Oracle Cloud Infrastructure Security Professional

Course Duration: 32 Hours **Course code: 1Z0-1104-25**

1. Course Overview

This course provides comprehensive training on securing Oracle Cloud Infrastructure (OCI) environments. Participants will learn to implement identity and access management, data protection, network security, monitoring, and compliance strategies. The course emphasizes practical security operations in OCI to prepare participants for professional-level security responsibilities.

2. What you'll learn?

By the end of the course, participants will be able to:

- Understand Oracle Cloud Infrastructure security architecture
- Implement identity and access management policies
- Configure network security, including firewalls and virtual cloud networks
- Secure storage and database services
- Monitor security events and perform incident response
- Apply compliance frameworks and governance controls
- Use OCI security tools such as Cloud Guard, Security Zones, and Audit

3. Target Audience

- Cloud security engineers and administrators
- IT professionals responsible for securing OCI environments
- Architects and compliance officers implementing OCI security controls

4. Pre-Requisites

- Basic understanding of Oracle Cloud Infrastructure services
- Familiarity with networking, databases, and operating systems
- Knowledge of cloud security concepts

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

5. Course content

Module 1: Course Introduction

- Introduction to the course
- Course objectives and expected outcomes

Module 2: OCI Security Overview

- OCI security principles and shared responsibility model
- OCI architecture and key security components
- Common security threats and best practices

Module 3: Identity and Access Management (IAM)

- Users, groups, and compartments
- Policies and permission management
- Federation and single sign-on

Module 4: Network Security in OCI

- Virtual Cloud Networks (VCN) and subnets
- Security lists, network security groups, and firewalls
- VPNs, FastConnect, and private connectivity

Module 5: Data Security and Encryption

- Securing object storage and databases
- Encryption at rest and in transit
- Key management with OCI Vault

Module 6: Monitoring and Logging

- Configuring audit logs and monitoring
- Using OCI Logging and Metrics
- Setting up alerts and notifications

Module 7: Threat Detection and Response

- Introduction to OCI Cloud Guard

- Security Zones and automated protections
- Incident response and remediation workflows

Module 8: Compliance and Governance

- Understanding compliance frameworks (ISO, GDPR, SOC)
- Configuring policies for regulatory compliance
- Security assessments and reporting

Module 9: Advanced Security Features

- Identity and security federation
- Security for compute, Kubernetes, and serverless workloads
- Best practices for multi-cloud and hybrid environments

Module 10: Hands-On Labs

- Implementing IAM policies and compartments
- Configuring network security and firewalls
- Monitoring security events and responding to incidents
- Securing storage and databases

Module 11: Summary and Next Steps

- Key takeaways and review
- Preparing for OCI Security Professional responsibilities
- References for further learning