



ORACLE

Oracle Cloud Infrastructure Security

Oracle Corporation
Feb 2020

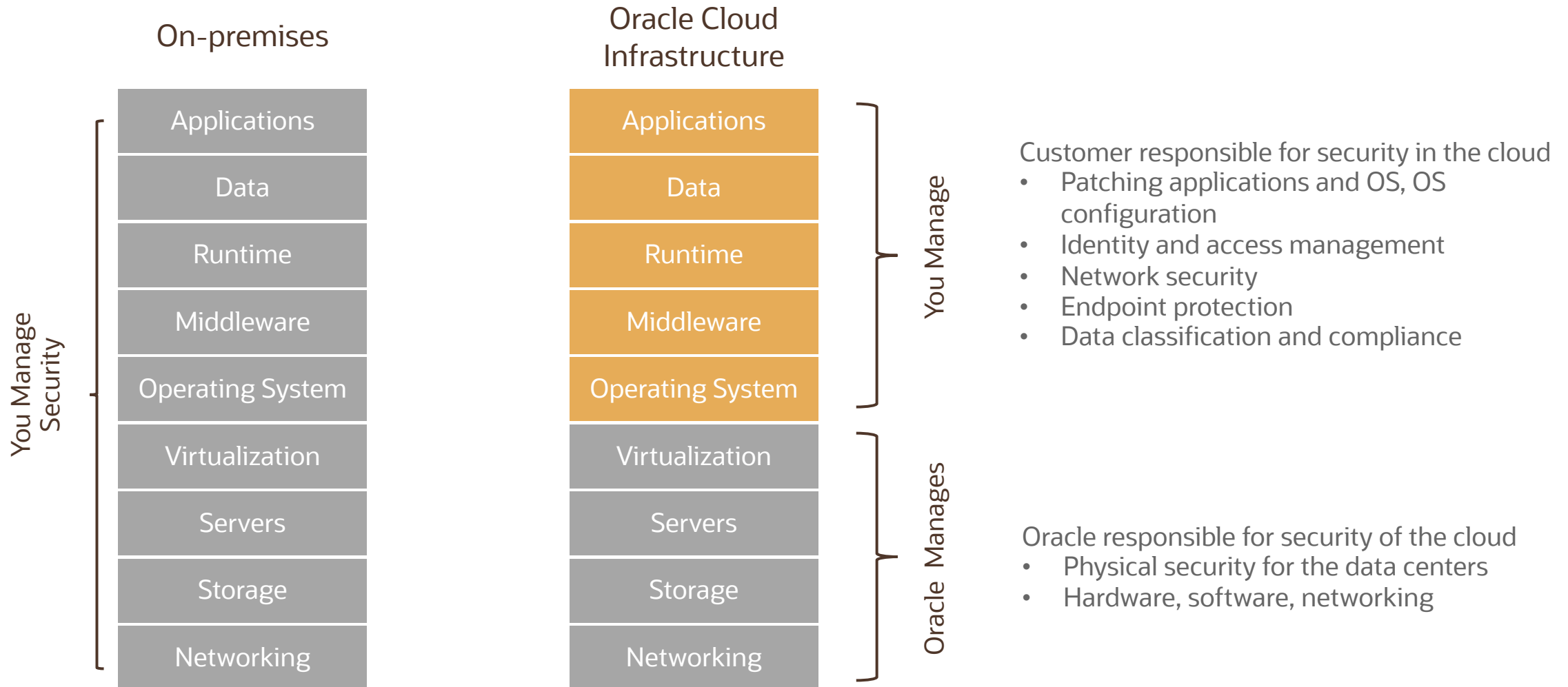
Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Agenda

Shared Security Model
Security services
Identity and Access Management
Data protection
OS and workload isolation
Infrastructure protection

Shared Security Model

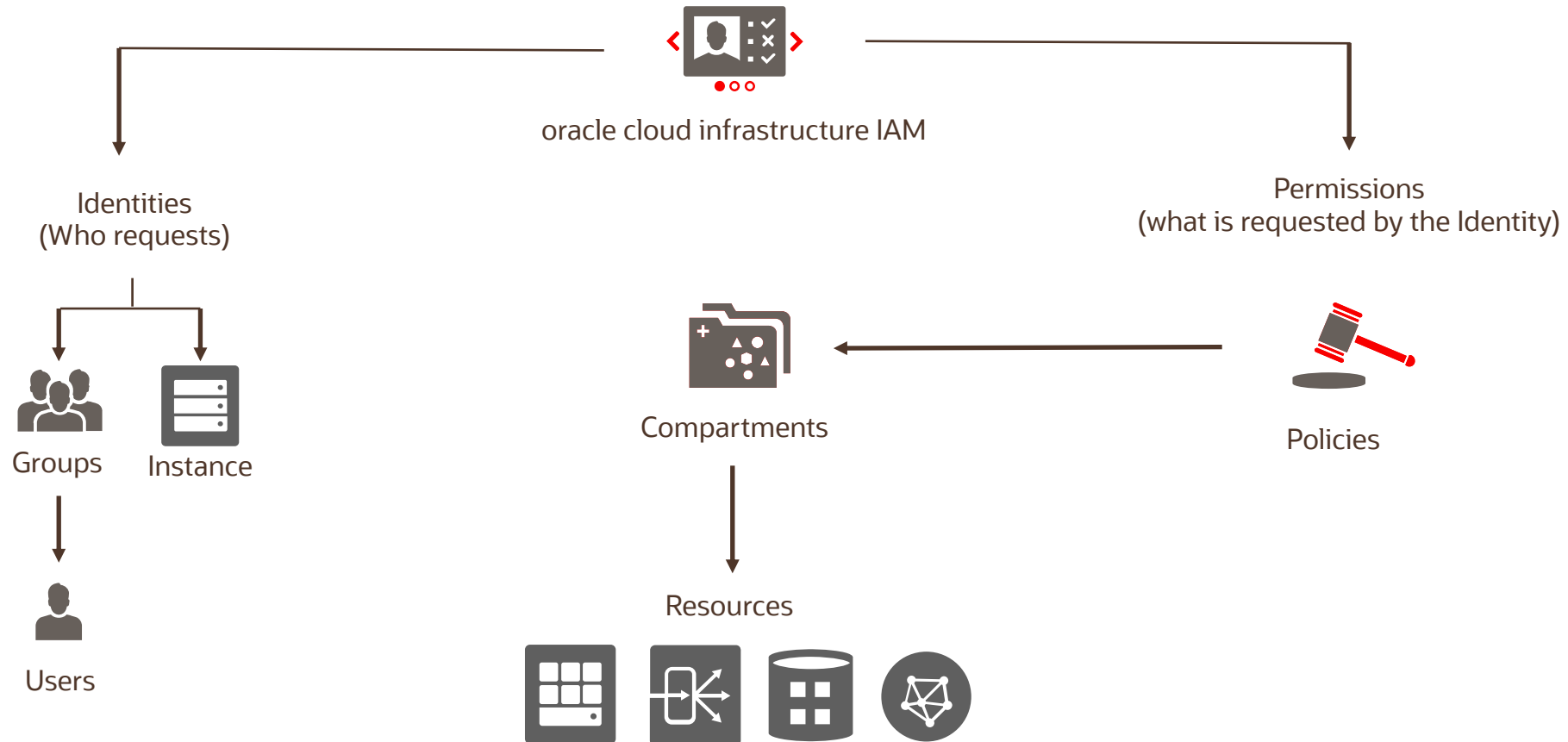


Security Services

•

	Use case	Service
Identity and Access Management	Manage user access and policies	Oracle Cloud Infrastructure IAM
	Manage multi-factor authentication	MFA
	Single sign-on to identity providers	Federation
	Encryption for data at rest, in-transit	Storage and DB services
Data Protection	Discover, classify and protect your data	Data Safe
	Hardware based key storage	Key Management
	Centralized key management	Key Management
OS and workload management	Patch Management	OS Management service
	Workload isolation	Bare Metal, Dedicated VM Hosts
Infrastructure Protection	Network security controls	VCN NSG, SL
	Filter Malicious web traffic	Web Application Firewall
	DDoS Protection	In-built

Identity and Access Management



Multi-factor Authentication (MFA)



Multi-factor authentication (MFA) is a method of authentication that requires the use of more than one factor to verify a user's identity. Examples of authentication factors are a password (something you know) and a device (something you have)

Federation

- Enterprises use an identity provider (IdP) to manage user login/passwords and to authentications
- When someone in your company wants to use oracle cloud infrastructure console, they must sign in with a user login and password.
- Your administrators can federate with a supported IdP so that each employee can use an existing login and password (and not create a new set to use oracle cloud infrastructure)
- Federated users choose which IdP to use for sign-in, and then they're redirected to that IdP's sign-in experience for authentication
- After entering their login and password, they are authenticated by the IdP and redirected to the oracle cloud infrastructure Console

Signing in to cloud tenant:
ociobenablement

[Change tenant](#)

Single Sign-On (SSO)

We have detected that your tenancy has been federated to another Identity Provider.

Select your Identity Provider below.

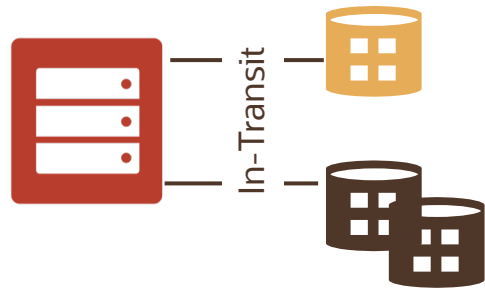
IDENTITY PROVIDER

identitycloudservice ▼

Continue

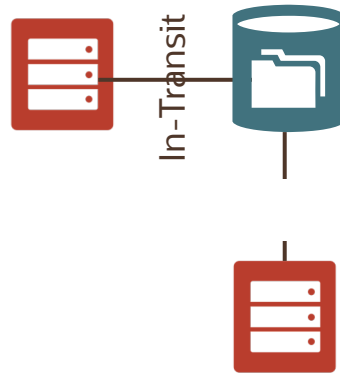
Data Protection

Block Volume



- Data encrypted at-rest
- Data encrypted in-transit
- Bring Your Own Keys

File Storage



- Data encrypted at-rest
- Data encrypted in-transit
- Bring Your Own Keys

Object Storage



- Data encrypted at-rest
- Bring Your Own Keys
- Private Buckets, Pre-authenticated Requests

Database



- Transparent Data Encryption
- Data Safe
- Data Vault

Key Management

- Managed service that enables you to encrypt your data using keys that you control
- Key Management provides you with
 - Centralized key management capabilities
 - Highly available, durable, and secure key storage in hardware security modules (HSMs)*
 - Integration with select Oracle Cloud Infrastructure services
- Uses HSMs that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification
- HSM hardware is tamper-evident, has physical safeguards for tamper-resistance, requires identity-based authentication, and deletes keys from the device when it detects tampering

* A HSM is a physical computing device that safeguards digital keys and provides crypto processing

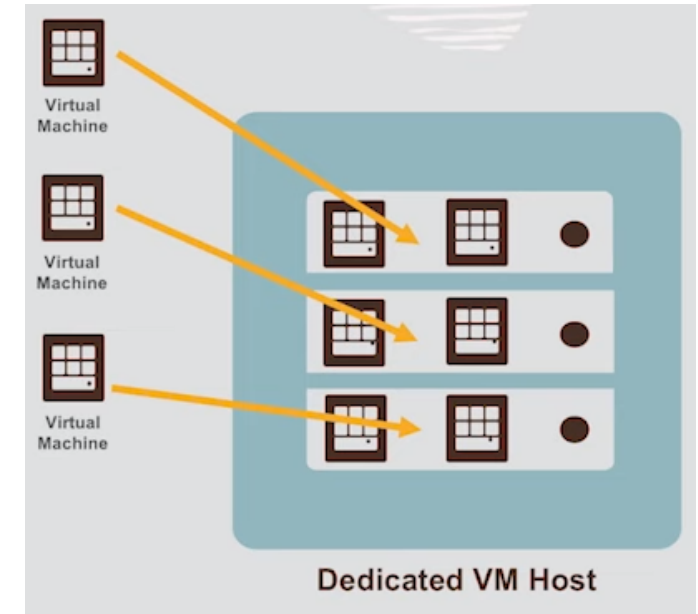
Data Safe

- Managed service that provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases
- Features include Security Assessment, User Assessment, Data Discovery, Data Masking, and Activity Auditing
- Supports ATP (shared), ADW (shared), VM/BM DB Systems
- Saves time and mitigates security risks
- Defense in Depth for all customers
- No special security expertise needed
- No extra costs to use



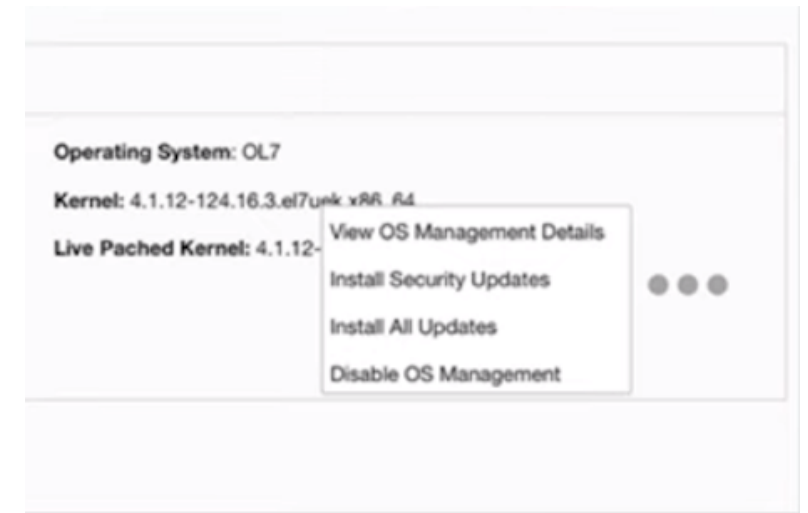
Dedicated VM Host

- Security of Bare Metal combined with ease and flexibility of VMs
- Single-tenant: never share HW with another customer's VMs
- Pay only for dedicated VM Host – no additional charge for the VMs running on it
- Control and convenience
 - Control over placement across Dedicated VM Hosts, or let Oracle optimize it automatically
 - Oracle manages and monitors the hypervisor and hardware

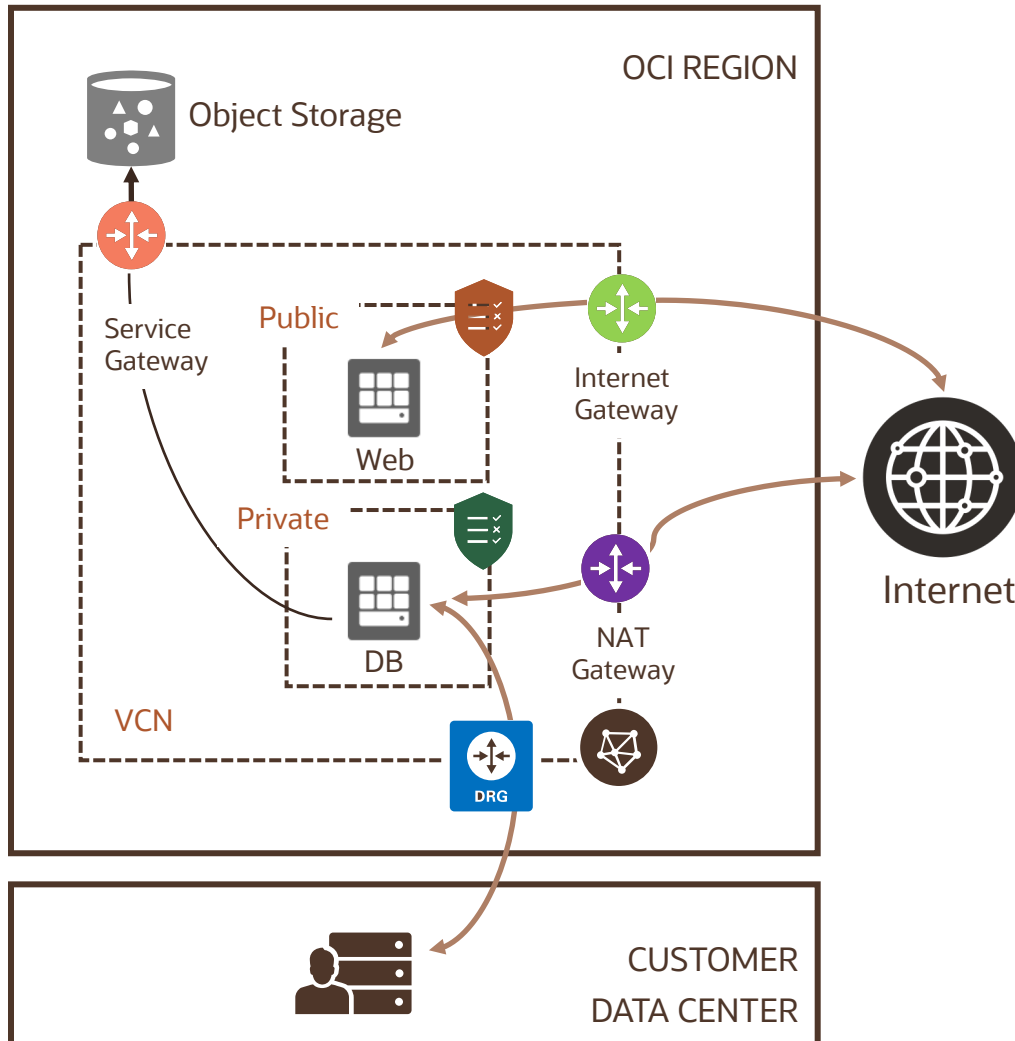


OS Management Service

- Executes and automates common and complex management tasks
- Package management, configuration management
- Security/compliance reporting
- Enables live patching of critical components and Linux kernel w/o downtime
- Configured by default for Oracle Linux instances in oracle cloud infrastructure



Network protection



Tiered subnet strategy for the VCN

- DMZ subnet for load balancers
- Public subnet for web servers
- Private subnet for internal hosts such as databases

Gateways

- NAT Gateway – for connectivity to internet for patching
- Service Gateway – for connectivity to public oracle cloud infrastructure services
- Dynamic Routing Gateway – for connectivity to on-premises

Security Lists, NSG

- SL determines the types of traffic allowed in and out of the subnet
- NSG the types of traffic allowed in and out of a VNIC

OCI Web Application Firewall

What is a WAF?

- WAF refers to a device, server-side plugin, or filter that applies a set of rules to HTTP/S traffic
- By intercepting HTTP/S traffic and passing them through a set of filters and rules, WAF is able to uncover and protect against attack streams hitting a web application
- Rules cover common attacks (Cross-site Scripting (XSS), SQL Injection) and ability to filter specific source IPs or bad bots
- Typical responses from WAF will either be allowing the request to pass through, audit logging the request, or blocking the request by responding with an error page.

Oracle Cloud Infrastructure Web Application Firewall (WAF) is a cloud-based, PCI-compliant, global security service that protects applications from malicious and unwanted internet traffic.

Use cases:

- Protect any internet-facing endpoint from cyberattacks and malicious actors
- Protect against cross-site scripting (XSS) and SQL injection
- Bot management – dynamically blocking bad bots
- Protection against layer 7 DDoS attacks

Compliance certifications

Global	 SOC 1 : SOC 2 : SOC 3	 27001 : 27017 : 27018	 Level 1	 US Privacy Shield			
Government	 DoD DISA SRG IL2	 DoD DISA SRG IL5	 Moderate – Agency ATO	 VPAT – Section 508	 G-Cloud 11 - UK	 Model Clauses - EU	
Industry	 HIPAA	 PCI DSS	 FISC - Japan	 IG Toolkit - UK	 FINMA - Switzerland		
Regional	 GDPR - EU	 BSI C5 - Germany	 TISAX - Germany	 PIPEDA - Canada	 Cyber Essentials Plus - UK	 My Number - Japan	 Cloud Security Principles - UK



Summary

Shared Security Model

Security services

Identity and Access Management

Data protection

OS and workload isolation

Infrastructure protection



Oracle Cloud always free tier:

oracle.com/cloud/free/

OCI training and certification:

cloud.oracle.com/en_US/iaas/training

cloud.oracle.com/en_US/iaas/training/certification

education.oracle.com/oracle-certification-path/pFamily_647

OCI hands-on labs:

ocitraining.qcloudable.com/provider/oracle

Oracle learning library videos on YouTube:

youtube.com/user/OracleLearning

Thank you

