Oracle Cloud Infrastructure (OCI) and the United Kingdom National Cyber Security Centre Cloud Security Principles (NCSC)

April 2024, Version 3

Public

Disclaimer

This document in any form, software, or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you assessing your use of Oracle Cloud Infrastructure in the context of the applicable guidelines under United Kingdom National Cyber Security Centre (UKNSC) Cloud Security Principles. This may also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document as the information in this document is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

This document does not make any 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 in this document remains at the sole discretion of Oracle.

(UKNSC) Cloud Security Principles are subject to periodic changes or revisions by the United Kingdom Government and governing bodies. The current version (UKNSC) Cloud Security Principles is available at:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

This document is based upon information available at the time of drafting, it is subject to change at the sole discretion of Oracle Corporation and may not always reflect changes in the regulations.

Table of Contents

Introduction

The UK National Cyber Security Centre (NCSC) published a collection of cloud security principles as guidance that is intended to help UK cloud users understand important cloud security needs for their businesses' cloud data and use.

The NCSC's 14 Cloud Security Principles outline the security standards that both cloud users and cloud service providers (CSPs) may use as their guidelines to implement and maintain a strong security posture. Some of these guidelines include important considerations for data in-transit protection, supply chain security, identity and authentication, and secure use of cloud services.

About Oracle Cloud Infrastructure

Oracle's mission is to help people see data in new ways, discover insights, and unlock endless possibilities. Oracle provides several cloud solutions tailored to customers' needs. These solutions provide customers the benefits of the cloud, including global, secure, and high-performance environments in which to run all their workloads.

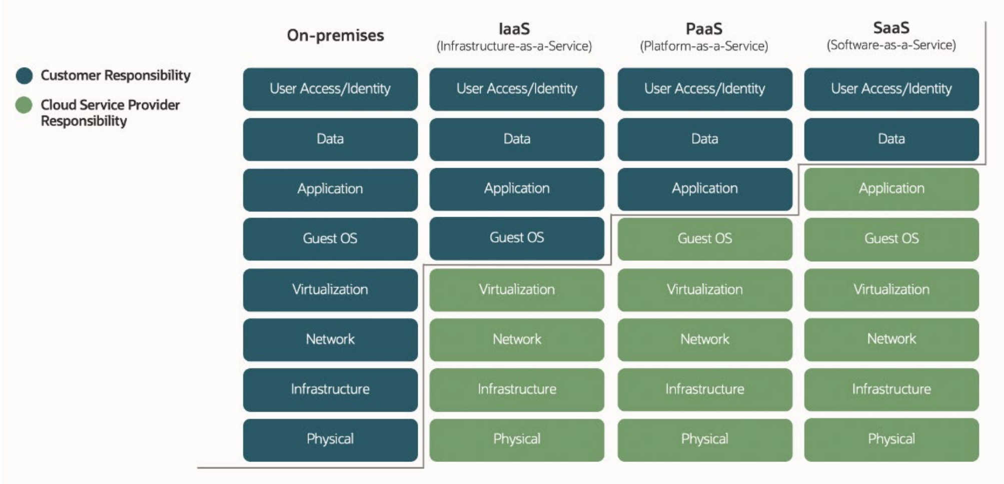
OCI is a set of complementary cloud services that enable customers to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance compute capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from an on-premises network. OCI delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI, see docs.oracle.com/en-us/iaas/Content/home.htm.

The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On-premises customers are in full control of their technology infrastructure. For example, they may have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers use components that are partially under the management of the cloud service providers. As a result, the management of security in the cloud is a shared responsibility between the cloud customers and the cloud service provider.

Because the responsibility is shared, customers too must be aware of and manage their security and compliance responsibilities when running their workloads in Oracle cloud environments. By design, Oracle provides security functions for cloud infrastructure and operations (e.g., cloud operator access controls, infrastructure security patching), and customers are responsible for securely configuring and using their cloud resources. For more information, you should refer to your cloud service documentation. Oracle provides best-in-class security technology and operational processes to secure enterprise cloud services.

The following figure illustrates this division of responsibility at a high level.



● Customer Responsibility
🟢 Cloud Service Provider Responsibility

On-premises	IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
● User Access/Identity	● User Access/Identity	● User Access/Identity	● User Access/Identity
● Data	● Data	● Data	● Data
● Application	● Application	● Application	🟢 Application
● Guest OS	● Guest OS	🟢 Guest OS	🟢 Guest OS
● Virtualization	🟢 Virtualization	🟢 Virtualization	🟢 Virtualization
● Network	🟢 Network	🟢 Network	🟢 Network
● Infrastructure	🟢 Infrastructure	🟢 Infrastructure	🟢 Infrastructure
● Physical	🟢 Physical	🟢 Physical	🟢 Physical

Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers.

Summary of the National Cyber Security Centre (NCSC) 14 Cloud Security Principles

The NCSC cloud security principles are broadly applicable as important guidelines for cloud service models including SaaS, PaaS, and IaaS. This document provides information about Oracle practices and capabilities in the context of the 14 principles, and how OCI cloud customers can use services, features, and capabilities of OCI to meet their security needs within the shared responsibility model.

Cloud Security Principle 1: Data in Transit Protection

"User data transiting networks should be adequately protected against tampering and eavesdropping.

- ***Data in transit protection should be achieved through a combination of:***
- ***encryption – denying your attacker the ability to read or modify data***
- ***network protection – denying your attacked the ability to intercept data***
- ***authentication – denying your attacker the ability to impersonate the service"***

Oracle has formal cryptography, encryption, and key management requirements. Compliance with these requirements is monitored by Oracle Global Product Security.

Oracle defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include:

- Locations and technologies for storing encryption keys
- Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures
- Changing default encryption keys
- Replacement schedule for various types of encryption keys

Encryption

Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to use up-to-date versions of approved security-related implementations. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms. Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption when data is at rest (in storage) on laptops, devices, and removable media.

The Cloud Compliance Standard for Encryption establishes encryption methods and procedures to protect the confidentiality, integrity, and availability of data. The standard specifies appropriate encryption technologies and acceptable levels of encryption for Oracle Cloud. The Cloud Compliance Standard for Encryption is based on standards from the National Institute of Standards and Technology (NIST), the Federal Government Standards on encryption (FIPS 140 and FIPS 180), and Oracle's Cryptographic Review Board.

Customers are responsible for appropriately safeguarding encryption keys that they own, manage, and maintain.

Vault allows customers to centrally manage the encryption keys that protect their data and the secret credentials that they use to securely access resources. Customers can use the OCI Vault service to create and manage vaults, keys, and secrets. Vaults securely store master encryption keys and secrets. Specifically, depending on the protection mode, keys are stored either on the server or on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 2 security certification.

Key management requirements

- OCI stores master encryption keys securely in a FIPS validated hardware security module (HSM) by default, keys cannot be exported from the HSM in plain text
- Connections to the customer administration console, APIs, or host region must be made over an encrypted protocol using HTTPS and TLS 1.2 or above
- Data stored on OCI Block Volume, Object Storage, File Storage, and Exadata Cloud Service storage is encrypted at rest by using AES 256-bit encryption
- OCI Data Transfer uses AES 256 for encryption of data at rest
- OCI Vault offers the ability to create master encryption keys and data encryption keys, rotate keys to generate new cryptographic material, enable or disable keys for use in cryptographic operations, assign keys to resources, and use keys for encryption and decryption
- Solutions for managing encryption keys and cryptographic libraries at Oracle must be approved per the Corporate Security Solution Assurance Process (CSSAP)

Network Protection

Customers are responsible for securely configuring network elements such as virtual networking, load balancers, DNS, and gateways.

Virtual Private Networks (VPNs)

OCI supports tunnel mode for IPSec Virtual Private Networks (VPNs). Each Oracle IPSec VPN consists of multiple redundant IPSec tunnels that use static routes to route traffic. Border Gateway Protocol (BGP) is not supported for the Oracle IPSec VPNs.

Private Connections

FastConnect offers a dedicated, private connection between the customer's data centre and OCI's network; FastConnect provides higher-bandwidth options, and a more reliable and consistent networking experience compared to internet-based connections

With FastConnect, customers can choose to use private peering, public peering, or both:

- **Private peering**: To extend existing infrastructure into a virtual cloud network (VCN) in OCI (for example, to implement a hybrid cloud or a migration scenario). Communication across the connection is with IPv4 private addresses (typically RFC 1918)
- **Public peering**: To access public services in OCI without using the internet—for example, Object Storage, the Console and APIs, or public load balancers in the customer's VCN. Communication across the connection is with IPv4 public IP addresses; without FastConnect, the traffic destined for public IP addresses would be routed over the internet. With FastConnect, that traffic goes over a private physical connection

All the customer's compute and storage resources are enclosed in an OCI VCN, which the customer configures and controls. The VCN is a software-defined network, resembling the on-premises physical network used by customers to run their workloads. Formulating a VCN security architecture includes tasks such as these:

- Creating VCN subnets for network segmentation
- Formulating VCN and load balancer firewalls using VCN security lists
- Using load balancing for high availability and TLS

- Determining the type of VCN external connectivity, whether internet, on-premises network, peered VCN, or a combination of these
- Using virtual network security appliances (for example firewalls, IDs)
- Creating DNS zones and mappings. An important security consideration in load balancers is using customer TLS certificates to configure TLS connections to a customer's VCN
- A customer's VCN can be partitioned into subnets, each mapped to an availability domain; instances inside private subnets cannot have public IP addresses; instances inside public subnets can optionally have public IP addresses at the customer's discretion

Gateways

Gateways let resources in a VCN communicate with destinations outside the VCN. The gateways include the following:

1. **Internet gateway** for internet connectivity (for resources with public IP addresses)
2. **NAT gateway** for internet connectivity without exposing the resources to incoming internet connections (for resources with private IP addresses)
3. **Dynamic routing gateway (DRG)** for connectivity to networks outside the VCN's region (for example, the on-premises network by way of an IPSec VPN or FastConnect, or a peered VCN in another region). Route tables control how traffic is routed from the customer's VCN's subnets to destinations outside the VCN. Routing targets can be VCN gateways or a private IP address in the VCN.
4. **Service gateway** for private connectivity to public OCI services such as Object Storage
5. **Local peering gateway (LPG)** for connectivity to a peered VCN in the same region

Cloud Security Principle 2: Asset Protection and Resilience

"Your data (and the assets storing or processing it) should be protected.

You should consider:

- ***Physical location and legal jurisdiction***
- ***Data centre security***
- ***Data encryption***
- ***Data sanitisation and equipment disposal***
- ***Physical resilience and availability"***

Physical location and legal jurisdiction

Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets.

For more information, see oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html.

Data residency laws or data localization laws may require certain categories of data to be stored in a specific jurisdiction. Customers are solely responsible for adhering to laws or regulations that may apply to your data and the region it is residing in, and then determine what you must do to comply.

Oracle Global Physical Security uses a risk-based approach to physical and environmental security. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained. For more information, see oracle.com/corporate/security- practices/corporate/governance/global-physical-security.html.

The OCI Data Center Services (DCS) Program Management, Audit, Security, and Safety (PASS) team performs an assessment of data center and PoP site control environments, including physical security controls and environmental safeguards, prior to the data center hosting production traffic (go-live) and then thereafter in accordance with the schedule defined in the Data Center Assessment Program.

The Data Center Assessment Program is completed through multifaceted review and analysis techniques to comprehensively evaluate the effectiveness of controls at the data centers. This involves artifact and evidence collection and review, on-site observation, and interviews with data center personnel.

Evidence collection includes the review of data center attestation reports, or internationally recognized certifications, by OCI. In the event a data center does not have an attestation report or internationally recognized certification, OCI performs an on-site assessment of the site's control environment, in accordance with the schedule defined in the Data Center Assessment Program.

On-site data center observations include the following areas if applicable to the site:

- External areas including parameters, parking lots, and outside equipment storage
- Reception and lobby areas, office spaces, and conference rooms
- Data halls
- Oracle cages and suites
- Generators, batteries, fuel storage, and heating, ventilation, and air conditioning (HVAC) equipment
- Delivery and staging areas
- Loading docks

Data centre security

Oracle Cloud data centres are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Potential build sites and provider locations undergo an extensive risk evaluation that considers environmental threats, power availability and stability, vendor reputation and history, neighbouring facility functions (for example, high-risk manufacturing or high-threat targets), and geopolitical considerations among other criteria.

Oracle Cloud data centres align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centres housing OCI services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data centre staff are trained in incident response and escalation procedures to address security and availability events that may arise.

Oracle Cloud data center colocation facilities maintain ISO/IEC 27001:2013 certifications, SOC 2 Type 2 attestations, or both. OCI performs an annual review of available certifications and assurance reports from each facility and periodic on-site compliance inspections. OCI's independent auditors conduct periodic on-site walkthroughs to ensure data centre controls are in place and operating. The Oracle Supplier Co-Location Security Standard details the requirements for physical, administrative, and technical safeguards that data center co-location suppliers must adhere to.

Data Encryption

Encryption is the process of rendering data unreadable without the specific key to decrypt the data. Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption when data is at rest (in storage) on laptops, devices, and removable media.

Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to only use up-to-date versions of approved security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms.

Oracle implements a variety of technical security controls designed to protect information assets at rest and in transit. These controls are guided by industry standards and are deployed across the corporate infrastructure:

- Corporate systems such as applications and collaboration tools
- Removable storage media
- Laptops and mobile devices

The Oracle Cloud Infrastructure Object Storage service encrypts and decrypts all objects using 256-bit Advanced Encryption Standard (AES-256) to encrypt object data on the server. Each object is encrypted with its own data encryption key. Data encryption keys are always encrypted with a master encryption key that is assigned to the bucket. Encryption is enabled by default and cannot be turned off. By default, Oracle manages the master encryption key. In addition to this default encryption, you can employ these strategies to encrypt data:

1. Use client-side encryption to encrypt objects with their encryption keys before storing them in Object Storage buckets. An available option is to use the Amazon S3 Compatibility API, along with client-side object encryption support available in AWS SDK for Java. See Amazon S3 Compatibility API for more details about on this SDK.
2. Use server-side encryption with your own keys. For more information, see Using Your Own Keys for Server-Side Encryption.
3. Assign an Oracle Cloud Infrastructure Vault master encryption key that you control and rotate on your own schedule. For more information, see Using Your Own Keys in Vault for Server-Side Encryption.

Data sanitisation and equipment disposal

Oracle follows National Institute of Standards and Technology (NIST) *Special Publication 800-88 Guidelines on Media Sanitization*, which addresses ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitisation.

Oracle's Media Sanitisation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitisation) and disposal of information that is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. Electronic storage media includes laptops, hard drives, storage devices, and removable media such as tape.

OCI provides deletion capability in all its data storage services. For more information about each service, see the following resources:

- **Block Volume***:* See "Deleting A Volume" at docs.cloud.oracle.com/iaas/Content/Block/Tasks/deletingavolume.htm.
- **Object Storage**: See "Deleting an Object" at docs.cloud.oracle.com/iaas/Content/Object/Tasks/managingobjects.htm#To_delete_an_object and "To Delete a Bucket" at docs.cloud.oracle.com/iaas/Content/Object/Tasks/managingbuckets.htm.
- **Compute instances and NVMe storage**: See "Terminating an Instance" at docs.cloud.oracle.com/iaas/Content/Compute/Tasks/terminatinginstance.htm.
- **File Storage**: See "To Delete a File System" at docs.cloud.oracle.com/iaas/Content/File/Tasks/managingfilesystems.htm.

OCI offers Object Lifecycle Management feature to help manage your Object Storage and Archive Storage data. For more information, see *Using Object Lifecycle Management* at docs.cloud.oracle.com/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm.

Physical Resilience and Availability

Physical resilience

Resiliency is the ability of an application or workload to recover quickly from failures and maintain high availability. It's a critical aspect of cloud computing because it ensures that applications and workloads remain accessible and functional, even when unexpected events occur. The following information describes Oracle Cloud Infrastructure (OCI) resiliency. The information highlights the importance of resiliency in cloud computing and the resiliency features provided by OCI. Resiliency should be a key consideration because it ensures business continuity and minimizes the risk of service disruptions.

The Risk Management Resiliency Program (RMRP) objective is to establish a business-resiliency framework to help provide an efficient response to business interruption events affecting Oracle's operations. For more information, see oracle.com/corporate/security-practices/corporate/resilience-management/.

- The RMRP approach is comprised of several subprograms: emergency response to unplanned and emergent events, crisis management of serious incidents, technology disaster recovery, and business-continuity management; tthe goal of the program is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored
- Each of these subprograms is a uniquely diverse discipline; however, by consolidating emergency response, crisis management, business continuity, and disaster recovery, they can become a robust collaborative and communicative system
- Oracle's RMRP is designed to engage multiple aspects of emergency management and business continuity from the onset of an event and to leverage them based on the needs of the situation
- The RMRP is implemented and managed locally, regionally, and globally; the RMRP program management office provides executive scorecard reporting on program activities and status within the lines of business

Many OCI regions are composed of physically isolated and fault-tolerant availability domains. Customers can use these availability domains to build replicated system and architect solutions to meet their business continuity strategies. To learn more about architecting high-availability solutions with OCI, see https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/high-availability.htm.

Availability

OCI is physically hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centers within a region. A region is composed of one or more availability domains. Each availability domain contains three fault domains. A fault domain is a grouping of hardware and infrastructure within an availability domain. Fault domains provide anti-affinity: they let customers distribute their instances so that the instances are not on the same physical hardware within a single availability domain. A hardware failure or Compute hardware maintenance event that affects one fault domain does not affect instances in other fault domains. In addition, the physical hardware in a fault domain has independent and redundant power supplies, which prevents a failure in the power supply hardware within one fault domain from affecting other fault domains.

The availability domains within the same region are connected to each other by a low-latency, high-bandwidth network, which makes it possible for customers to provide high-availability connectivity to the internet and on-premises, and to build replicated systems in multiple availability domains for both high-availability and disaster recovery. Regions are independent of each other and can be separated by vast geographical distances. Dedicated regions are public regions assigned to a single organization. Generally, customers deploy an application in the region where it is most heavily used, because using nearby resources is faster than using distant resources. However, customers can also deploy applications in different regions for the following reasons:

- To mitigate the risk of region-wide events such as large weather systems or earthquakes
- To meet varying requirements for legal jurisdictions, tax domains, and other business or social criteria

All the availability domains in a region are connected to each other by a low-latency, high bandwidth network. This predictable, encrypted interconnection between availability domains provides the building blocks for both high availability and disaster recovery.

Fault domains are grouping of hardware and infrastructure within an availability domain. You can optionally specify the fault domain for a new compute instance at launch time. This allows you to distribute your compute instances so that they are not on the same physical hardware within a single availability domain. For more information, see the following topics:

- Fault Domains at docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm#fault
- Editing the Fault Domain for an Instance at docs.cloud.oracle.com/iaas/Content/Compute/Tasks/edit-fault-domain.htm

The Oracle PaaS and IaaS Public Cloud Services Pillar Document (PDF) provides the details on the Service Level Agreements (SLAs) available for each OCI service.

Cloud Security Principle 3: Separation Between Customers

"Separation techniques ensure a customer's service can't access or affect the service (or data) of another.

You rely on security boundaries implemented by your cloud provider to ensure that:

- ***you can control who has access to your data, and how the service is robust enough to defend against another customer having malicious code in their instance of the service***
- ***Large cloud services, such as platforms, may offer many different services. These services might each take a different approach to separation."***

Access Control & Authentication

Customers are responsible for managing access and authentication to their cloud services.

OCI Identity and Access Management (IAM) service provides identity and access management features such as authentication and single sign-on (SSO). With IAM an administrator in your organization will set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies. For specific details about writing policies for each of the different services, see Policy Reference.

Access to the Oracle Cloud Console and customer tenancy is managed by the customer, OCI Identity and Access Management (IAM) provides identity and access management features such as authentication, single sign-on (SSO), and identity lifecycle management for Oracle Cloud. Employees, business partners, and customers can access resources at any time, from anywhere, and on any device in a secure manner. Customers must implement your own policies, configurations, and artifacts for all IAM features and create and administer users, policies, configurations, and artifacts using IAM.

Key customer considerations for using Identity and Access Management:

- Allows the customer to create users, groups, security policies, and federation mechanisms for all IAM features

- Creates at least one administrator for the identity domain to grant the identity domain administrator role directly (in addition to any identity domain administrator roles granted by group membership)
- Grants users or groups the identity domain administrator role for domains other than the default domain grants them full administrator permissions to only that domain (not to the tenancy)
- Formulates authentication mechanisms (for example, Console access using a password, API access using API keys, and an auth token for object store) for the IAM users created
- Groups customer tenancy resources into logical groups using compartment
- Federates enterprise on-premises users and groups to their tenancy is an important consideration
- Must adhere to all the requirements and guidelines for NIST 800-63, including IAL3, AAL3 and FAL3

Customer Separation

The Oracle Cloud Infrastructure architecture was designed for security of the platform through isolated network virtualisation, highly secure firmware installation, a controlled physical network, and network segmentation.

All customer's compute and storage resources are enclosed in a virtual cloud network (VCN) created for the customer. A VCN is a software-defined network, resembling the on-premises physical network used by customers to run their workloads. Formulating a VCN security architecture includes tasks such as:

- Creating VCN subnets for network segmentation.
- Formulating VCN and load balancer firewalls using VCN security lists.
- Using load balancing for high availability and TLS.
- Determining the type of VCN external connectivity, whether internet, on-premises network, peered VCN, or a combination of these.
- Using virtual network security appliances (for example, firewalls, IDs).
- Creating DNS zones and mappings. Compute Instances Security Configuration

For additional information, the Oracle Cloud Infrastructure Security Architecture describes how OCI meets the security requirements of enterprises and customers who run critical and sensitive workloads.

Cloud Security Principle 4: Governance Framework

"A governance framework is vital to co-ordinate and direct the management of the service. An effective governance framework will ensure that procedural, personnel, physical and technical controls continue to work through the lifetime of a service. It should also respond to changes in the service, technological developments, and the appearance of new threats."

New and emerging cyberthreats require businesses to rethink their approach to cloud security, data protection, consumer privacy protection, and user authentication. Cloud governance policies for authenticating or monitoring access can configure and manage the security protocols and tailor them to your business needs.

OCI Governance Framework

Establishing clear and comprehensive policies is a foundational step in cloud governance to ensure responsible and effective cloud adoption. These policies outline the rules, guidelines, and expectations that govern various aspects of cloud usage within an organization. The following information explains the key elements to cover in these policies:

1. **Security Policies:** These policies define security measures and controls to protect data, applications, and infrastructure in the cloud environment. They encompass authentication, encryption, access controls, and vulnerability management to mitigate security risks.

2. **Data Protection Policies:** Data protection policies outline how sensitive and confidential data must be handled, stored, processed, and transmitted in the cloud. They ensure compliance with data privacy regulations and include guidelines for data classification, encryption, and data retention.
3. **Compliance Policies:** Compliance policies ensure adherence to industry-specific regulations, legal requirements, and internal standards. They specify how cloud usage aligns with relevant laws and regulations and include audit procedures and documentation.
4. **Usage Guidelines:** Usage guidelines provide best practices for deploying, configuring, and using cloud services. They cover aspects such as resource provisioning, network configuration, application deployment, and data management.
5. **Cost Management Policies:** Cost management policies set guidelines for optimizing cloud spending. They include budget allocation, resource utilization guidelines, and cost-tracking procedures to prevent overspending and manage cloud expenses efficiently.
6. **Resource Provisioning and Scaling:** These policies define procedures for provisioning and scaling cloud resources based on business needs. They ensure that resources are allocated appropriately, and auto-scaling mechanisms are configured for optimal performance.
7. **Access Control and Authentication:** Access control policies outline rules for granting and managing user access to cloud resources. They establish authentication methods, role-based access controls, and permissions to prevent unauthorized access.
8. **Incident Response and Reporting:** These policies provide a framework for handling security incidents and breaches. They detail the steps to detect, respond to, and report incidents, ensuring timely and coordinated incident management.
9. **Data Retention and Deletion:** Data retention and deletion policies specify how long data must be stored in the cloud and outline procedures for securely deleting data when it is no longer needed.
10. **Disaster Recovery and Business Continuity:** These policies address disaster recovery and business continuity plans in the event of cloud service disruptions or failures. They define backup strategies, recovery processes, and testing procedures.
11. **Change Management and Version Control:** Change management policies guide the process of making changes to cloud configurations, applications, and services. They ensure that changes are documented, tested, and implemented in a controlled way.
12. **Service Level Agreements:** Service Level Agreements (SLAs) policies establish expectations for the quality, performance, and availability of cloud services. They outline the terms of service agreements with cloud providers.

Cloud Security Principle 5: Operational Security & Cloud Security Principle 6: Personnel Security

"Services must be operated and managed in a way to impede, detect or prevent attacks.

Good operational security should not require complex, bureaucratic, time consuming or expensive processes. The aspects to consider are:

1. ***Vulnerability management***
2. ***Protective monitoring***
3. ***Incident management***
4. ***Configuration and change management"***

“Services must be operated and managed in a way to impede, detect or prevent attacks.

Vulnerability Management

The Oracle Patching and Security Alerts Implementation Policy requires the deployment of the Oracle Critical Patch Update and Security Alert updates as well as associate recommendations. This policy also includes requirements for remediating vulnerabilities in non-Oracle technology using a risk-based approach.

The Oracle Server Security Policy requires servers (both physical and virtual) managed by Oracle or third-parties on behalf of Oracle to be physically and logically secured in order to prevent unauthorized access to the servers and associated information assets.

Protective Monitoring

Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, or logs being overwritten.

Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security-incident management process. Access to security logs is provided based on need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.

Security Event, Information Monitoring & Alerts

OCI has deployed a security information and event monitoring (SIEM) solution that ingests and stores security-related logs and alerts from networking devices, hosts, and other components within the infrastructure. OCI’s Detection and Response Team (DART) monitors the SIEM for event correlations and other relevant detection scenarios 24x7x365 to defend and protect against unauthorised intrusions and activity in the production environment.

Alerts are sent to Oracle’s IT security and cloud security operations teams for review and response to potential threats. Oracle requires that these alerts are monitored within the Lines of Business (LoBs) 24x7x365.

Incident Management

Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed customer data has been improperly handled or access. Oracle’s Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle’s Lines of Business.

GIS defines roles and responsibilities for the incident response teams embedded within the Lines of Business. All LoBs must comply with GIS incident response guidance about detecting events and timely corrective actions. Corporate requirements for LoB incident-response programs and operational teams are defined per incident type:

- Validating that and incident has occurred
- Communicating with relevant parties and notifications
- Preserving evidence
- Documenting and incident itself and related response activities
- Containing an incident
- Addressing the root cause of an incident
- Escalating an incident

Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defence in depth. Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.

In the event that Oracle determines that a confirmed security incident involving Information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared. Incident history is also Oracle Confidential and is not share externally.

As a controller, you must determine whether any of your end users or regulators must be notified of a personal information breach. Customers may have responsibilities for incident and personal information breach detection within the security environment that they control. For example, OCI cannot detect whether a user's login to a customer's tenancy was unauthorized. Cloud Guard and the Audit service (see the following section) can help you monitor software, depending on the functionality that you have implemented on the Oracle Infrastructure platform.

Change Management

OCI has a comprehensive change management process as a core requirement of its commitment to security, availability, and confidentiality. The change management process is reviewed annually, at a minimum, and outlines the processes and procedures to be followed for each change.

The process incorporates segregation of duties and requires changes to be approved and tested prior to implementation. All change requests are documented in an electronic, access-controlled ticketing system. The workflow prevents the ticket from being moved into the scheduled or implementation phase without the required review and approval of child tickets being in the closed state.

All changes must be peer reviewed prior to implementation. The reviewer is typically a member of the same team with knowledge of the in-scope system service who can technically review the change for accuracy and potential issues. Changes that have the potential to have a significant impact on customers are also required to have a documented approval from the manager of the team managing the service.

Cloud Security Principle 7: Secure Development

"Cloud services should be designed and developed and deployed in a way that minimises and mitigates threats to their security.

Cloud services which aren't designed, developed, and deployed in a secure way may be vulnerable to security issues which could compromise your data, cause loss of service, or enable other malicious activity."

Secure Development

Encompassing every phase of the product development life cycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products , whether they are used on-premises by customers, or delivered through Oracle Cloud.

OSSA is a set of industry-leading standards, technologies, and practices aimed at:

- **Fostering security innovations. Oracle has a long tradition of security innovations.** Today this legacy continues with solutions that help organizations implement and manage consistent security controls across the technical environments in which they operate, on-premises and in the clouds.

- **Reducing the incidence of security weaknesses in all Oracle products.** Oracle Software Security Assurance key programs include Oracles Security Coding Standards, mandatory security training for development, the cultivation of security layers within development groups, and the use of automated analysis and testing tools.
- **Reducing the impact of security weaknesses in released products on customers.** Oracle has adopted transparent security vulnerability disclosure and remediation policies. The company is committed to treating all customers equally and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs.

Secure Coding

Developing secure software requires consistently applied methodologies across the organization; methodologies that conform to stated policies, objectives, and principles. Oracle's objective is to produce secure code. To that end, Oracle requires that all of development abide by secure coding principles that have been documented and maintained to remain relevant. Additionally, Oracle has adapted its secure coding principles for use by our consulting and services organizations when they are engaged in producing code on behalf of our customers.

Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. They discuss general security knowledge areas such as design principles, cryptography and communications security, common vulnerabilities, etc., and provide specific guidance on topics such as data validation and user management.

All Oracle developers must be familiar with these standards and apply them when designing and building products. The coding standards have been developed over a number of years and incorporate best practices as well as lessons learned from continued vulnerability testing by Oracle's internal product assessment team. Oracle provides that developers are familiar with its coding standards by requiring that they undergo secure coding training. The Secure Coding Standards are a key component of Oracle Software Security Assurance and adherence to the Standards is assessed and validated throughout the supported life of all Oracle products.

Oracle products and services are required to be secure by default. Products and services should only install the essential components to perform their intended functions. Any features not intended for a production deployment. Such as demonstration content, default accounts and debug tools, should not be installed by default. This is commonly referred to a minimizing of the attack surface. By default, the product or service should only use secure protocols and algorithms.

Cloud services are deployed in a specific configuration, or a small number of configurations. The security of this configuration should be planned from the design phase, by the development team. The developers implementing the service need to be aware of the planned configuration. Testing must be performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment.

Cloud development teams are required to deliver the service to cloud operations teams in an automated, fully secured configuration. Use of containers, such as Docker and automated deployment pipelines, help development teams satisfy this requirement.

Cloud Security Principle 8: Supply Chain Security

"Third party supply chains should support all of the security principles which the service claims to implement.

Cloud services rely upon third party products and services. Consequently, if this principle is not implemented, supply chain compromise can undermine the security of the service and affect the implementation of other security principles."

Supply chain security

Oracle's Supply Chain Risk Management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity and security across Oracle's products and services.

Quality and reliability for Oracle's hardware systems are addressed through a variety of practices, including:

- Design, development, manufacturing, and materials management processes
- Inspection and testing processes
- Requiring that hardware supply chain suppliers have quality control processes and measurement systems
- Requiring that hardware supply chain suppliers comply with applicable Oracle requirements and specifications

Supply **availability**, **continuity** and **resiliency** in Oracle's hardware supply chain, are addressed through a variety of practices, including

- Multiple-supplier and/or multiple-location sourcing strategies where possible and reasonable
- Review of supplier financial and business conditions
- Requiring suppliers to meet minimum purchases periods and provide end-of-life (EOL)/end-of-support-life (EOSL) notice
- Requiring advance notification of product changes from suppliers so that Oracle can access and address any potential impact
- Managing inventory availability affected by changes in market conditions and natural disaster

Authenticity and the risk of counterfeit products are addressed throughout the product and service life cycle, including:

- Oracle supplier selection and contracting practices for sourcing components and materials from original manufacturers or their reputable and authorized distributors
- Inspection and testing processes

In addition, Oracle suppliers are required to protect the data and assets Oracle entrusts to them. The Oracle Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers are required to adopt when accessing Oracle or Oracle customer facilities, networks and/or information systems, handling Oracle confidential information, or controlling custody of Oracle hardware assets. Suppliers are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards.

For more information about Oracle Supply Chain Security and Assurance, see:
https://www.oracle.com/corporate/security-practices/corporate/supply-chain/

Cloud Security Principle 9: Secure User Management

"Providers should make the tools available for you to securely manage your use of their service.

Your provider should make the tools available for you to securely manage your access to their service, preventing unauthorized access and alteration to your resources, applications, and data."

OCI offers a suite of security services to help customers securely manage their tenancy. For more information, see OCI documentation, at https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_features.htm

Additionally, OCI maintains a robust library of documentation with information about how you can securely setup and manage your cloud tenancy.

- Oracle Cloud Infrastructure Security Guide: https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm
- Oracle Cloud Adoption Framework – Security: https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/security.htm

Identity and Access Management

You are responsible for protecting your cloud access credentials and setting up individual user accounts. When you sign up for OCI, Oracle creates a tenancy for you. The tenancy contains your identity and access management (IAM) entities (users, groups, compartments, and some policies) and other OCI resources. IAM service provides authentication and authorization for all OCI resources and services. For more information, see https://docs.oracle.com/en-us/iaas/Content/Identity/getstarted/identity-domains.htm#overview.

An identity domain is a container for managing users and roles, federating and provisioning users, securing application integration through single sign-on (SSO) configurations, and SAML/OAuth-based identity provider administration. The domain represents a user population in OCI and its associated configurations and security settings, such as multi-factor authentication (MFA).

Access Governance

Oracle Access Governance is a cloud native identity governance and administration service that provides access reviews and identity analytics to define and govern access privileges. It provides visibility and prescriptive recommendations to help reviewers make informed decisions about access privileges to reduce risk across the organization. For more information, see https://docs.oracle.com/en-us/iaas/access-governance/doc/overview.html.

Cloud Security Principle 10: Identity and Authentication

"Access to service interfaces should be constrained to authenticated and authorised individuals.

Services and data should only be accessible to an authenticated and authorised identity, which may be either a user or a service identity.

To apply effective access control as described in Principle 9: secure user management, you must have confidence in the authentication method used to determine the identity performing the access.

Weak authentication to these interfaces may enable unauthorised access to your systems, resulting in the theft or modification of your data, changes to your service, or a denial of service. Importantly, authentication should occur over secure channels, as described in Principle 1: data in transit protection."

OCI offers a suite of security services to help customers securely manage their tenancy. For more information, see OCI documentation, at https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_features.htm.

Authentication and Authorisation

Each service in OCI integrates with IAM for authentication and authorisation, and for all interfaces (Console, SDK, CLI, and REST API). An administrator in your organisation needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, and so on. For more information, see Getting Started with Policies. For details about writing policies for each of the different services, see Policy Reference.

Least-Privilege Access & Multifactor Authentication

To reduce the risk from overly permissioned users or applications, we use the principle of *least-privilege access* when granting access to production systems. OCI periodically review the approved lists of service team members and revoke access if no justifiable need for access exists.

Access to production systems requires multifactor authentication (MFA). The Security team grants MFA tokens and disables the tokens of inactive members. All access to production systems is logged, and the logs are kept for security analysis.

Multiple Authentication Layers

Weak account credentials also pose a significant threat to cloud environments. To strengthen authentication, OCI use several layers of advanced access control to meter access to network devices and the servers that support those resources. One of those layers is compulsory virtual private network (VPN) connectivity to the production network. This VPN requires high password diversity and the use of Universal 2nd Factor (U2F) authentication, an open standard for strengthening and simplifying two-factor authentication by using a hardware key.

All administrative access is logged, and all access permissions are audited for least-privilege. By using multiple factors for authentication, we help prevent an attacker from accessing the administrative network with weak or breached passwords.

Audit Service

The Audit service records calls to the OCI public API, whether those calls originated from the Console, SDK, or CLI, the customer's custom clients, or other OCI services. Audit log contents include the activity that occurred, the user who initiated it, the date and time of the request, the source IP address, the user agent, and the HTTP headers of the request. Data from these logged events can help you safeguard your data by enabling you to monitor activity within your tenancy. This logging occurs automatically, and you can setup the Audit log retention period. For more information about OCI Audit service, see docs.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm, and *Setting Audit Log Retention Period* at docs.oracle.com/iaas/Content/Audit/Tasks/settingretentionperiod.htm

Cloud Security Principle 11: External Interface Protection

"All external or less trusted interfaces to the service should be identified and appropriately defended.

Defensive measures may include application programming interfaces (APIs), web consoles, command line interfaces (CLIs), or direct connect services. Also, the cloud provider's administration interfaces, the interfaces you use to access the service, and any interfaces to your services built on top of the cloud service.

If some of the interfaces exposed are private (such as management interfaces) then the impact of compromise may be more significant. You can use different models to connect to cloud services which expose your enterprise systems to varying levels of risk."

The customer is responsible for the physical security of computing resources within their own operating environment. With respect to logical interface security, all of the customer's compute and storage resources are enclosed in a virtual cloud network (VCN), which the customer configures and controls. Additionally, the Oracle Cloud Infrastructure Domain Name System (DNS) service provides dynamic, static, and recursive DNS solutions for enterprise customers. The service connects visitors to customer websites and applications with fast and secure services.

The DNS service operates on a global anycast network of multiple data centres on six continents and offers fully redundant DNS constellations and multiple Tier 1 transit providers. The service provides a DNS-based Distributed Denial of Services (DDoS) protection and in-house security expertise that leverages a vast sensor network that collects and analyses billions of data points per day. The DNS service also fully supports secondary DNS features to complement the customer's existing DNS service, providing resiliency at the DNS layer.

The VCN is a software-defined network, resembling the on-premises physical network used by a customer to run their workloads. Formulating a VCN security architecture includes tasks such as the following ones:

- Creating VCN subnets for network segmentation.
- Formulating VCN and local balancer firewalls using VCN security lists.
- Using load balancing for high availability and TLS.
- Determining the type of VCN external connectivity, whether internet, on-premises network, peered VCN, or a combination of these.

- Using virtual network security appliances (for example, next-generation firewalls, IDs).
- Creating DNS zones and mapping. An important security consideration in load balancers is using customer Transport Layer Security (TLS) certificates to configure TLS connections to a customer's VCN.

The customer's VCN can be partitioned into subnets, each mapped to an availability domain. Instances inside private subnets cannot have public IP addresses. Instances inside public subnets can optionally have public IP addresses at the customer's discretion.

Security lists provide stateful and stateless firewall capability to control network access to the customer's instances. A security list is configured at the subnet level and enforced at the instance level. The customer can apply multiple security lists to a subnet. A network packet is allowed if it matches any rule in the security lists.

Gateways let resources in a VCN communicate with destinations outside the VCN. The gateways include the following ones:

- **Internet gateway** for internet connectivity (for resources with public IP addresses)
- **NAT gateway** for internet connectivity without exposing the resources to incoming internet connections (for resources with private IP addresses)
- **Dynamic routing gateway (DRG)** for connectivity to networks outside the VCN's region (for example, the on- premise network by way of an IPSec VPN or FastConnect, or a peered VCN in another region)
- **Service gateway** for private connectivity to public OCI services such as Object Storage
- **Local peering gateway (LPG)** for connectivity to a peered VCN in the same region

Route tables control how traffic is routed from the customer's VCN's subnets to destinations outside the VCN. Routing targets can be VCN gateways or a private IP address in the VCN.

Cloud Security Principle 12: Secure Service Administration

"Cloud providers should recognise the high value of administration systems.

The design, implementation, and management of the cloud provider's administration systems used by your cloud provider should follow enterprise good practice, whilst recognising their high value to attackers.

Systems used by the vendor for administration of their cloud services will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data."

Organisations can create and manage cloud service resources in the following ways:

- **Console:** The Oracle Cloud Console (docs.oracle.com/iaas/Content/GSG/Concepts/console.htm) is an intuitive, graphical interface that facilitates the creation and management of instances, cloud networks, and storage volumes, as well as users and permissions.
- **APIs**: The OCI APIs are typical REST APIs (docs.oracle.com/iaas/Content/API/Concepts/usingapi.htm) that use HTTPS requests and responses.
- **SDKs**: Software Development Kits (docs.oracle.com/iaas/Content/devtoolshome.htm) are available for easy integration with the APIs, including SDKs for Java, Ruby, and Python.
- **CLI:** The customer can use a CLI (docs.oracle.com/iaas/Content/API/Concepts/cliconcepts.htm) with some services.

Cloud Security Principle 13: Audit Information and alerting for customers

"Providers should supply logs needed to monitor access to your service, and the data held within it.

You should be able to identify security incidents and should have the information necessary to determine how and when they occurred.

This will require:

- ***audit information***
- ***security alerts"***

The OCI Audit service automatically records calls to all supported OCI public API endpoints as log events. Currently, all services support logging by Audit. Log events recorded by the Audit service include API calls made by the OCI Console, CLI, SDKs, the customer's own custom clients, or other OCI services. Information in the logs shows what time API activity occurred, the source of the activity, the target of the activity, what the action was, and what the response was.

Each log event includes a header ID, target resources, the timestamp of the recorded event, request parameters, and response parameters. The customer can view events logged by the Audit service by using the Console, API, or the Java SDK. The customer can view events, copy the details of individual events, and analyse events or store them separately. Data from events can be used to perform diagnostics, track resource usage, monitor compliance, and collect security-related events. For more information about OCI Audit service, see https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm.

The OCI Logging service allows customers to enable, view, and manage all the logs in their tenancy, and provide access to logs form OCI resources. These logs include critical diagnostic information that describes how resources are performing and being accessed. For more information about OCI Logging service, see https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/loggingoverview.htm.

Cloud Security Principle 14: Secure Use of the Service

"Providers should make it easy for you to adequately protect your data.

Your cloud provider should make it easy for you to meet your responsibility to adequately protect your data.

You should consider:

- ***whether the service is secure by design and by default***
- ***what helps the provider gives you to meet your responsibilities."***

Security in the cloud is a shared responsibility between you and Oracle. For you to securely run your workloads in Oracle Cloud Infrastructure, you must be aware of your security and compliance responsibilities.

Whereas Oracle ensures the security of cloud infrastructure and operations, your organization must define its own security guidelines. The following table introduces the shared security model between your organization and Oracle.

OWNER	AREA OF RESPONSIBILITY
Customer	Security *in* the cloud. For example: • Organization's data • User credentials, other account information • Account access management, application management • Secure user access behavior, strong Oracle Cloud Infrastructure Identity and Access Management (IAM) policies • Patching

	• Network and firewall configuration • Security rules, route rules, virtual cloud network (VCN) configuration • Client-side encryption • Vault
Oracle	Security *of* the cloud. For example: • Other Oracle Cloud Infrastructure services and functionality, such as Load Balancing, WAF, Cloud Guard, distributed denial-of-service (DDoS) protection • Compute, network, and storage isolation • IAM framework • Data center physical security • Hardware, software, networking, and facilities that run Oracle services

Oracle is responsible for all aspects of the physical security of the availability domains and fault domains in each region.

Both Oracle and your organization are responsible for the security of software and the associated logical configurations and controls.

Oracle Cloud Infrastructure enables enterprises to migrate their mission-critical workloads to the cloud while continuing to maintain the same security posture. Reduce the overhead of building and operating data center infrastructure without sacrificing security.

All Oracle Cloud Infrastructure security capabilities have been designed with one goal in mind: allowing you to run your mission-critical workloads in the cloud with complete control and confidence. Oracle continues to invest in these areas and more to offer unmatched security and assurance to enterprise customers.

- For a general overview of Oracle Cloud Infrastructure security concepts, see Security Overview.
- For an overview of the security services in Oracle Cloud Infrastructure, see Security Services.
- For an overview of the security capabilities in core services like Compute, Networking, and Block Volume, see Security for Core Services.
- For general recommendations on getting started with Oracle Cloud Infrastructure security, see Securing Your Tenancy.

For service-specific best practices and policy examples, see Security Best Practices.NCSC Cloud Security Principles and OCI.

NCSC has outlined several steps that you can take to gain confidence that the services and features OCI offers and the security controls in place are operating effectively. Ultimately you are responsible for determining if the OCI services and architecture will meet your security needs.

The following sections provide additional information about Oracle practices and OCI compliance programs that may further assist in your evaluation of OCI.

Contractual Commitment from a Supplier

Oracle has standard contracts and policies that govern the terms, service descriptions, and delivery of cloud services to customers. Oracle's Cloud Services Hosting and Delivery Policies describe how Oracle delivers cloud services, including how Oracle addresses security, change management, and backups.

- Oracle Cloud Services Contracts, at oracle.com/corporate/contracts/cloud-services/contracts.html

- Cloud Services Hosting and Delivery Policies at oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html

Security Architecture Review

The Oracle corporate security architect helps set internal information-security technical direction and guides Oracle's IT departments and lines of business toward deploying information security and identity management solutions that advance Oracle's information security goals. The corporate security architect works with Global Information Security, Global Product Security, and the development security leads to develop, communicate, and implement corporate security architecture roadmaps.

Corporate Security architecture manages a variety of programs and leverages multiple methods of engaging with leadership and operational security teams responsible for Oracle operations, services, cloud, and all other lines of business. An example program for managing the security of Oracle's architecture is the Corporate Security Solution Assurance Process (CSSAP).Corporate Security Solution Assurance Process (CSSAP) is a security review process developed by Corporate Security Architecture, Global Information Security, Global Product Security, Oracle Global IT, and Oracle's IT organisations to provide comprehensive information-security management review.

CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews be carried out throughout the project life cycle, so that projects are aligned with:

- **Preview**: The risk management teams in each line of business must perform a pre-assessment of each project using the approved template.
- **CSSAP review**: The security architecture team reviews the submitted plans and performs a technical security design review.
- **Security assessment review**: Based on risk level, systems and applications undergo security verification testing before production use.

Independent the Implementation of Controls

OCI operates under policies that are generally aligned with the ISO/IEC 27002 Code of Practice for Information Security Controls. The internal controls of OCI are subject to periodic testing by independent third-party audit organisations. Such audits may be based on the Statement on Standards for Attestation Engagements (SSAE) 18, Reporting on Controls at a Service Organisation ("SSAE 18"), the International Standard on Assurance Engagements (ISAE) No. 3000, Assurance Engagements on Other than Audits or Reviews of Historical Financial Information ("ISAE 3000"), or other third-party auditing standards or procedures applicable to OCI.

Oracle requires that external facing systems and cloud services undergo penetration testing performed by independent security teams. Global Information Security's Penetration Testing Team provides oversight to all lines of business in instances where other internal security teams or an approved third-party perform penetration testing activities. This oversight is designed to drive quality, accuracy, and consistency of penetration testing activities and their associated methodology. Oracle has formal penetration testing requirements which include test scope and environment definition, approved tools, findings classification, categories of exploits to attempt via automation and manual steps, and procedures for reporting results.

Audit reports about Oracle Cloud services are periodically published by Oracle's third-party auditors. Reports might not be available for all services or all audit types, or at all times. Customers may request access to available audit reports for a particular Oracle Cloud service by using available through Sales.

OCI Compliance with Recognized and Appropriate Standards

OCI's ISO/IEC 27001:2013 certification covers its Information Security Management System (ISMS). The ISMS is centrally managed from the OCI main office in Seattle, Washington, USA. In-scope applications, systems, people, and processes are globally implemented and operated by teams located in Seattle, Washington, and Nashua, New Hampshire, USA; Dublin, Ireland; Bangalore and Hyderabad, India; and Kaunas, Lithuania. The services are supported by in-scope data centres and transit sites in several regions throughout the globe, including London (LTN) and Newport (BRS), England.

OCI's Cyber Essentials certification provides independent verification of cybersecurity safeguards from an accredited certification body. The NCSC developed the Cyber Essentials scheme to provide clarity around the basic controls all organisations should implement to mitigate risks from common internet-based threats. The scheme's assurance framework offers a mechanism for an organisation to demonstrate to customers and other interested parties that it has relevant technical controls in place.

OCI's SOC 2 Type 2 attestation provides the opinion of an independent auditor on the design effectiveness and operating effectiveness of controls relevant to security, confidentiality, and availability. The description of OCI's in-scope services, tests of controls, and results of testing outlined in the report provides customers with assurance that OCI's service commitments and requirements were achieved based on the applicable AICPA Trust Services Principles and Criteria.

OCI has implemented Payment Card Industry Data Security Standard (PCI DSS) into "business-as-usual" processes as part of its overall security strategy. This enables OCI to continuously monitor the effectiveness of security controls and to maintain a PCI DSS compliant environment in between annual PCI DSS assessments.

For more compliance information, see Oracle Cloud Compliance.

Conclusion

Oracle has designed OCI with a security-first approach, ensuring that security is built into the platform from the ground up, to reduce the risk and attack surfaces commonly associated with first-generation clouds. This includes implementing prescriptive security controls across both the architecture and business processes. As organizations look to cloud computing to drive IT modernization and innovation, OCI strives to deliver cost-effective solutions that are easy to implement and effectively address their security requirements.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com   facebook.com/oracle   twitter.com/oracle