Oracle Fusion Cloud HCM

Securing HCM Questions and Answers

fa-latest

Oracle Fusion Cloud HCM
Securing HCM Questions and Answers

fa-latest

G30219-07

Author: Prashanth Rayakar

Contents

Get Help

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

Get Help in the Applications

Some application pages have help icons to give you access to contextual help. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. If the page has contextual help, help icons will appear.

Get 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*.

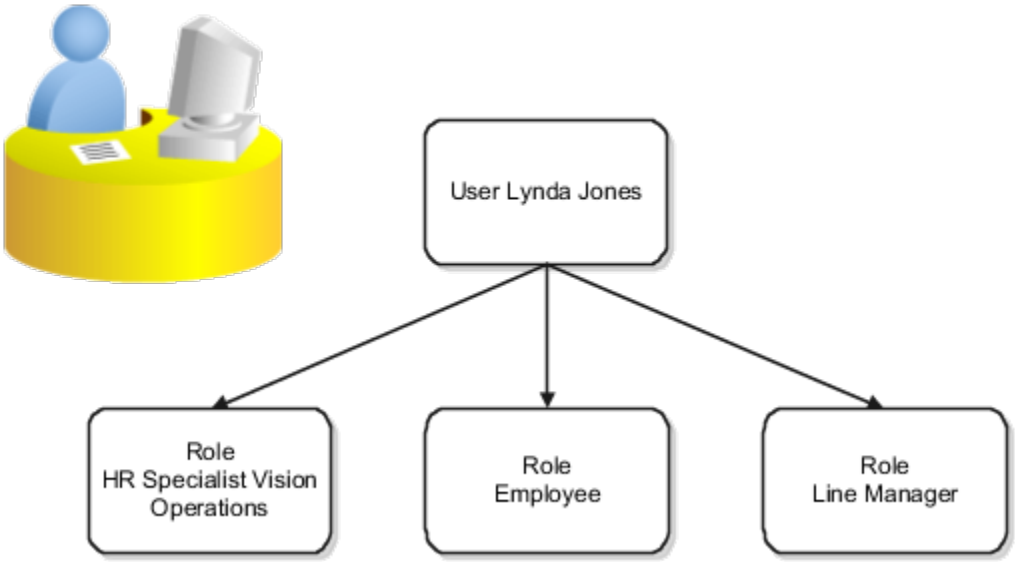
Thanks for helping us improve our user assistance!

1 Securing HCM Questions and Answers

What's role-based security?

In Oracle Fusion Applications, users have roles through which they gain access to functions and data. Users can have any number of roles.

In this figure, user Lynda Jones has three roles.



When Lynda signs in to Oracle Human Capital Management Cloud (Oracle HCM Cloud), she doesn't have to select a role. These roles are active concurrently.

The functions and data that Lynda can access are determined by this combination of roles.

- As an employee, Lynda can access employee functions and data.
- As a line manager, Lynda can access line-manager functions and data.
- As a human resource specialist (HR specialist), Lynda can access HR specialist functions and data for Vision Operations.

Role-Based Access Control

Role-based security in Oracle Fusion Applications controls who can do what on which data.

This table summarizes role-based access.

Component	Description
Who	Is a role assigned to a user
What	Is a function that users with the role can perform

Component	Description
Which Data	Is the set of data that users with the role can access when performing the function

This table provides some examples of role-based access.

Who	What	Which Data
Line managers	Can create performance documents	For workers in their reporting hierarchies
Employees	Can view payslips	For themselves
Payroll managers	Can report payroll balances	For specified payrolls
HR specialists	Can transfer workers	For workers in specified organizations

Which are the predefined roles in HCM?

Many job and abstract roles are predefined in Human Capital Management Cloud (HCM Cloud).

The predefined HCM job roles are:

- Benefits Administrator
- Benefits Manager
- Benefits Specialist
- Cash Manager
- Compensation Administrator
- Compensation Analyst
- Compensation Manager
- Compensation Specialist
- Corporate Social Responsibility Manager
- Employee Development Manager
- Employee Wellness Manager
- Environment, Health, and Safety Manager
- Human Capital Management Application Administrator
- Human Capital Management Integration Specialist
- Human Resource Analyst
- Human Resource Help Desk Administrator

- Human Resource Help Desk Agent
- Human Resource Help Desk Manager
- Human Resource Manager
- Human Resource Specialist
- IT Auditor
- Knowledge Author HCM
- Knowledge Search HCM
- Learning Specialist
- Payroll Administrator
- Payroll Manager
- Recruiter
- Recruiting Administrator
- Time and Labor Administrator
- Time and Labor Manager

The predefined HCM abstract roles are:

- Contingent Worker
- Employee
- Executive Manager
- Hiring Manager
- Job Application Identity for Recruiting
- Line Manager
- Pending Worker

You can find a brief summary of these roles documented in the guide *Security Reference for HCM*.

These predefined job and abstract roles are part of the Oracle HCM Cloud security reference implementation. The security reference implementation is a predefined set of security definitions that you can use as supplied.

Also included in the security reference implementation are roles that are common to all Oracle Fusion applications, such as:

- Application Implementation Consultant
- IT Security Manager

You can include the predefined roles in HCM data roles, for example. Typically, you assign abstract roles, such as Employee and Line Manager, directly to users.

Which are the role types in HCM Cloud?

HCM Cloud defines five types of roles, namely data roles, abstract roles, job roles, aggregate privileges, and duty roles.

Data Roles

Data roles combine a worker's job and the data that users with the job must access. For example, the HCM data role Country Human Resource Specialist combines a job (human resource specialist) with a data scope (country). You define the data scope of a data role in one or more HCM security profiles. HCM data roles aren't part of the security reference implementation. You define all HCM data roles locally and assign them directly to users.

Abstract Roles

Abstract roles represent a worker's role in the enterprise independently of the job that you hire the worker to do. The three main abstract roles predefined in HCM Cloud are:

- Employee (ORA_PER_EMPLOYEE_ABSTRACT)
- Contingent Worker (ORA_PER_CONTINGENT_WORKER_ABSTRACT)
- Line Manager (ORA_PER_LINE_MANAGER_ABSTRACT)

You can also create abstract roles. All workers are likely to have at least one abstract role. Their abstract roles enable users to access standard functions, such as managing their own information and searching the worker directory. You assign abstract roles directly to users.

Job Roles

Job roles represent the job that you hire a worker to perform. Human Resource Analyst and Payroll Manager are examples of predefined job roles. You can also create job roles. Typically, you include job roles in data roles and assign those data roles to users. The IT Security Manager and Application Implementation Consultant predefined job roles are exceptions to this general rule because they're not considered HCM job roles. Also, you don't define their data scope in HCM security profiles.

Aggregate Privileges

Aggregate privileges combine the functional privilege for an individual task or duty with the relevant data security policies. The functional privileges that aggregate privileges provide might grant access to task flows, application pages, work areas, reports, batch programs, and so on. Aggregate privileges don't inherit other roles. All aggregate privileges are predefined, and you can't edit them. Although you can't create aggregate privileges, you can include the predefined aggregate privileges in custom job, abstract, and duty roles. You don't assign aggregate privileges directly to users.

Duty Roles

Each predefined duty role represents a logical grouping of privileges that you might want to copy and edit. Duty roles differ from aggregate privileges as follows:

- They include multiple function security privileges.
- They can inherit aggregate privileges and other duty roles.
- You can create duty roles.

Job and abstract roles might inherit duty roles either directly or indirectly. You can include predefined and custom duty roles in custom job and abstract roles. You don't assign duty roles directly to users.

What's role inheritance?

When you assign data and abstract roles to users, they inherit all the data and function security associated with those roles. You can explore the complete structure of a job or an abstract role on the Security Console.

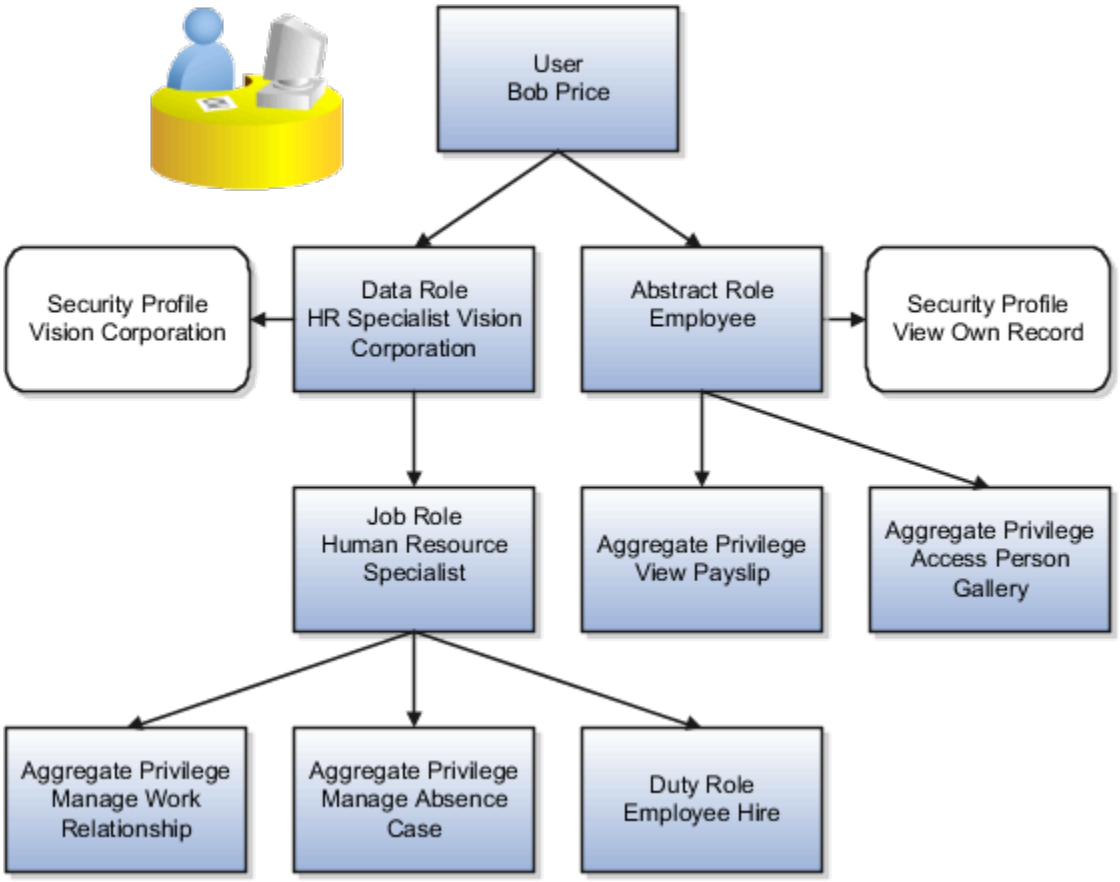
Each role is a hierarchy of other roles:

- HCM data roles inherit job roles.
- Job and abstract roles inherit many aggregate privileges. They might also inherit a few duty roles.

  In addition to aggregate privileges and duty roles, job and abstract roles are granted many function security privileges and data security policies directly.
- Duty roles can inherit other duty roles and aggregate privileges.

Role Inheritance Example

This example shows how roles are inherited. The figure shows a few representative aggregate privileges and a single duty role. In reality, job and abstract roles inherit many aggregate privileges. Any duty roles that they inherit might themselves inherit duty roles and aggregate privileges.



In this example, user Bob Price has two roles:

- HR Specialist Vision Corporation, a data role
- Employee, an abstract role

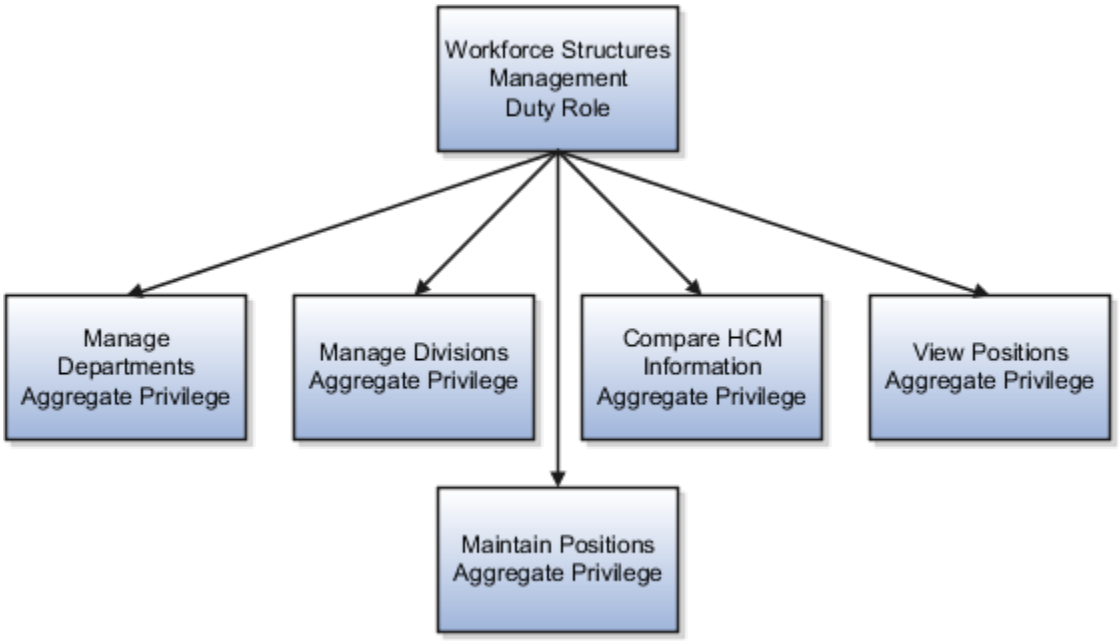
This table describes the two roles.

Role	Description
HR Specialist Vision Corporation	Inherits the job role Human Resource Specialist. This role inherits the aggregate privileges and duty roles that provide access to the tasks and functions that a human resource specialist performs. The security profile assigned to the data role provides access to secured data for the role.
Employee	Inherits the aggregate privileges and duty roles that provide access to all tasks and functions, unrelated to a specific job, that every employee performs. The security profile assigned to the abstract role provides access to secured data for the role.

What are the components of a duty role?

This topic describes the components of a typical duty role. You must understand how duty roles are constructed if you plan to create duty roles, for example.

Function security privileges and data security policies are granted to duty roles. Duty roles might also inherit aggregate privileges and other duty roles. For example, the Workforce Structures Management duty role has the structure shown in this figure.



In addition to its aggregate privileges, the Workforce Structures Management duty role is granted many function security privileges and data security policies.

Data Security Policies

Many data security policies are granted directly to the Workforce Structures Management duty role, including Manage Location, Manage Assignment Grade, and Manage HR Job. It also acquires data security policies indirectly, from its aggregate privileges.

Each data security policy combines:

- The role to which the data security policy is granted. The role can be a duty role, such as Workforce Structures Management, job role, abstract role, or aggregate privilege.
- A business object, such as assignment grade, that's being accessed. The data security policy identifies this resource by its table name, which is PER_GRADES_F for assignment grade.
- The condition, if any, that controls access to specific instances of the business object. Conditions are usually specified for resources that you secure using HCM security profiles. Otherwise, business object instances can be identified by key values. For example, a user with the Workforce Structures Management duty role can manage all grades in the enterprise.
- A data security privilege that defines permitted actions on the data. For example, Manage Assignment Grade is a data security privilege.

Function Security Privileges

Many function security privileges are granted directly to the Workforce Structures Management duty role, including Manage Location, Manage Assignment Grade, and Manage HR Job. It also acquires function security privileges indirectly, from its aggregate privileges.

Each function security privilege secures the code resources that make up the relevant pages, such as the Manage Grades and Manage Locations pages. Some user interfaces aren't subject to data security, so some function security privileges have no equivalent data security policy.

Predefined Duty Roles

The predefined duty roles represent logical groupings of privileges that you might want to manage as a group. They also represent real-world groups of tasks. For example, the predefined Human Resource Specialist job role inherits the Workforce Structures Management duty role. To create a Human Resource Specialist job role with no access to workforce structures, you'd:

1. Copy the predefined job role.
2. Remove the Workforce Structures Management duty role from the copy.

What are aggregate privileges?

Aggregate privileges are a type of role. Each aggregate privilege combines a single function security privilege with related data security policies. All aggregate privileges are predefined. This topic describes how aggregate privileges are named and used.

Aggregate Privilege Names

An aggregate privilege takes its name from the function security privilege that it includes. For example, the Promote Worker aggregate privilege includes the Promote Worker function security privilege.

Aggregate Privileges in the Role Hierarchy

Job roles and abstract roles inherit aggregate privileges directly. Duty roles might also inherit aggregate privileges. However, aggregate privileges can't inherit other roles of any type. As most function and data security in job and abstract roles is provided by aggregate privileges, the role hierarchy has few levels. This flat hierarchy is easy to manage.

Use of Aggregate Privileges in Custom Roles

You can include aggregate privileges in the role hierarchy of a custom role. Treat aggregate privileges as role building blocks.

Creating, Editing, or Copying Aggregate Privileges

You can't create, edit, or copy aggregate privileges, nor can you grant the privileges from an aggregate privilege to another role. The purpose of an aggregate privilege is to grant a function security privilege only with a specific data security policy. Therefore, you must use the aggregate privilege as a single entity.

If you copy a job or abstract role, then the source role's aggregate privileges are never copied. Instead, role membership is added automatically to the aggregate privilege for the copied role.

What are the guidelines for configuring security?

If the predefined security reference implementation doesn't fully represent your enterprise, then you can make changes. For example, the predefined Line Manager abstract role includes compensation management privileges.

If some of your line managers don't handle compensation, then you can create a line manager role without those privileges. To create a role, you can either copy an existing role or create a role from scratch.

When you assign predefined roles and privileges as is, you're entrusting users with full access to all data and functionality. Such unrestricted access without really determining the business need might pose a security concern. Also, the assigned privileges might account for subscription consumption irrespective of whether you purchased the cloud service or not. A detailed list of all the predefined roles that impact licensing is available for reference. See the spreadsheet *Predefined Roles with Subscription Impact*.

During implementation, you evaluate the predefined roles and decide whether changes are needed. You can identify predefined roles easily by their role codes, which all have the prefix ORA_. For example, the role code of the Payroll Manager job role is ORA_PAY_PAYROLL_MANAGER_JOB. All predefined roles are granted many function security privileges and data security policies. They also inherit aggregate privileges and duty roles. The recommended process is to always make a copy of the predefined role, remove the privileges you don't need, and assign only the required privileges. That way, you'll hit the subscription usage in a controlled way, based on your business need. Creating roles from scratch is most successful when the role has very few privileges and you can identify them easily.

Note: Updates to Fusion Applications might also include changes to certain predefined roles. Check the release readiness documents for your product area to know if there are any updates to the predefined roles that are in use. If you find changes that are relevant, incorporate the same changes to your custom role. This will remain an ongoing maintenance activity for the custom roles.

Missing Enterprise Jobs

If jobs exist in your enterprise that aren't represented in the security reference implementation, then you can create your own job roles. Add aggregate privileges and duty roles to custom job roles, as appropriate.

Predefined Roles with Different Privileges

If the privileges for a predefined job role don't match the corresponding job in your enterprise, then you can create your own role. If you copy the predefined role, then you can edit the copy. You can add or remove aggregate privileges, duty roles, function security privileges, and data security policies, as appropriate.

Predefined Roles with Missing Privileges

If the privileges for a job aren't defined in the security reference implementation, then you can create your own duty roles. However, the typical implementation doesn't use custom duty roles. You can't create aggregate privileges.

What are the options for reviewing predefined roles?

This topic describes some ways in which you can access information about predefined roles. This information can help you to identify which users need each role and whether to make any changes before provisioning roles.

The Security Console

On the Security Console, you can:

- Review the role hierarchy of any job, abstract, or duty role.
- Extract the role hierarchy to a spreadsheet.
- Identify the function security privileges and data security policies granted to a role.
- Compare roles to identify differences.

Tip: The role codes of all predefined roles have the prefix **ORA_**.

Reports

You can run the User and Role Access Audit Report. This XML-format report identifies the function security privileges and data security policies for a specified role, all roles, a specified user, or all users.

The Security Reference Manuals

Two manuals describe the security reference implementation for Oracle HCM Cloud users:

- The Security Reference for Oracle Applications Cloud includes descriptions of all predefined security data that's common to Oracle Fusion Applications.
- The Security Reference for Oracle HCM Cloud includes descriptions of all predefined security data for Oracle HCM Cloud.

Both manuals contain a section for each predefined job and abstract role. For each role, you can review its:

- Duty roles and aggregate privileges
- Role hierarchy
- Function security privileges
- Data security policies

You can access the security reference manuals on **docs.oracle.com**.

What's the Security Console?

Security Console is an easy-to-use administrative work area where you perform most security-management tasks.

Use the Security Console to:

- Review role hierarchies and role analytics.

  > **Note:** You can review HCM data roles on the Security Console. However, you must manage them on the Manage Data Roles and Security Profiles page.

- Create and manage custom job, abstract, and duty roles.
- Review the roles assigned to users.
- Create and manage implementation users and their roles.
- Compare roles.
- Simulate the Navigator for a user or role.
- Create and manage user categories.
- Manage the default format of user names and the password policy for each user category.
- Manage notifications for user-lifecycle events, such as password expiration, for each user category.
- Manage PGP and X.509 certificates for data encryption and decryption.
- Set up federation, and sync user and role information between Applications Security and Microsoft Active Directory, if appropriate.

Accessing the Security Console

You must have the IT Security Manager job role to access the Security Console. You open the Security Console by selecting the Security Console work area. These tasks, performed in the Setup and Maintenance work area, also open the Security Console:

- Create Implementation Users
- Manage Applications Security Preferences
- Manage Duties
- Manage Job Roles
- Revoke Data Role from Implementation Users

How do I provision HCM data roles to users?

On the Create Role Mapping page, create a role mapping for the role.

Select the **Autoprovision** option to provision the role automatically to any user whose assignment matches the mapping attributes.

Select the **Requestable** option if any user whose assignment matches the mapping attributes can provision the role manually to other users.

Select the **Self-Requestable** option if any user whose assignment matches the mapping attributes can request the role.

How do I provide read-only access to users?

Read Only Mode (FND_READ_ONLY_MODE) profile option controls read-only access.

To enable read-only mode for a user:

1. In the Setup and Maintenance work area, use the **Manage Administrator Profile Values** task.
2. In the Search section of the **Manage Administrator Profile Values** page, enter **FND_READ_ONLY_MODE** in the **Profile Option Code** field and click **Search**.
3. In the FND_READ_ONLY_MODE: Profile Values section of the page, click the **New** icon.
4. In the new row of the profile values table:
    a. Set **Profile Level** to **User**.
    b. In the **User Name** field, search for and select the user.
    c. Set **Profile Value** to **Enabled** to activate read-only access for the selected user.
5. Click **Save and Close**.

When the user next signs in, a page banner reminds the user that read-only mode is in effect and no changes can be made.

Some situations in which read-only access is required are:

- A help desk representative must replicate a user's transaction without saving any changes.

- An auditor reviews application data for regulatory reasons but isn't authorized to change anything.

What happens if a person has multiple assignments or person types?

A user who can access a person record can access all of the person's assignments, regardless of the assignment type. The assignments can also be with different legal employers.

Which are the business objects and privileges securing them for defaulting and validation rules?

Business objects and privileges securing them are listed in this table:

Product Area	Referenced Business Objects	Aggregate Privilege Name and Code	Function Privilege Name and Code
Employment	Work Relationship	Read Work Relationship Business Object ORA_PER_READ_WORK_RELATIONSHIP_BO	Not Applicable
	Employment Contracts	Read Worker Contract Business Object ORA_PER_READ_WORKER_CONTRACT_BO	Not Applicable
	• Assignment • Assignment Additional Info • Assignment Grade Step • Assignment Supervisor • Assignment Work Measures	Read Worker Assignment Business Object ORA_PER_READ_WORKER_ASSIGNMENT_BO	Not Applicable
Payroll	Assigned Payroll	Read Assigned Payroll Business Object ORA_PAY_READ_ASSIGNED_PAYROLL_BO	Not Applicable
Person	Person	Read Person Business Object	Not Applicable

	ORA_PER_READ_PERSON_BO	
Person Additional Info	Read Person Additional Info Business Object ORA_PER_READ_PERSON_ADDITIONAL_INFO_BO	Not Applicable
Person Address	Read Person Address Business Object ORA_PER_READ_PERSON_ADDRESS_BO	Not Applicable
Person Citizenship	Read Person Citizenship Business Object ORA_PER_READ_PERSON_CITIZENSHIP_BO	Not Applicable
Person Driver License	Read Person Drivers License Business Object ORA_PER_READ_PERSON_DRIVERS_LICENSE_BO	Not Applicable
Person Email	Read Person Email Business Object ORA_PER_READ_PERSON_EMAIL_BO	Not Applicable
Person Image	Read Person Image Business Object ORA_PER_READ_PERSON_IMAGE_BO	Not Applicable
Person Name	Read Person Name Business Object ORA_PER_READ_PERSON_NAME_BO	Not Applicable
Person Biographical Info	Read Person Biographical Info Business Object ORA_PER_READ_PERSON_BIOGRAPHICAL_INFO_BO	Not Applicable
Person National Identifier	Read Person National Identifier Business Object ORA_PER_READ_PERSON_NATIONAL_IDENTIFIER_BO	Not Applicable
Person Legislative Info	Read Person Legislative Info Business Object ORA_PER_READ_PERSON_LEGISLATIVE_INFO_BO	Not Applicable
Person Religion	Read Person Religion Business Object ORA_PER_READ_PERSON_RELIGION_BO	Not Applicable

	Person Ethnicity	Read Person Ethnicity Business Object ORA_PER_READ_PERSON_ETHNICITY_BO	Not Applicable
	Person Disability	Read Person Disability Business Object ORA_PER_READ_PERSON_DISABILITY_BO	Not Applicable
	Person Passport	Read Person Passport Business Object ORA_PER_READ_PERSON_PASSPORT_BO	Not Applicable
	Person Phone	Read Person Phone Business Object ORA_PER_READ_PERSON_PHONE_BO	Not Applicable
	Person Other Communication	Read Person Other Communication Business Object ORA_PER_READ_PERSON_OTHER_COMMUNICATION_BO	Not Applicable
	Person Visa Permit	Read Person Visa Permit Business Object ORA_PER_READ_PERSON_VISA_PERMIT_BO	Not Applicable
	Person Contacts	Read Person Contact Business Object ORA_PER_READ_PERSON_CONTACT_BO	Not Applicable
	Person Identifiers for External Applications	Read Person Identifier for External Applications Business Object ORA_PER_READ_PERSON_IDENTIFIER_FOR_EXTERNAL_APPLICATIONS_BO	Not Applicable
Recruiting	Job Requisition	Read Job Requisition Business Object ORA_IRC_READ_JOB_REQUISITION_BO	Not Applicable
Workforce Structure	Department	Read Department Business Object ORA_PER_READ_DEPARTMENT_BO	Not Applicable
	Grade	Not Applicable	Read Assignment Grade Business Obje PER_READ_ASSIGNMENT_GRADE_BO
	Grade Ladder	Not Applicable	Read Assignment Grade Ladder Busine Object

			PER_READ_ASSIGNMENT_GRADE_LA BO
	Grade Rate	Not Applicable	Read Assignment Grade Rate Business PER_READ_ASSIGNMENT_GRADE_RA
	Job	Not Applicable	Read HR Job Business Object PER_READ_HR_JOB_BO
	Job Family	Not Applicable	Read HR Job Family Business Object PER_READ_HR_JOB_FAMILY_BO
	Location	Not Applicable	Read Location Business Object PER_READ_LOCATION_BO
	Position	Read Position Business Object ORA_PER_READ_POSITION_BO	Not Applicable
	Worker Union	Read Worker Union Business Object ORA_PER_READ_WORKER_UNION_BO	Not Applicable