

Oracle Cloud Infrastructure Security Professional (2025): Hands-on Workshop

Oracle Cloud Infrastructure

DURATION

4 Days

MODULES

19 Lectures

COURSE CODE

—

Course Overview

This hands-on workshop covers Oracle Cloud Infrastructure Security Professional (2025): Hands-on Workshop. Gain practical experience through guided exercises and real-world scenarios in Oracle Cloud Infrastructure.

What You Will Learn

Module 1: Course Introduction

- Course Overview
- Course Description
- Target Audience
- Prerequisites
- Certification Exam Objectives
- Course Outline
- Skill Checks to Test Your Knowledge
- OCI Documentation: Exploring Resources
- 📄📄"Ask Your Instructor" Form
- Getting Started

Module 2: Security Fundamentals

- Shared Security Model
- Zero Trust Security
- Concept
- Principles
- Security Services Introduction
- Security Services Overview
- Object Storage Security
- Security Services Use Cases

- Security Questions
- Security Design and Controls
- Platform Security
- Physical Security: Data Center Site & Inside Data Center
- Operational Security
- Secure Connectivity
- Data and Application Protection
- Culture of Trust and Compliance

Module 3: OCI Identity and Access Management (IAM)

- Introduction to OCI IAM
- Authentication (AuthN) & Authorization (AuthZ)
- IAM Components
- Identity Domains
- What They Are
- Use Cases
- Lifecycle Management
- Creating Identity Domains (Demo Included)
- Identity Domain Types & Default Domains
- Administrator Users: Dos & Don'ts
- Managing Groups & Users
- Default Groups
- Group & User Creation (Demo Included)
- Administrator Roles
- Key Points, Types, and Demo
- IAM Policies
- Subjects Clause, Actions Clause, Placement
- Compartments
- Resource Compartments, Access, Interaction of Resources
- Movement Across Regions, Nested Compartments
- Compartment Quotas and Budgets (Demo Included)

Module 4: Advanced IAM Policies

- Policy Inheritance and Attachment (Demo Included)
- Conditional Policies & Examples (Demo Included)
- Enforcing Least Privilege: Advanced Policies
- Permissions & Network Sources (Demo Included)
- Tag-Based Access Control (Demo Included)
- Dynamic Groups & Policies (Demo and Scenarios)
- Optimizing IAM Policies
- Eliminating Duplicates
- Consolidating Membership
- Combining Policy Statements
- Pattern-Based Optimization
- Object-Level Granular Access Control for OCI Object Storage

- Organization Management
- Benefits, Governance Rules, and Demo

Module 5: Securing Access using IAM

- Password Policies
- Types and Demo
- Multi-Factor Authentication (MFA)
- Enablement and Demo
- Adaptive Security
- Risk Providers
- Passwordless Authentication
- Network Perimeter Security (Demo)
- OCI IAM Reports
- Types and Accessing Reports
- Notifications & Branding

Module 6: Oracle Access Governance Overview

- Course Overview & Introduction to Access Governance
- Why Access Governance is Important
- Oracle Access Governance Features and Benefits
- Identity Governance and Administration (IGA)
- Challenges with Ungoverned Identities
- Access Control Challenges
- Evolving Requirements
- IGA Capabilities
- Access Governance Architecture
- Functional and Physical Views
- Core Functional Areas
- Roles, Application Roles, and User Access Model
- Demo: Creating Access Governance Service Instance & Roles

Module 7: Identity Orchestration

- Core Functional Areas of Access Governance
- Identity Orchestration in Hybrid & Multicloud Environments
- Identity Provisioning and Reconciliation
- Integration with Authoritative Sources
- Connected Systems and Integration Architecture
- OIG and OCI Integration Examples
- Codeless Integration: Design Goals & Demo
- Integration with OCI IAM
- Custom Identity Attributes & Identity Marking
- Workforce & Consumer Users
- Access Control Mechanisms
- Access Requests & Approval Workflows
- Identity Collections (Demo)

- Access Bundles (Demo)

Role-Based Access Control (RBAC) & Policy-Based Access Control (PBAC) (Demos Included)

Module 8: Governance and Compliance

- Core Functional Areas in Governance and Compliance
- Enforcing Compliance through Access Reviews
- Campaigns and Access Reviews
- Policy Reviews & Event-Based Reviews
- Delegation in Access Governance (Demo Included)
- Identity Intelligence
- Key Capabilities
- Prescriptive Analytics and Insights
- Dashboards
- Enterprise-wide Access
- Identity Correlation
- Remediation (Demos Included)

Module 9: Virtual Cloud Network (VCN) Security

- OCI Architecture Overview
- Virtual Cloud Network (VCN) Concepts
- CIDR Notation & Examples
- IP Address Ranges, Subnets
- IAM Policies for Networking Admins/Users
- Compartments & NSGs
- Nuances of Different Verbs
- Demo: Public and Private Subnets
- VCN Security
- Security List (SL) & Network Security Groups (NSG)
- Stateful and Stateless Security Rules
- Bastion Host (Demos Included)
- Zero Trust Packet Routing (ZPR)
- Concept, Benefits, Setup, Use Case
- VCN Connectivity
- Connectivity Options
- Site-to-Site VPN (IPSec) & Configuration Workflow
- FastConnect Use Cases & Connectivity Providers
- IPSec VPN and FastConnect Summary

Module 10: Load Balancer Concepts

- Load Balancer Primer
- OCI Load Balancing Service
- OCI Flexible Load Balancer
- Fixed to Flexible Load Balancer
- HTTP/2 Support

- Public and Private Load Balancers
- Public Load Balancer (Regional Subnets & AD-Specific Subnets)
- Private Load Balancer (Using Regional & AD-Specific Subnets)
- Load Balancer Policies and Health Checks
- Load Balancing Policies
- Health Check
- SSL Handling
- LB with SSL Not Enabled
- Generate Private Key and CSR
- Generate Self-Signed Certificate
- Add Certificate to LB & Create Listener on Port 443
- SSL Termination Enabled for LB (Demo Included)
- High Availability with IP Hash Load Balancing
- Troubleshoot Load Balancer Critical Health Check Errors
- Certificates Overview
- TLS and Mutual TLS Connections
- Certificate Authority (CA) & Chain of Trust
- Types of Certificates, Certificate Pain Points
- OCI Certificates Service
- Lifecycle Management Features
- Use Cases: Public, Private, mTLS, Code Signing
- Demo: OCI Certificates

Module 11: OCI Network Firewall

- Why We Need a Firewall
- OCI Network Firewall Overview
- Deployment and Workflow
- Use Cases
- Perimeter Security
- Intrusion Detection and Prevention
- Selective Access to Oracle Services Network (OSN)
- Application Segmentation and Zero-Trust
- Network Firewall Policies
- Building Rules: Create Policy Workflow
- Policy Components
- Demo: OCI Certificates & Scenario

Module 12: Securing Applications in the Cloud

- Part 1: Objectives & Multiple Layers of Defense
- Web Application Firewall (WAF)
- OCI WAF Overview & Architecture
- WAF Points of Presence (PoPs)
- Use Cases
- OWASP Rules in OCI WAF
- Part 2: WAF Service Components

- Origin Management
- Protection Rules
- Access Control
- Bot Management
- Caching Rules
- Threat Intelligence
- Shared Responsibility Model
- Benefits
- Required IAM Policies
- Getting Started with WAF: Prerequisites & Workflow

Demos: Load Balancer and WAF Policy, Creating WAF Policy, Enabling Protection Rules, Bot Management, Adding Access Control Rules

Module 13: Compute Security Best Practices

- Compute Security Recommendations
- Shielded Instances
- OCI Bastion Service
- Session Types: Managed SSH, Port Forward, Dynamic Port Forward
- OCI Bastion Details
- Required IAM Policies
- Demos: Manage Bastion, Port Forwarding
- Oracle OS Management Hub (OSMH)
- Challenges of IT Administrator
- Service Architecture & Dashboard
- Patch Updates: Simplify and Automate
- Supported Platforms & OCI IAM Policies
- Management Station & Lifecycle Environments
- Dedicated Virtual Machine Hosts
- Example Scenarios, Shapes, and Limitations

Module 14: OCI Vulnerability Scanning Service (VSS)

- Overview of OCI Vulnerability Scanning Service
- Setting up VSS
- Scanning Reports
- Cloud Guard Integration

Demos: Vulnerability Scanning, Cloud Guard Integration, Container Image Scanning

Module 15: OCI Key Management Service (KMS)

- OCI Encryption Options & KMS Portfolio
- Choosing the Right OCI KMS Offering
- Encryption Basics: At Rest, In-Transit, Symmetric, Asymmetric
- Hardware Security Module (HSM)
- Vault Introduction and OCI Vault
- Vaults, Keys, Master/Data Encryption Keys
- Key Management: Protection Modes, Wrapping, Rotating, Import/Export

- Demo: Encryption and Decryption of Data with Vault
- OCI Services Integration with Vault
- Oracle-Managed vs Customer-Managed Keys
- Object Storage Integration
- Backup, Restore, Cross-Region Replication
- Secrets Management
- Secret Rules
- Demos: Automate Secret Generation & Retrieve Secret using Instance Principal
- OCI Dedicated KMS
- Architecture, Workflow, Use Cases, Benefits
- OCI External KMS
- Overview, How it Works, Onboarding, Vaults, Key References, Use Cases

Module 16: Oracle Database Security

- Objectives & Data Vulnerability
- Database Security in OCI
- Controlled Access & Safeguarding Databases
- Data Encryption
- Database Patching
- Security Assessment
- Autonomous Database (ADB) Security
- Oracle Data Safe
- Introduction & Features
- Security Assessment
- User Assessment
- Activity Auditing
- Data Discovery & Data Masking
- Architecture & Administration
- Target Database Connectivity: Public, Private Endpoints, On-Prem Connectors

Module 17: Cloud Security Posture Management (CSPM)

- Overview & Problem Statement
- CSPM Capabilities, Outcomes, and Benefits
- DevSecOps Integration
- Cloud Guard Introduction
- Supported Services & CIS OCI Foundations Benchmark
- Reporting Region
- Demo: Enable Cloud Guard
- Cloud Guard Concepts
- Targets, Detectors, Detector Rules & Recipes
- Problems, Responders, Responder Rules & Recipes
- Problem Processing & Managed Lists
- Notifications & Integration with Events Service
- Demos: Cloud Guard & Notifications

Module 18: OCI Threat Intelligence Service

- Threat Intelligence Overview
- Two Pillars of Threat Detection
- OCI Threat Intelligence Service & Concepts
- Demo: Threat Indicator Database
- Cloud Guard Threat Detector Integration
- Sighting Type Reference & Threat Detection Benefits
- Security Zones & Security Advisor
- Concepts, Policies
- Demos: Security Zones & Custom Security Zones

Module 19: Managing Security Operations

- Security Priorities & Observability Overview
- Monitoring Service
- Capabilities, Workflow, Demo
- Logging Service
- Concepts, Log Groups, Types, Searching Logs
- Audit Logs & IAM Policies
- Demos: Logging Service, Audit Events
- Ingesting Logs for Analytics
- Sources: Compute, Object Storage, OCI Cloud Services, On-Demand Upload
- Service Connector & Configuration Parameters
- Logging Analytics
- Insights, Architecture, Storage, Log Archiving, Log Explorer
- Dashboards, OCI Audit Analysis, Log Clustering
- Audit Service
- Audit Log Viewing, IAM Policies
- Demo: Logging Analytics with Management Agent
- Notifications & Events Service
- Overview, Creating Topics, Rule Actions, Event Metrics
- Demo: Notifications and Events Service