destination instance.

To export user assignment groups:

1. Navigate to Risk Management > Risk Management Data Security. This opens the User Assignment Groups page.
2. Click the check boxes for the groups you want to export. You can select one or multiple groups.
3. Select Actions > Export User Group. A message presents a job ID. Note the ID, then close the message.
4. Click the Monitor Jobs button to navigate to the Monitor Jobs page.
5. Locate the row displaying the job ID you noted.
6. When the status displayed in that row reaches Completed, click the Download icon.
7. A file-download window offers you options to open or save the export file. Select the Save option. In a distinct save-as dialog, navigate to the folder you want to save the file in.

To import user assignment groups:

1. From the User Assignment Groups page, select Actions > Import User Group.
2. In an Import User Group page, select a file that contains groups you want to import. Click Browse, navigate to the location of the file, and select the file name. It consists of the phrase "User_Groups" followed by a number, with a json file extension. That file name then populates the File field on the Import page.
3. Click the Submit button. Again, a message presents a job ID. Note the ID, then close the message.
4. Click the Monitor Jobs button to navigate to the monitor jobs page. Locate the row displaying the job ID you noted, and confirm that it reaches the Completed state.

Use the Mass Edit Security Assignment Tool

Use the Mass Edit Security Assignment tool to modify the security settings for any number of records at once. You can perform these security mass-edits only on records for which you're authorized as owner.

Note: There's one special case: If you're assigned the Risk Administrator job role, you can act as the owner of every record in your system, even those for which you haven't been directly selected as owner. Because that feature makes the role very powerful, it should be assigned to few users.

Broadly, the procedure for security mass edits involves selecting the records you want to update, and then defining how security should change for those records. But an access or transaction control may generate thousands of incidents. To accommodate such large numbers, you use either of two specialized procedures to select records as you mass-edit incident security. More on these in a minute.

Other records for which you can mass-edit security assignments include models and advanced controls; processes, risks, controls, issues, remediation plans, assessments, and surveys; and role-certification projects. You can also update the owners, editors, or viewers selected for user-assignment groups, or update their membership. Here's how:

1. Navigate to Risk Management > Risk Management Data Security. Select the Mass Edit Security Assignment tab.
2. In a Select Object field, select an object to update security for records of that object. A list of object records appears.
3. Optionally, filter the list of object records. Click Show Filters, and enter filtering parameters in the Filters panel. Then click Search.

   You may want to apply certain filters regularly to discover records whose security needs updating: If you selected the User Group Membership object, you can filter for groups with ineligible members or with no members. If you selected any other object, you can filter for records with users or groups that are ineligible for an authorization you specify, for instance processes with owners who are no longer eligible. Or you can filter for records missing eligible users or groups for an authorization, for example advanced controls with no editors.
4. Optionally, review existing assignments for records in your list. If you selected the User Group Membership object, select a Group Members link for each group to view its current membership. Or if you selected any other object, click a Security Assignment link for each record to view its current security assignments.
5. Select the check boxes for records whose security authorizations you want to reassign. Or click a Select All check box. If you filtered the list of records, the Select All option applies only to the records returned by your filter.
6. Click the Edit button.
7. Enter values in a Define Security Assignment Goals panel. Then click Continue.
   - In a What Assignment Type Do You Want to Update field, select Group Assignment or User Assignment.
   - In a What Action Do You Want to Perform field, select Append to add users or groups to records, Remove to remove them from records, or Replace to substitute one user or group for another in records. Subsequent options depend on the selection you make here.
8. If you selected the User Assignment and Append options in step 7, a Define Security Assignment Authorizations panel becomes active. Make selections, then click Continue.
   - Select Owner, Editor, or Viewer in a What Authorization Do You Want to Update list field. This is required.
   - Depending on the object you selected, check boxes representing object-specific authorizations may also appear. Optionally select among them.

   If you made any other combination of selections in step 7, the Define Security Assignment Authorizations panel doesn't apply and so disappears from view.
9. In a final "Identify" panel, your options depend on previous selections.
   - If you chose to append or remove users or groups, select check boxes representing any number of users or groups to be added or removed. You can filter the list of users or groups; use the Show Filters option to enter filtering parameters. Again, if you filter and click the Select All check box, it applies only to the users or groups returned by your filter.

- If you chose to replace a user or group, search for and select a single user or group you want to replace, and a single user or group you want to replace it with.

10. Click the Submit button.

If you're mass-editing security for access or transaction incidents, one option is to use the preceding procedure with adaptations:

- As you complete step 2, select Access Incident or Transaction Incident in the Select Object field. An Advanced Control Name field appears. In it, search for a control; you'll be updating security for the incidents it has generated. (For any other type of object, this field doesn't apply, and so doesn't appear.)
- As you complete step 5, the list of incidents includes a maximum of 500 records, but the control may have generated more. The page notifies you of the total number of incidents. You can select from the initial list or a filtered list. You may instead click the Select All check box to update security for the total number of incident records, not just the 500 on display.

A second option is to select incidents for mass-edit. For complete details, see the *Mass-Edit Incidents* topic and, in particular, its "Select Incidents from the Results Page" section. But in summary:

- Start from either the Controls page in the Advanced Controls work area or the Results by Control Summary page in the Results work area. In the record of a control, click its Results Count value.
- A Results page lists incidents generated by the control you selected. Filter the list to include only those you want to edit. Then click a Mass Edit button.
- In a Mass Edit page, select a Mass Edit Security radio button.
- That takes you to the Mass Edit Security Assignment tool. The incidents you want to update are already selected, so all that's left is to define how you want to update them. To do that, complete steps 7 through 10 of the preceding procedure.

Secure Business Objects

To work with transaction models or controls, users require access to business objects. By default, however, they don't have any. Your organization must assign each user the objects he or she can use.

A business object is, in effect, a data set. A "delivered" business object supplies values for a set of related data fields from a business application. An "imported" object includes data imported from an xml file. A "user-defined" object consists of data returned by a specially configured advanced control. The need to assign objects to users applies to each of these object types.

> **Note:** This feature applies only to transaction models and controls. Business objects that apply to access models and controls, and to access certifications, are available automatically to all users who work with these items.

To select the business objects available to users of Advanced Financial Controls:

1. Navigate to Risk Management > Risk Management Data Security. Select the Business Object Security tab.
2. A Business Object Security page presents a list of users under the heading User Access to Business Objects. Users appear in this list if they're assigned roles that include two privileges, View Transaction Model and View Transaction Control. Use a search field to filter the list for users for whom you want to select business objects.
3. For each user, you may select a "Grant access to all business objects" check box. Or, click the user's name to assign objects to the user.

4. If you click the user's name:
    - No objects may yet be assigned to the user. In that case, a page offers you a choice between adding objects manually or selecting another user to copy that user's access. To do the latter, search for and select a user in the User field, and click the Copy button. Or, to select business objects manually, click Add.
    - If objects have already been assigned to the user, the page offering the option to copy another user's access is skipped, and the page to add objects appears, displaying the user's current access.

In the page to add objects, you can select products, and so add all the business objects that apply to each product you select. If you take this approach, the user's access to business objects is updated automatically to reflect any future changes to the business objects that apply to each product.

1. Click Add in the Access by Product panel of the page to add objects. A new row appears.
2. Use the drop-down list to search for and select a product.
3. Click Save. This selects all the business objects appropriate for that product.

Repeat the process for any other products you want to select. Or, you can click the x icon in the row for any product you want to delete.

Alternatively, you can select business objects themselves:

1. Click Add in the Access by Business Object panel of the page to add objects. A new row appears.
2. Use the drop-down list to search for and select a business object.
3. Click Save.
4. Repeat the process to add other objects.

You can make selections in both panels, but can't select the same object in both. That is, if you select a product, the business objects that belong to it are no longer available for selection in the Access by Business Object panel. If you select an object, the product it belongs to is no longer available for selection in the Access by Product panel. (For reference, the Access by Business Object panel displays both the names of business objects and, for each, the name of the product it belongs to, in parentheses.)

If you've selected some objects belonging to a product, but then want to select their product instead, first remove the objects from the Access by Business Object panel:

1. Use the search field to search for the objects you want to remove.
2. Click the check box in the row for each object.
3. Click the Remove button.