Oracle Risk Management Cloud
Securing Risk Management

19C
# Contents

<table>
<thead>
<tr>
<th>Preface</th>
<th>i</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong> Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Overview of Risk Management Security</td>
<td>1</td>
</tr>
<tr>
<td>Perspectives</td>
<td>2</td>
</tr>
<tr>
<td>Predefined Security Job</td>
<td>2</td>
</tr>
<tr>
<td><strong>2</strong> Users</td>
<td>3</td>
</tr>
<tr>
<td>The Risk Management Implementation User</td>
<td>3</td>
</tr>
<tr>
<td>Prepare for and Manage Risk Management Users</td>
<td>3</td>
</tr>
<tr>
<td><strong>3</strong> Functional Security</td>
<td>5</td>
</tr>
<tr>
<td>Overview of Risk Management Roles</td>
<td>5</td>
</tr>
<tr>
<td>Security Visualizations</td>
<td>6</td>
</tr>
<tr>
<td>Generate a Visualization</td>
<td>7</td>
</tr>
<tr>
<td>Options for Viewing a Visualization Graph</td>
<td>7</td>
</tr>
<tr>
<td>Visualization Table Display Options</td>
<td>9</td>
</tr>
<tr>
<td>Create Risk Management Roles in the Security Console</td>
<td>9</td>
</tr>
<tr>
<td>Copy or Edit Risk Management Roles in the Security Console</td>
<td>12</td>
</tr>
<tr>
<td>Compare Roles</td>
<td>13</td>
</tr>
<tr>
<td>Simulate Navigator Menus in the Security Console</td>
<td>14</td>
</tr>
<tr>
<td>Analytics for Roles</td>
<td>15</td>
</tr>
<tr>
<td>Administrate the Security Console</td>
<td>15</td>
</tr>
<tr>
<td><strong>4</strong> Data Security</td>
<td>19</td>
</tr>
<tr>
<td>Overview of Risk Management Data Security Policies</td>
<td>19</td>
</tr>
<tr>
<td>Create or Edit a Data Security Policy for Risk Management</td>
<td>20</td>
</tr>
<tr>
<td>How a Policy Applies Multiple Perspective Values</td>
<td>20</td>
</tr>
<tr>
<td>Map Risk Management Data Security Policies to Roles</td>
<td>21</td>
</tr>
<tr>
<td>Examples of Data Security Policy Mappings to Roles</td>
<td>22</td>
</tr>
<tr>
<td>What happens if I edit roles that are mapped to Risk Management data security policies?</td>
<td>22</td>
</tr>
</tbody>
</table>
Preface

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

Using Oracle Applications

Using Applications Help

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

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

You can also read Using Applications Help.

Additional Resources

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

- **Guides and Videos:** Go to the Oracle Help Center to find guides and videos.

- **Training:** Take courses on Oracle Cloud from Oracle University.

Conventions

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

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

Documentation Accessibility

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

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

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

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

Overview of Risk Management Security

In the Risk Management family of applications, duty and job roles grant access to functionality, and data security policies grant access to data.

- 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.

Commonly in Risk Management, a lower-level duty role uses function security policies to define an individual task. A higher-level duty role gathers related tasks together, by defining a hierarchy that consists of lower-level duty roles. A job role defines a hierarchy of higher-level duty roles providing 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 create and manage roles in Oracle Applications Security, also known as the Security Console.

- A data security policy defines a set of data. You map the policy to a role, and so apply the functionality granted by the role to the data defined by the policy. You create and manage data security policies, and map them to roles, in the Manage Security page of Risk Management.

"Role" and "data security policy" are conceptually different in Risk Management than they are in other Oracle Cloud applications:

- In other applications, a duty role grants access to functionality, but it also has a data-definition component. In effect, the role selects functional privileges, but it also selects data required to support those privileges.

  In Risk Management, a duty role has no data-definition component. It purely defines functionality: a set of functional privileges that constitute a duty, or a set of duties that support a larger duty or a job.

- In other applications, a data security policy is the data-definition component of a duty role, and so is an integral part of a duty role.

  In Risk Management, a data security policy is configured completely independently of any role. It uses entirely different criteria to define data. For example, it may use perspectives, which don’t exist in other applications. It may map to either a duty role or a job role.

- Other applications may include aggregate privileges as elements of duty or job roles. Again, these have both functional- and data-definition components.

  Risk Management roles don’t use aggregate privileges.

- HCM applications may define data roles. These are based on HCM security profiles and can be assigned directly to users.

  Risk Management uses neither data roles nor security profiles. Risk Management job roles are assigned directly to users.
• Typically, a user is assigned at least one abstract role. For example, an Employee role provides access to tasks and functions that are both unrelated to a specific job and performed by every employee. Abstract roles have no bearing on Risk Management security.

Perspectives

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

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

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

Perspectives and Security

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

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

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

Predefined Security Job

Risk Management roles, and their assignment to users, are managed in the Security Console. A predefined job, called Security Synchronization, enables Risk Management to recognize changes made in the Security Console. The job also updates worklists to match current security definitions.

The job runs the first time you start Risk Management, and at scheduled intervals thereafter. The first time it runs, it maps predefined roles to predefined data security policies.

By default, the Security Synchronization job runs once a week, on Sundays. It’s anticipated you will modify this default schedule. Your ideal schedule should reflect the frequency of changes to roles, user assignments, and data security policies in your environment. Use the Scheduling page to modify the schedule, or use its Run Now feature to run the job on demand.

Related Topics

• Modify Schedules
2 Users

The Risk Management 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 Risk Management within each environment. Setup involves:

- Configuring perspectives that are to be incorporated into data security policies.
- Configuring security: At minimum, creating job roles and data security policies.
- Selecting features and assessment activities available to objects in the Financial Reporting Compliance module. 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 Risk Management for use and routine maintenance.
- Testing the implementation, in effect by using Risk Management features to ensure they return expected results.

**Note:** You may use Risk Management as a tool to manage risk in other Oracle Cloud offerings. If so, you’re expected to coordinate the implementation of Risk Management with the implementation of those other offerings. This is likely to require the creation of implementation users for those other offerings in addition to the Risk Management implementation user. Consult documentation for those other offerings for information about their requirements.

Create the Risk Management implementation user in Oracle 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 for the Risk Management implementation user. Use HCM, not the Security Console, to create the Risk Management implementation user.

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

- Enterprise Risk and Control Manager: Among the duties it grants, this role enables the user to perform module and administrative setup, to create perspectives and data security policies, and to test the implementation.
- IT Security Manager: This role provides access to the Security Console, where the user can create Risk Management roles.

It’s recommended that you revoke the assignment to the Enterprise Risk and Control Manager role when implementation is complete. This super user role isn’t intended for everyday use. While creating roles in the Security Console, the implementation user may create a Risk Management Administrator job role to replace it. This role would include only duty roles for module, administrative, perspective, and data security policy management.
Prepare for and Manage Risk Management Users

During implementation, you prepare your Oracle 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 the Securing ERP document.

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

Overview of Risk Management Roles

You’re expected to create your own job roles for assignment to Risk Management users.

- Only six predefined job roles exist. Each is a super user role, granting far more access than everyday application users should have. You should not assign any of these roles to application users. You should instead create roles that grant access limited to the tasks individual users are to complete.

- You can’t alter the mappings of predefined data-security policies to predefined roles. To implement perspective-based security, therefore, you must not only create data-security policies that incorporate perspective values, but also create job roles you can map them to.

A common strategy for developing job roles is to copy a predefined role that applies to a product area, then remove duties from the copy until you’re left with what you want users to have. The six predefined job roles are:

- Application Access Auditor. This provides Advanced Access Controls features (other than those that apply to Access Certification), and setup and administration features that support Advanced Access Controls.

- User Access Certification Manager. This provides features of the Access Certification component of Advanced Access Controls, and setup and administration features that support Access Certification.

- Application Control Manager. This provides Advanced Financial Controls features, and setup and administration features that support Advanced Financial Controls.

- Compliance Manager. This provides Financial Reporting Compliance features, and setup and administration features that support Financial Reporting Compliance.

- Enterprise Risk and Control Manager. This is the most expansive job role. In addition to Financial Reporting Compliance features, it grants access to all Risk Management Tools functionality. In particular, this is the only predefined job role that provides access to perspective management. It’s typically the starting point for administrative and implementation job roles.

- Risk Management Auditor. This role organizes activities for users responsible for enterprise auditing in advanced access and transaction controls, and in financial reporting compliance controls.

Moreover, Oracle provides a large set of predefined duty roles, and you may select from these to add functional access to each job role you create. You can’t modify predefined roles. You can 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 meet your needs.

It’s generally preferred that you design roles so that you can assign multiple job roles to any given user. Each job role would contain a subset of the duty roles the user requires. This affords flexibility: Each job role remains available for assignment to other users in varying combinations with other job roles.
Security for Access Certification

The Access Certification component of Advanced Access Controls presents a special case. As is customary, you may develop job roles by removing duty roles from copies of a predefined job role (in this case, User Access Certification Manager), or by adding duty roles to job roles you create. However:

- It’s important that you use only the predefined duty roles. These are Access Certification Administrator, Access Certification Owner, Access Certification Certifier, and Access Certification Configuration and Maintenance. Don’t modify copies of them or create new Access Certification duty roles.

It’s expected that each Access Certification user serves in one capacity: administrator, owner, or certifier. To enforce this, you would add only one of the administrator, owner, or certifier duty roles to a given job role. However, this isn’t required. The configuration and maintenance duty role enables a user to run an Access Certification Synchronization job on demand or to enable email alerts, and is typically granted to an administrator. You can add each duty role to a job role expressly for Access Certification or to a job role with duties unrelated to Access Certification.

- An Access Certification job role doesn’t require a data security policy. There’s no need to create a policy that specifies perspective values, which don’t apply to Access Certification. Each job role that contains a predefined Access Certification duty role inherits a predefined data security policy mapped to that duty role.

If you add an Access Certification duty role to a job role with duties unrelated to Access Certification, that job role may be mapped to a data security policy, and that policy may specify perspective values. If so, these have no effect on the Access Certification duties.

How to Work with Roles

You configure Risk Management 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 show nodes representing the duty roles encircling a node representing the job role.
- The Layers view initially show 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.

## Generate a Visualization

Here’s how you can generate a visualization:

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 is 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 is 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.

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>
<thead>
<tr>
<th>Table Name</th>
<th>What it displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles</td>
<td>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.</td>
</tr>
<tr>
<td>Privileges</td>
<td>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.</td>
</tr>
<tr>
<td>Users</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 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 would 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 a 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 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 would 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 value Privileges 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 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 x icon.
Data Security Policies

Data security policies (as they can be configured in the Security Console) apply to Oracle Cloud applications other than Risk Management. To create data security policies appropriate for Risk Management, you use a Manage Security page within Risk Management. In the Data Security Policies page in the Create Role train of the Security Console, make no entries. Simply click Next to move to the next page.

Note: For Risk Management purposes, you may opt to set the Data Security Policies page to be read-only. To do so, select the Administration tab, and then the Roles tab on the Administration page. Locate and clear an "Enable edit of data security policies" option.

Configure the Role Hierarchy

A Role Hierarchy page displays either a visualization graph, with the role you’re creating as its focus, or a visualization table. Select the Show Graph button or View as Table button to select between them. In either case, 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.

To add a role:

1. Select Add Role.
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 have 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.

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.)

Note: For the Users page to be active, you must select an "Enable edit of user role membership" option. To locate it, select the Administration tab, and then the Roles tab on the Administration page. If this option isn’t selected, the Users page is read-only.

You may add users to a job role before you map that role to a data security policy. If so, the users can access pages the role grants functional access to, but no data. Data would appear in these pages after you map the role to a data security policy.

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 x icon.

**Complete the Role**

On a Summary and Impact Report page, review the selections you have made. Summary listings show the numbers of function security policies, roles, and users you have 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.

**Copy or Edit Risk Management Roles in the Security Console**

You can edit roles you have 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 have 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 have 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 Risk Management. Use the Manage Security page within Risk Management to create or edit data security policies appropriate for 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 Copy 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 have 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 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 to Risk Management, 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 is not 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.

### 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.

### Administrate the Security Console

To prepare the Security Console for use, arrange to run background processes that refresh security data. You can use Security Console Administration pages to select general and role-oriented options, 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 Oracle Cloud Applications Security tables. Run it once, during 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, search for the Run User and Roles Synchronization Process task and select it.
2. Click **Submit**.
3. Review the confirmation message and click **OK**.

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

1. In the Tools work area, select **Scheduled Processes**.
2. Click **Schedule New Process**.
4. Click **OK**.
5. Click **Submit**.
6. Review the confirmation message and click **OK**.

Configure the General Administration Options

1. On the Security Console, click **Administration**.
2. Under Certificate Preferences, 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. Under Synchronization Process Preferences, 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 has not 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.
5. Enable edit of data security policies: Determine whether users can enter data on the Data Security Policies page of the role-creation and role-edit trains available from the Roles tab.
6. Enable edit of user role membership: Determine whether users can enter data on the Users page of the role-creation and role-edit trains available from the Roles tab.
View the Role Copy Status

1. On the Security Console, click **Administration**.
2. On the Role Copy 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

Overview of Risk Management Data Security Policies

A Risk Management data security policy consists of filters that select data to which the policy grants access. Each filter expresses a relationship between an attribute and a value. It may grant access to data that satisfies the defined relationship. Or it may be configured to prevent such access, in effect granting access to all other data.

For example, the attribute may be the name of a perspective, such as Region. The value in that case would be a node of that perspective, such as North America. The filter may then select records of objects assigned the North America value as they were created. Or it may exclude those objects, in effect selecting objects associated with all other regions.

Data security policies map to roles maintained in the Security Console. Functional access granted by a role applies to data designated by the mapped data security policy.

You may design job roles so that each defines a hierarchy consisting of predefined duty roles. If so, you need not create data security policies for duty roles. That’s because every predefined role maps to a predefined data security policy. A Security Synchronization process completes that mapping automatically the first time Risk Management runs.

You would, nevertheless, create data security policies for job roles you have designed. These policies apply to roles that enable users to work directly with objects that perspectives can be assigned to. In Financial Reporting Compliance, these include processes, risks, and controls. In Advanced Financial Controls, these include models, advanced controls, and incidents. Typically, filters for such a policy would:

- Select the data security policies already mapped to all duty roles included in the hierarchy of the job role. So far, the policy grants access to all the data defined by its member policies.
- Select perspective values. The job-level policy now limits the access granted by its duty-level policies to data associated with the perspective values.

Note: This defines a strategy for implementing perspective-based data security at the job level. You can implement perspective-based security at the duty level, but this is not recommended. The duty-level approach requires you to create and maintain many more roles and policies.

You may create duty roles. If so, you must create data security policies for them. Filters for these policies may specify:

- The module data applies to.
- One or more states data must exist in for the policy to grant access to it.
- An action that may be performed on data at any of the specified states.
- Optionally, other duty-level data security policies, to adopt the data access granted by those policies.
- If the role supports assessment activities, a value for an Activity perspective. This limits the policy to data needed for a particular type of assessment.

You may copy a predefined duty role to modify the copy. If so, you may copy the data security policy mapped to the source role, and map the copied policy to the copied role.

To work with data security policies, select Risk Management Tools in the home page. Among its options, select Setup and Administration. Then select the Security Configuration tab.
Create or Edit a Data Security Policy for Risk Management

To create a Risk Management data security policy:

1. Select the Create Data Security Policy action in the Manage Security page.
2. Supply a name and, optionally, description of the policy. Select a status: Active or Inactive.
3. Select Add in the Policy section. A new row appears; in it, a filter is to be defined. In its Filter Name field, enter a name.
4. In the Object field, select Perspectives if the filter is to designate a perspective value. Select Data Attributes for any other type of filter.
5. If you selected Data Attributes in the Object field, use the Attribute field to select a value appropriate for the filter you’re creating:
   - Module, for a filter that grants access to data from a specific module, either Financial Reporting Compliance or Advanced Controls Management. A module filter is typically appropriate for a policy that maps to a duty role.
   - State, for a filter that selects the state or states data must exist in for the policy to grant access to it. A state filter is typically appropriate for a policy that maps to a duty role.
   - State Action, for a filter that specifies the action that may be performed on data at the specified states. A state action filter is typically appropriate for a policy that maps to a duty role.
   - Data Policy, for a filter that selects another policy, and so adopts its data definition. A data policy filter may be appropriate for a policy that maps to a duty role or a job role.

   If you selected Perspectives in the Object field, select the name of a perspective hierarchy in the Attribute field. A perspective filter applies typically to a policy that maps to a job role. However, it’s also used in a policy that maps to a duty role that supports assessment activities.

6. If you selected Data Attributes in the Object field, select Equals or Not Equals in the Condition field.

   If you selected Perspectives in the Object field, select Equals, Not Equals, or Includes Children in the Condition field. For the last of these, the filter would designate data associated with a node you select and all its child nodes.

7. In the Value field, click the Add button, then select a value that completes the relationship definition already begun in the Attribute and Condition fields.

   For example, if your attribute is State and your condition is Equals, your value is the name of a specific state (such as In Edit). This would designate data existing at the state you have named. Or, if you select the Not Equals condition, the filter would designate data existing at all states other than the one you have named.

   Or, your attribute may be the Activity Type perspective. If your condition is Equals, the value may be the name of a node in the Activity Type hierarchy (for example, Certification). This would designate data associated with that node.

8. Select Include to allow access to the data you have defined, or Exclude to prevent access to that data.
9. Repeat these steps for each remaining filter the policy requires.

To edit a policy:

- Select a policy on the Manage Security page, then select the Edit Data Security Policy action.
- You can add or modify filters. Work with them as you would if you were creating a policy.
- You can remove filters. Select a filter, then select the Delete action.
How a Policy Applies Multiple Perspective Values

A data security policy may include filters that specify more than one perspective value:

- A filter may cite a single perspective value, but use an Includes Children condition. If so, the filter selects objects tagged with the node you select or any of its child nodes.
- You may include more than one perspective value (set off by semicolons) in a single filter. If so, OR logic applies: the filter selects objects tagged with any one of the values, or any combination of them.
- You may include more than one filter, each designating a perspective value. If so, AND logic applies: the policy grants access only to objects tagged with values from all the filters.

For example, imagine an Organization perspective has three values: Division1, Division2, and Division3. A single filter cites the Organization perspective and includes "Division1;Division2" as its value. A policy including this filter selects objects tagged with either Division1, Division2, or both. It doesn’t select an object tagged with Division3, unless that object is also tagged with Division1 or 2.

Next, imagine a Region perspective has two values, North and South. A policy includes one filter with Organization equal to Division1 and a second with Region equal to North. The policy selects only objects tagged with both the Division1 and North values.

Finally, suppose a policy contains a filter that sets the Organization value to "Division1;Division2" and a second filter that sets Region equal to North. That policy would select objects tagged with either the Division1 and North values, or with the Division2 and North values.

Map Risk Management Data Security Policies to Roles

Use the Manage Security page of Risk Management to map duty roles or job roles to data security policies. You would do this only for roles you created in the Security Console, either from scratch or by copying existing roles and editing the copies. You can’t modify the mappings of predefined roles to policies.

To select data security policies for roles:

1. In the Security Objects region of the Manage Security page, search for the role you want to map data security policies to.

   [Note:] For Risk Management to recognize a role created in the Security Console, a Security Synchronization process must run. By default it’s scheduled to run weekly. To work with a role created after the most recent run of this process, you can wait for its next scheduled run. Or, you can run it manually from the Scheduling page, available from the Scheduling tab in the Setup and Administration work area.

2. Do either of the following:
   - Click in the row for the role, then select the Edit icon.
   - Click the name of the role to open a page to view details about it. In that page, click the Edit button.
3. An Edit page opens. Use its Selected Privileges region to add or remove data security policies from the role:
   - To add policies, select the Add action. Then search for and select one or more policies in a Privileges dialog. (You may apply any number of data security policies to a role.) Click OK to complete the selection and close the dialog.
   - To remove a policy, select its row in the Selected Privileges region, then select the Delete action.

4. When you’re satisfied with your selections, click Save and Close.

Examples of Data Security Policy Mappings to Roles

Under certain circumstances, you may map a single data security policy to a given role. Under other circumstances, you may map multiple policies to a role. You may make multiple copies of a role, each providing the same functional access, so you can map different data security policies to them.

In the following examples, assume that a company has two business units. One is for operations in Los Angeles, and the other is for operations in New York.

Map Single Policies to Roles

David Chetley handles control management for the Los Angeles business unit, and Neil Sturbush does the same work for the New York business unit. Although both need the same functional access, each must be restricted to data appropriate for his business unit.

To assign distinct sets of data access to a single set of functional rights, you might:

- Begin with a job role that incorporates the functional access required for managing controls. Make two copies of the job role, one for each business unit. One might be called ControlManagerLA, and the other ControlManagerNY.
- Create an Organization perspective hierarchy. It maps the structure of the company, and so contains nodes that represent the business units. These nodes are called BU_LA and BU_NY.
- Create two data security policies, one for each business unit. They might be largely alike, containing filters that select the policies mapped to duty roles that form the hierarchy of the job-role copies. But one, called LAControlPolicy, would contain a perspective filter that selects the BU_LA value. The other, NYControlPolicy, would contain a perspective filter that selects the BU_NY value.
- Map LAControlPolicy to the ControlManagerLA job role, and assign it to David Chetley. Map NYControlPolicy to the ControlManagerNY job role, and assign it to Neil Sturbush.

Map Multiple Policies to a Role

Barry Campbell oversees the work of David Chetley and Neil Sturbush, and so needs access to data for both business units. To grant that access, you might make another copy of the base job role, called ControlManagerAll. You would then map both the LAControlPolicy and NYControlPolicy data security policies to this role, and assign it to Barry Campbell.
What happens if I edit roles that are mapped to Risk Management data security policies?

If you edit a role in Applications Security, there's no effect on its mappings to data security policies in Risk Management. (However, you will want to consider whether the mapping of a role to a data security policy remains appropriate after the role changes.)

If you delete a role in Applications Security, its mappings to data security policies are removed in Risk Management. The data security policies are unchanged, and you can map them to other roles.
Glossary

**data security policy**
A set of filters that select data. The policy is mapped to a duty role or to a job role. A user assigned one of these roles has access to data defined by the mapped policy, and can apply functionality defined by the role to that data.

**duty role**
A grant of access to privileges required to complete a specific task, or a set of related tasks.

**job role**
A grant of access to duties required to complete a broad range of tasks. You can assign job roles to users. In combination, the job roles assigned to a person encompass all he or she’s hired to do.

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

**privilege**
A specific feature the application can make available to users.

**role hierarchy**
A definition of parent-child relationships among roles. A parent role inherits functional access from the child roles in its hierarchy. For example, the hierarchy of a job role may include duty roles, and the hierarchy of a duty role may include more narrowly focused duty roles.