Oracle Fusion Cloud ERP: Security Implementation

Oracle Financials Cloud

DURATION	MODULES	COURSE CODE
3 Days	**13 Lectures**	**—**

Course Overview

Oracle Fusion Cloud ERP: Security Implementation training teaches you how to configure and use Oracle Security. Experienced Oracle University instructors help you learn to follow the task list in Functional Setup Manager and the Security Console. You use the hands on practices to test your security setups and apply your new knowledge to solving security issues you may encounter on the job.

What You Will Learn

Introducing Security

- Course Objectives
- Course Schedule
- Lesson Objectives
- Introduction to Oracle Cloud Applications
- Oracle Cloud Applications: Product Families
- Oracle ERP Cloud: Overview
- Security Implementation Overview
- Oracle ERP Cloud Security Methodology
- Security Reference Implementation
- Security Model: Role Based Access Control
- Role-Based Access Terminology
- The Security Console
- Users
- Practice: Reviewing a User
- Job and Duty Roles
- Privileges
- Aggregate Privileges
- Resources
- Data Security Policies
- Advanced Data Security

- Practice: Reviewing a Predefined Job Role
- Practice: Reviewing a Predefined Duty Role
- Practice: Reviewing a Privilege, an Aggregate Privilege, and an Abstract Role
- Summary

Using Functional Setup Manager

- Objectives
- Functional Setup Manager Overview
- What is Functional Setup Manager?
- Functional Setup Manager Benefits
- Key Concepts
- Review Offerings and Prepare to Opt In
- Opt into Offering, Functional Areas, and Features
- Review What’s New and Opt into New Features After Upgrade
- Manage Setup Data Using Functional Areas
- Related Setup Tasks
- Tasks with Scope
- Searching for a Task
- Export and Import of Security Setup Data
- Practices and Demonstration for Using FSM
- Summary

Configuring Security Console

- Objectives
- Security Console Overview
- Accessing the Security Console
- Security Console Task List
- Using the Security Console for Roles and Users
- Using Role Analytics
- Analyze Data Security Policies by Resource
- Managing Certificates
- User Categories
- User Name Generation Rules
- Password Policies
- Notification Templates
- Add Users to User Category
- Practice: Managing User Categories
- Self-Service External Identity Provider Setup
- Performing Administration in the Security Console
- Summary

Managing Users

- Objectives
- Define User Types

- Comparing User Types
- Creating Implementation Users
- Administrator Password Management
- User Password Management: Self-Service
- User Password Changes Audit Report
- User Account Locking
- Application User Management
- User and Role-Provisioning Setup Options in HCM
- Creating Application Users
- User Details System Extract Report
- Location Based Access
- Practices for Managing Users
- Practice for Managing Users
- Summary

Configuring Roles

- Objectives
- Role Inheritance
- Upgrade-Safe Management of Factory Shipped Roles
- Role Visualization- Part1
- Role Visualization- Part2
- Search in Role Hierarchy Visualization
- Tabular Role Hierarchy View
- Copy Role
- Deep Copy
- Shallow Copy
- Copy Role Process
- Configuring Copied Roles
- Practices for Role Copying Features
- Creating a New Role
- Creating FSCM User Data Security
- FSCM Data Security Conditions for Direct Accesses
- FSCM Data Security Conditions for Derived Accesses
- Practice: Creating a New Role
- Guidance for Assigning Predefined Roles
- Processes to Align the Security Console Tables
- Demonstration: Running the ESS Processes to Align the Security Console
- Tables
- Reports that need Import User and Role Application Security Data Process to get
- Data Populated
- Practice: Running the User Role Membership Report
- Simulate Navigator Menu
- Practice: Accessing the Simulate Navigator Menu
- Role Optimization Report
- Summary

Comparing Roles

- Objectives
- Why Role Comparison?
- Difference between Function Security and Data Security
- Compare Roles Feature in Security Console
- Move Function and Data Security Policies
- Compare Users
- Remove All User’s Roles
- Practices for Comparing Roles
- Examples of Predefined Roles in Accounts Receivables
- Comparing Function Security Policies within AR Roles
- Additional Setup Privileges for AR Managers
- Additional Accounting Privileges for AR Managers
- Additional Period Closure Privileges for AR Managers
- Additional Reporting Privileges for AR Managers
- Comparing Data Security Policies within AR Roles
- Examples of Predefined Roles in Fixed Assets
- Comparing Function Security Policies within FA Roles
- Comparing Data Security Policies within FA Roles
- Examples of Predefined Roles in General Ledger
- Comparing Function Security Policies within GL Roles
- Additional Setup Privileges for General Accounting Manager
- Additional Period Closure Privileges for General Accounting Manager
- Additional ESS and Secondary Ledger Activity Privileges for General Accounting
- Manager
- Comparing Data Security Policies within GL Roles
- Examples of Predefined Roles in Accounts Payables
- Comparing Function Security Policies within AP Roles
- Comparing Function Security Policies within AP Roles: Creating Setups
- Comparing Function Security Policies within AP Roles: Period Closure
- Activities
- Comparing Function Security Policies within AP Roles: Run Reports
- Comparing Function Security Policies within AP Roles
- Comparing Data Security Policies within AP Roles
- Examples of Predefined Roles in Cash Management
- Summary

Provisioning Roles

- Objectives
- Provisioning Roles
- Automatic Role Provisioning
- Auto Provision Roles for All Users Process
- Manual Role Provisioning
- Data Access

- Manual Data Provisioning
- Automatic Data Provisioning
- Demonstration and Practices for Automatic and Manual Provisioning
- Practices for Automatic and Manual Provisioning
- Data Deprovisioning
- ERP Data Access Assignment Report
- Auditing Security
- Security Dashboard
- Practice: Accessing the Security Dashboard
- Summary

Segregating Duties

- Objectives
- Segregation of Duties
- Segregation of Duties Violations in Payables
- Segregation of Duties Compliance in Payables
- Practice: Creating and Assigning New Users for SOD
- Practice: Assigning Business Units and Data Access
- Practice: Creating Payable Transactions using the SOD Users
- Practice: Creating Online Accounting for Payables Transactions
- Practice: Viewing the OTBI SOD Payables Reports
- Segregation of Duties Violations in Receivables
- Segregation of Duties Compliance in Receivables
- SOD Compliance achieved through AR Manager Segregated Roles
- SOD Compliance achieved through AR Specialist Segregated roles
- SOD Compliance achieved through Customer Account Administrator Segregated
- Role
- Segregation of Duties Violations in Subledger Accounting
- Segregation of Duties Compliance in Subledger Accounting
- Summary

Securing Oracle Financials Applications

- Objectives
- Segment Value Security By Business Function
- Segment Value Security By Business Function – Examples
- Key Steps to Configure Segment Value Security By Business Function
- Manage Segment Value Security Rules Spreadsheet
- Segment Value Security By Business Function vs Without Business Function
- Segment Value Security Without Business Function
- Demonstration: Setting up Segment Value Security
- Practice: Defining the Segment Value Security Rules
- Demonstration: Disabling Segment Value Security
- General Ledger Security
- Data Access Set Security in General Ledger
- Cross Validation Rules in General Ledger

- Practice: Defining the Cross Validation Rules
- Payables Security
- Demonstration: Setting Up Routing for an Approval Notification
- Practice: Verifying the Approval Notification Routing
- Payables Security
- Practice: Understanding Payables Security
- Receivables Security
- Practice: Understanding Receivables Security
- Receivables Security
- Fixed Assets Security
- Practice: Understanding Fixed Assets Security
- Payments Security
- Practice: Understanding Payments Security
- Cash Management Security
- Legal Entity Based Data Access for Bank Account Setup
- Practice: Understanding Cash Management Security
- Subledger Accounting Security
- Country- Specific Features Security
- Access for Workflow Administrators
- Financial Reporting Security
- Practice: Understanding Financials Reporting Security
- Security Resources
- Summary

Securing Oracle Procurement

- Objectives
- Defining Security for Procurement Setup and Maintenance
- Procurement Role-Based Access Control Example
- Types of Security Roles
- Procurement Role Inheritance Example
- Purchase Order Creation Example: Job Roles and Associated Duty Roles
- Purchase Order Creation Example: Duty Role and Tasks
- Procurement Job and Abstract Roles
- Analytics Publisher Security: Duty Roles
- Additional Analytics Publisher Security: Duty Roles
- Self Service Procurement Additional Privileges
- Requester Data Security
- Procurement-Specific Data Security: Define Procurement Agents
- Supplier Agreement: Agent Data Security
- Purchase Order: Agent Data Security
- Analyze Spend Business Intelligence: Agent Data Security
- Practice: Securing Oracle Procurement
- Supplier Data Security
- Creating Supplier Users
- Supplier User Role Assignment

- Security Resources
- Summary

Securing Oracle Project Portfolio Management Applications

- Objectives
- Project Financial Management Security
- Define Users and Security for Project Management Setup Task Lists
- Security Model: Role Based Access Control
- Role-Based Access Control in Project Management
- Practice Overview: Creating an Implementation Administrator
- Nonproject Role needed to Access Contracts and Post Invoices
- Practice Overview: Creating a Functional User
- Project Execution Management Security
- Define Common Project Execution Options: Setup Tasks and Task Lists
- Common Project Execution Options Overview
- Project Implementation Administrator
- Practice Overview: Creating an Implementation Administrator in Project
- Execution
- User Provisioning
- Enterprise Roles
- Project Management Roles
- Defining Project Roles with Limited Actions for Managing Resources
- Practice Overview: Creating and Adding Project Roles
- Use a Single Set of Project Roles Across Your Organization
- Summary

Risk Management Functional Security

- Objectives
- Security Model: Role-Based Access Control
- Role-Based Access Control Example
- Role-Based Access Terminology
- Risk Management vs Other Fusion Applications Security
- What Does It Mean to Be Eligible vs Authorized?
- Functional Security Overview
- Roles Overview
- What Is a Privilege?
- The Security Console
- Viewing the Privileges for a Role
- Copy or Edit Risk Management Roles
- Practice Overview: Copying the Predefined Job Roles
- Assessment and Mass Edit Security Related Privileges
- Refreshing Risk Management Security Data
- Run the Retrieve Latest LDAP Changes Process
- Run the Import User and Role Application Security Data Job
- Run the Risk Management Security Synchronization Process

- Practice Overview: Running the Security Processes
- Provisioning Rules
- Autogenerate Provisioning Rules
- Reviewing the Autogenerated Rules Panel
- Create and Edit Provisioning Rules Manually
- Summary

Risk Management Data Security

- Objectives
- Risk Management Data Security Overview
- Records Affected by Data Security
- What Does It Mean to Be an Owner?
- User Assignment Groups
- Create User Assignment Groups
- Edit Existing User Assignment Groups
- Export and Import User Assignment Groups
- Importing User Assignment Groups
- Practice Overview: Creating a User Assignment Group
- Secure Records in Financial Reporting Compliance
- Authorizing Users for Financial Reporting Compliance Records
- Additional Authorizations in Financial Reporting Compliance
- Securing Financial Reporting Compliance Issues
- Securing Batch Assessments in Financial Reporting Compliance
- Securing Individual Assessments within the Batch
- Selecting Individual Users for Financial Reporting Compliance Records
- Selecting Groups for Financial Reporting Compliance Records
- Securing Records in Advanced Controls
- Business Object Security for Transaction Models and Controls
- Securing Business Objects
- Securing Controls and Their Incidents
- Securing Access Certifications
- Practice Overview: Confirm a User Has Access to Business Objects
- Mass Edit Security Assignment Tool
- Using the Mass Edit Security Assignment Tool
- Searching for Ineligible and Missing Authorizations in the Mass Edit Security
- Assignment Tool
- Summary