ORACLE

National Cyber Security Centre (NCSC) Cloud Security Principles and Implementation in Oracle Cloud

August 2021, Version 2.2

Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license 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 in planning for the implementation and upgrade of the product features described. 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 in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Table of Contents

Introduction to Using the Cloud Security Principles

The National Cyber Security Centre (NCSC) published a collection of cloud security guidance that is intended to help you assess the security of a cloud service. The 14 Cloud Security Principles, taken as a whole, are intended to be used as a framework for evaluating the security of any cloud service provider. See details and context of the 14 Cloud Security Principles at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles.

Your security responsibility might vary depending on the type of services involved. As a buyer, you bear responsibility when using infrastructure as a service (IaaS). NCSC has published a specific guide for IaaS: Managing your responsibilities.

This technical brief is intended to provide you with an understanding of the following information:

- How Oracle Cloud Infrastructure's administrative, physical, and technical safeguards are aligned with NCSC Cloud Security Principles
- How the shared security responsibility model works based on the NCSC Cloud Security Principles
- How you can approach information security risk management and implementation of the NCSC Cloud Security Principles guidance using Oracle Cloud Infrastructure services

Overview of Oracle Cloud Infrastructure Services

Oracle Cloud Infrastructure (OCI) is IaaS that delivers on-premises, high-performance computing power to run cloud native and enterprise IT workloads. OCI provides real-time elasticity for enterprise applications by combing Oracle's autonomous services, integrated security, and serverless compute. It is available for public cloud and Dedicated Region Cloud@Customer, behind a company's private firewall and in its data centre.

Oracle Cloud Infrastructure includes services in the following categories:

- **Analytics**: oracle.com/business-analytics
- **Application Development**: oracle.com/application-development
- **Applied Software Technology**: oracle.com/emerging-technologies
- **Compute**: oracle.com/cloud/compute
- **Database**: oracle.com/database
- **Integration**: oracle.com/integration
- **Observability and Management**: oracle.com/manageability
- **Networking, Connectivity, and Edge Services**: oracle.com/cloud/networking
- **Security, Identity, and Compliance**: oracle.com/security
- **Storage**: oracle.com/cloud/storage

Oracle deploys cloud in data centre regions. Availability domains and three separate fault domains per data centre help ensure application availability; low-latency and high-bandwidth interconnect enables zero-data-loss architectures for applications such as Oracle Database and high availability for scale-out technologies such as Cassandra.

Data regions in Europe, the Middle East, and Africa (EMEA) are in the following cities:

- London (UK South)
- Newport (UK West)
- Frankfurt (Germany Central)
- Zurich (Switzerland North)
- Amsterdam (Netherlands Northwest)
- Jeddah (Saudi Arabia West)
- Dubai (UAE East)

For a complete list of regions and services available by region, see oracle.com/cloud/architecture-and-regions.

NCSC Cloud Security Principles: Customer Considerations and Oracle Cloud Infrastructure Implementation

The shared responsibility model outlines Oracle's responsibility to *maintain a secure and continuously available service* and the customer's responsibility to *ensure secure use of the service*.

Oracle Architecture and Shared Responsibility

Oracle Cloud customer deployments and uses vary; however, the cloud security shared responsibility model is inherent to the use of cloud services. In traditional on-premises data centre deployments, customers are responsible for all aspects of physical and logical security. In a cloud environment, the shared security model demonstrates how a cloud service provider is responsible for managing security *of* the public cloud, while the customer is responsible for securing their workloads that run *in* the cloud.

Shared Responsibility for Controls

In a shared, multiple-tenant compute environment, Oracle is responsible for the security of the underlying cloud infrastructure (such as data centre facilities, and hardware and software systems). Customers are responsible for securing their workloads and configuring their services (such as compute, network, storage, and database) securely. The shared responsibility model is intended to identify the technical and operational controls that are to be implemented by the cloud service provider and the cloud customer, respectively. Some domains, such as configuration management and compliance, are shared responsibilities between both parties. However, classifying and labeling data to meet compliance obligations is the customer's responsibility.

Oracle Responsibilities

The shared responsibility model outlines the cloud service provider's responsibility to maintain a secure and highly available service. Oracle provides security controls for cloud infrastructure and operations, such as cloud operator controls, infrastructure security patching, and data centre facility security. Controls that are part of a customer solution provided by OCI or another Oracle division remain the responsibility of the provider or are governed by the delivery agreements that OCI makes with the users of OCI.

Customer Responsibilities

Customers are responsible for securely configuring, deploying, and managing their cloud resources and workloads. OCI customers may be platform as a service (PaaS) and software as a service (SaaS) providers, or implement hybrid on-premises/cloud architectures or hybrid cloud infrastructure with more than one provider. In these situations, the shared responsibilities become broader and more complex, and customers should remain aware of responsibility for components when they are passed through to other parties.

With the cloud security shared responsibility model in mind, the following sections outline each of the 14 Cloud Security Principles described by the NCSC. Information about both customer considerations and OCI implementation is detailed for each principle, organised under the following areas:

- **Cloud Security Principle name and description**: As defined by NCSC.
- **Considerations**: Within the NCSC guide, "Implementing the Cloud Security Principles", these considerations are defined as "goals" that the customer (buyer) should be confident in when analysing and using a cloud service.
- **Oracle Cloud Infrastructure control or feature**: Details on the various processes, security controls, internal standards, and additional functionality offered to the customer (buyer) to enable secure architecture specific to the nature of each Cloud Security Principle.

Depending on the considerations for each given principle, the OCI control or feature focuses on the services where the security features are implemented.

Cloud Security Principle 1: Data in Transit Protection

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

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
The customer should be sufficiently confident that: • Data in transit is protected between the customer's end-user device(s) and the service. • Data in transit is protected internally within the service. • Data in transit is protected between the service and other services (e.g., where APIs are exposed).	**Encrypting Data in Transit** Your access to Oracle Cloud Services is through a secure communication protocol provided by Oracle. If access is through a Transport Layer Security (TLS) enabled connection, that connection is negotiated for at least 128-bit encryption. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configured for all web-based TLS-certified applications deployed at Oracle. It is recommended that the latest available browsers certified for Oracle programs, which are compatible with higher cipher strengths and have improved security, be used for connecting to the web-enabled programs. The list of certified bowers for each version of Oracle Cloud Services will be made available via a portal accessible to you or in the corresponding Service Description for the Oracle Cloud Services. In some cases, a third-party site that you want to integrate with the Oracle Cloud Services, such as a social media service, may not accept an encrypted connection. For Oracle Cloud Services for which HTTP connections with the third-party site are permitted by Oracle, Oracle will enable such HTTP connections in addition to the HTTPS connection. In-transit encryption provides a way to secure your data between instances and mounted file systems using TLS v.1.2 encryption. Together with other methods of security such as Oracle Cloud Infrastructure Vault and File Storage's encryption-at-rest, in-transit encryption providers for end-to-end security. • For general information about getting started with file systems, see Overview of File Storage. • For more information about the Vault service, see Overview of Vault. • For more information about securing your file system, see About Security and the Securing File Storage reference in the Security Guide. **Application Programming Interface (API) Encryption** All OCI API requests must support HTTPS and SSL protocol TLS 1.2. **Network Security** You are responsible for securely configuring network elements such as virtual networking, load balancing, DNS, and gateways. Oracle is responsible for providing a secure network infrastructure. **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.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	Private Connections Oracle Cloud Infrastructure FastConnect offers a dedicated, private connection between the customer's data centre and OCI. FastConnect provides higher-bandwidth options, and a more reliable and consistent networking experience compared to internet-based connections. With FastConnect, the customer 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 acrossthe 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 a 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, next-generation 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. 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** Security lists provide stateful and stateless firewall capability to control network access to a 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.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	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-premises 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. For more information, see the following topics: • Oracle Virtual Cloud Network • NAT Instance Configuration • Configuring IPsec • Bastion Hosts: Protected Access for Virtual Cloud Networks

Cloud Security Principle 2: Asset Protection and Resilience

User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage, or seizure.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
The customer should understand: • In which countries your data will be stored, processed, and managed. You should also consider how this affects your compliance with relevant legislation, e.g., Data Protection Act (DPA).	**Transparency of Processing** The Oracle Services Privacy Policy and Data Processing Agreement for Oracle Services provide transparency about Oracle's overall approach to the handling of your data. However, as a cloud provider, Oracle generally has no insight into the data that you store and process in Oracle Cloud Infrastructure, or whether it is personal data that belongs to a particular end user. In this context, Oracle has no relationship with your end users and therefore does not inform them about any of your data processing details. Only you can be transparent to your end users about how their data is processed.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
• Whether the legal jurisdictions within which the service provider operates are acceptable to you.	**Location Transparency** Oracle Cloud Infrastructure is transparent about where your data is processed and stored. This is important because some data privacy regulations lay down requirements for cross-border data transfers. When setting up your account, you choose a *home region* in which to initially locate your *tenancy*. Your data stays within that region unless you choose to move it outside the region. OCI offers powerful services that might operate cross-tenancy or cross-region. Through the OCI Console user interface and API documentation, you will always be made aware when your actions might cause data to move to another region or tenancy. Depending on the terms of your agreements with Oracle, Oracle may process data globally to fulfil the services. For more information, see the following topics: • "Regions and Availability Domains" at docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm • "Setting Up Your Tenancy" at docs.cloud.oracle.com/iaas/Content/GSG/Concepts/settinguptenancy.htm **Data Localization** Data localization laws, also known as data residency laws, may require certain categories of data to be stored in a specific country. Only you can take steps to familiarize yourself with the requirements of the data localization laws or regulations that may apply to your data, and then determine what you must do to comply. Oracle generally has no insight into the data that you store and process in Oracle Cloud Infrastructure, or whether it is in categories covered by data localization laws. The location transparency described in the previous section may help with data localization because you will always know the geographic location of your data in OCI. Oracle continues to open new data centre regions in countries around the world, which allows more of its customers to store their data within their own country. See "Oracle Cloud Infrastructure Data Centre Regions" at oracle.com/cloud/architecture-and-regions.html. For more information about data protection principles and compliance, see *Oracle Cloud Infrastructure and the GDPR* at oracle.com/a/ocom/docs/oci-gdpr.pdf.
• You should be confident that the physical security measures employed by the provider are sufficient for your intended use of the service.	**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. Candidate build sites and provider locations undergo an extensive risk evaluation by Oracle 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.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	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. **Data Centre Assurance** Colocation facilities have their own 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. Guidance on specific requirements for all Oracle buildings is included in the *Oracle Global Facility Physical Security Technology and Design Manual*. The Oracle Supplier Information and Physical Security Standard details requirements for physical, administrative, and technical safeguards that third-party suppliers must adhere to.
• You should have sufficient confidence that storage media containing your data are protected from unauthorised access.	**Security Safeguards: Shared Responsibility** Security in OCI is a shared responsibility between you and Oracle: • Oracle manages the security of the underlying cloud infrastructure (such as data centre facilities, and hardware and software systems). See "Oracle Corporate Security Practices" at oracle.com/corporate/security-practices/. • You, the customer, are responsible for securing your workloads and securely configuring services (such as compute, network, storage, and database). See "Shared Security Model" at docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_overview.htm#Shared_Security_Model. **Oracle Cloud Infrastructure Security** Cloud security posture management of OCI tenancies consists of two cloud security services: • **Oracle Security Zones**: Special compartments designed to enforce implicit and explicit security policies. • **Oracle Cloud Guard**: A scalable data processing security service that acts as the command centre for Oracle cloud security posture management. Oracle Cloud Guard gives a comprehensive picture of the security and risk posture of a customer's tenants in OCI. For more information, see Oracle Cloud Guard and Oracle Security Zones.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	Security Services, Features, and Best Practices OCI's many security services, features, and best practices are documented in the following topics: • "Security Services and Features" at docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_features.htm • *Oracle Cloud Infrastructure Security Architecture* at oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf • "Security Best Practices" at docs.cloud.oracle.com/iaas/Content/Security/Reference/configuration_security.htm **Encryption** The encryption described in this section occurs by default regardless of the nature of the underlying data. OCI does not have insight into the nature of your data, whether it is personal data, sensitive data, or otherwise. • **Block Volume**: Data is encrypted at rest by default, and the backups are also encrypted in Object Storage. See "Block Volume Encryption" at docs.cloud.oracle.com/iaas/Content/Block/Concepts/overview.htm#BlockVolumeEncryption. • **Object Storage**: Each object is encrypted with its own key. Encryption is enabled by default. See "Object Storage Features" at docs.cloud.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm#features. • **File Storage**: Customer data is encrypted at rest by default. See "Encryption" (File Storage) at docs.cloud.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm#encryption. • **Bare metal and Virtual Machine DB system**: Encryption of user-created tablespaces is enabled by default using Transparent Data Encryption (TDE). See "Transparent Data Encryption" (Bare metal/VM) at docs.cloud.oracle.com/iaas/Content/Database/Tasks/configuringDB.htm?#Transparent_Data_Encryption. • **Exadata Cloud Service**: All new tablespaces created by the customer in the Exadata Cloud Service database are encrypted by default. See "Managing Tablespace Encryption" (Exadata) at docs.cloud.oracle.com/iaas/Content/Database/Tasks/exaconfiguring.htm#Managing_Tablespace_Encryption.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	Vault Oracle Cloud Infrastructure Vault key management service provides centralized management of the encryption of customer data with keys that you control. It can be used for the following tasks: • 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 • Use keys for encryption and decryption to safeguard data The Block Volume, Object Storage, File Storage, and Streaming services integrate with Vault to support the encryption of data in those services. The integration of Vault with Identity and Access Management (IAM) lets you control who and what services have access to your keys. The Audit service (see next section) lets you track administrative actions on your keys and vaults. See "Overview of Vault" at docs.cloud.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.
You should be sufficiently confident that: • Your data is erased when resources are moved or reprovisioned, when your customer leaves the service or when you request it to be erased. • Storage media which has held your data is sanitised or securely destroyed at the end of its life.	**Storage Limitation** As a cloud provider, Oracle generally has no insight into the data that you store and process in OCI, whether the purposes for processing that data have passed, nor whether the data needs to be deleted. If you determine that your data must be deleted, OCI offers services designed to permanently delete data. **Data Deletion** 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.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	Object Lifecycle Management Oracle offers Object Lifecycle Management to help automate the archiving and deletion of data objects. See "Using Object Lifecycle Management" at docs.cloud.oracle.com/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm. **Data Subject (End User) Requests** As a cloud provider, Oracle generally has no insight into what personal information you collect from your data subjects (end users) and process in OCI. However, the "Privacy Inquiries and Requests from Individuals" section on the Data Process Agreement for Oracle Services describes the assistance that Oracle might be able to provide you to handle data subject requests such as requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to, or object to processing of specific personal information.
You should be sufficiently confident that: • All equipment potentially containing your data, credentials, or configuration information for the service is identified at the end of its life (or prior to being recycled). • Any components containing sensitive data are sanitised, removed, or destroyed as appropriate. • Accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker.	**Decommissioning Servers and Other Computing Resources** 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. **Data Sanitisation and Equipment Disposal** Oracle's Media Sanitisation and Disposal Policy sets forth the requirements for removal of information from electronic storage media including sanitisation and disposal of information to address scenarios such as end-of-life systems, system repair and reuse, and vendor replacement in conjunction with associated safe data handling. Oracle Cloud Infrastructure 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. **Service Termination** If you terminate your OCI service subscription, Oracle will make your data residing in the production Cloud Services environment available for you to retrieve. After the retrieval period, your data will be deleted. Details about this retrieval period are described in section 6, "Oracle Cloud Suspension and Termination Policy". See "Oracle Cloud Hosting and Delivery Policies" at oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html#hd.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
• You should be sufficiently confident that the availability commitments of the service, including their ability to recover from outages, meet your business needs.	The following OCI features help with data availability. **Availability Domains and Fault Domains** A customer's tenancy is created in the available home region of their choice. Many OCI regions are composed of physically isolated and fault-tolerant availability domains. Customers can use these availability domains to build replicated systems. 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 **Backups** The following flexible data storage backup options are available: • **Block Volume**: Block Volume backups can be manual or scheduled, incremental or full. Cross-region backups can be used for business continuity, disaster recovery, and application migration and expansion. Policy-based backups have different backup frequencies and retention periods. These backups are encrypted in Object Storage. See "Overview of Block Volume Backups" at docs.cloud.oracle.com/iaas/Content/Block/Concepts/blockvolumebackups.htm. • **Object Storage**: Object Storage replication aids in disaster recovery efforts, and addresses data redundancy compliance requirements. Copies of objects can be made to other buckets in the same region or across regions. See "Using Replication" (Object Storage) at docs.cloud.oracle.com/iaas/Content/Object/Tasks/usingreplication.htm and "Copying Objects" at docs.cloud.oracle.com/iaas/Content/Object/Tasks/copyingobjects.htm. • **Bare Metal and Virtual Machine DB Systems**: Backups can go to Object Storage or local storage; Data Guard can also be used for data protection and availability. See "Backing Up a Database" (Bare metal/VM) at docs.cloud.oracle.com/iaas/Content/Database/Tasks/backingup.htm and "Using Data Guard" (Bare metal/VM) at docs.cloud.oracle.com/iaas/Content/Database/Tasks/usingdataguard.htm.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	• **Exadata Cloud Service**: Exadata database backups go to Object Storage and can be managed or unmanaged. Data Guard can also be used for data protection and availability. See the following topics: "Managing Exadata Database Backups" (Oracle managed) at docs.cloud.oracle.com/iaas/Content/Database/Tasks/exabackingup.htm "Managing Exadata Database Backups by Using bkup_api" at docs.cloud.oracle.com/iaas/Content/Database/Tasks/exabackingupBKUPAPI.htm "Using Oracle Data Guard with Exadata Cloud Service" at docs.cloud.oracle.com/iaas/Content/Database/Tasks/exausingdataguard.htm Learn more about high-availability solutions for OCI at docs.oracle.com/en/solutions/design-ha.

Cloud Security Principle 3: Separation Between Users

A malicious or compromised user of the service should not be able to affect the service or data of another.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
You: • Understand the types of user you share the service or platform with. • Have confidence that the service provides sufficient separation of your data and service from other users of the service. • Have confidence that management of your service is keep separate from other users.	**Platform Security** The Oracle Cloud Infrastructure architecture was designed for security of the platform through isolated network virtualization, highly secure firmware installation, a controlled physical network, and network segmentation. OCI benefits from tiered defences and highly secure operations that span from the physical hardware in our data centres to the web layer, in addition to the protections and controls available in our cloud. Many of these protections also work with third-party clouds and on-premises solutions to help secure modern enterprise workloads and data where they reside. Oracle Cloud Infrastructure Security Architecture describes how OCI meets the security requirements of enterprises and customers who run critical and sensitive workloads. It details how security is fundamental to the architecture, data centre design, personnel selection, and processes for provisioning, using, certifying, and maintaining OCI. Security of an OCI tenancy is based on a combination of factors. The following steps provide high-level guidelines for configuring security of a tenancy. **User Authentication and Authorisation** The initial step in securely configuring a tenancy is to create mechanisms for authenticating users and authorising users to access tenancy resources in a least-privilege manner.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	This step comprises the following actions: • Creating OCI Identity and Access Management (IAM) users • Creating IAM groups • Formulating 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 • Grouping customer tenancy resources into logical groups using compartments • Formulating IAM security policies authorizing access of IAM groups to tenancy or compartment resources For enterprises, federating their on-premises users and groups to their tenancy is an important consideration. IAM allows the customer to create users, groups, security policies, and federation mechanisms. **Network Security Architecture** After formulating IAM user authentication and authorisation, a next step is creating a network security architecture for securely running the customer applications and storing their data in a tenancy. All the 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, next-generation firewalls, IDs). • Creating DNS zones and mappings. An important security consideration in load balancers is using customer Transport Layer Security (TLS) certificates to configure TLS connections to customer's VCN. **Compute Instances Security Configuration** Within a customer VCN, the customer applications run on compute instances including bare metal instances, VM instances, and GPUs. Compute instances are the basic compute building blocks. • Bare metal instances have no Oracle-managed software running on them, which means that the instances and data stored (in memory and local drives) are completely controlled by the customer.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	• VM instances are architected with least-privilege mechanisms and with corporate industry-leading hypervisor security best practices. Depending on security and performance requirements, customers have a choice of using bare metal and VM instances to run their application workloads in their tenancy. It is imperative to securely configure compute instances to maintain the security of customer applications running on them. **Data Storage Security Configuration** Depending on the type of data and access required, customers can store data in local drives (attached to compute instances), remote block volumes, object store buckets, databases, or file storage in their tenancy. To handle these data storage requirements, OCI offers multiple data storage services such as Block Volume, Object Storage, Database, and File Storage. To meet data security requirements, customers need to formulate a tenancy data storage architecture for storing their data in their tenancy, and securely configure the storage services used. Compliance and regulatory requirements are an important factor in determining an appropriate data storage security architecture. OCI API Audit logs record calls to APIs (for example, through the Console, SDKs, CLIs, and custom clients using the APIs) as log events. The API Audit logs are always on by default and cannot be turned off. These logs are available to customers for 90 days, with a retention period configurable up to 365 days. Information in the API Audit logs show what time API activity occurred, the source of the activity, the target of the activity, what the action was, and what the response was. Oracle recommends that customers periodically review the API Audit logs to ensure that they are in accordance with actions they took on their tenancy resources. For more information, see Oracle Cloud Infrastructure Security Features.

Cloud Security Principle 4: Governance Framework

The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
• You should have sufficient confidence that the service has a governance framework and processes which are appropriate for your intended use.	Global Information Security is responsible for security oversight, compliance and enforcement, conducting information-security assessments, leading the development of information security policy and strategy, and training and awareness at the corporate level. This organisation serves as the primary contact for security incident response, providing overall direction for incident prevention, identification, investigation, and resolution. Programs within Global Information Security are dedicated to preserving the confidentiality, integrity, and availability of Oracle information assets and the information assets entrusted to Oracle, including a focus on the following activities: • Defining global corporate technical standards to enable security, privacy, and compliance • Contributing to industry standards such as those issued by the international Organization for Standardization (ISO) and United States National Institute of Standards and Technology (NIST) • Assisting lines of business (LOBs) security organisations with fostering a culture of security across regions and functional area **Information Security Program** Global Information Security manages the Information Security Manager (ISM) Program. Information Security Managers serve as security advocates within their respective LOBs to increase awareness of and compliance with Oracle's security policies, processes, standards, and initiatives. **Oracle Security Oversight Committee** The Oracle Security Oversight Committee (OSOC) brings together senior management from LOBs and security organisations and provides an opportunity to communicate security strategy across the global Oracle organisation. OSOC performs the following actions: • Identifies and addresses corporate security requirements across the global organisation • Nominates and delegates LOBs, organisations, and teams to deliver worldwide security standards, practices, and policies • Communicates recommendations and action plans to senior management across all LOBs

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	Oracle Security Architecture Oversight The Oracle corporate security architect helps set internal information-security technical direction and guides Oracle's IT departments and LOBs toward deploying information security and identity management solutions that advance Oracle 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 uses multiple methods of engaging with leadership and operational security teams responsible for Oracle operations, services, cloud, and all other LOBs. **Oracle Cloud Infrastructure Risk Management** Oracle Cloud Infrastructure Risk Management is responsible for the following tasks: • Incorporating risk management practices into governance and operations • Communicating current, strategic, and emerging risks to operational and leadership teams • Discovering and managing risk • Advising on best practices • Evaluating and advising on risk to relevant teams • Designing security strategy • Architectural review of systems and solutions • Threat intelligence • Technical assessments of component groups and technologies

Cloud Security Principle 5: Operational Security

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
You should have confidence that: • The status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime. • Changes to the service are assessed for potential security impact. Then managed and tracked through to completion.	**Change Management** Oracle Cloud Infrastructure 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.
You should have confidence that: • Potential new threats, vulnerabilities, or exploitation techniques which could affect your service are assessed and corrective action is taken. • Relevant sources of information relating to threat, vulnerability, and exploitation techniques are monitored by the service provider. • The severity of threats and vulnerabilities is considered within the context of the service and this information is used to prioritise the implementation of mitigations.	**Vulnerability Management** The Oracle Critical Patch Update (CPU) and Security Alert Implementation Policy require the deployment of the Oracle CPU and Security Alert patches as well as associated recommendations within a reasonable time of their release. Additional policies require remediation of vulnerabilities in non-Oracle technology. The Oracle Server Security Policy requires servers (both physical and virtual) owned and managed by Oracle and servers managed by third parties for Oracle to be physically and logically secured in order to prevent unauthorized access to the servers and associated information assets. Penetration tests of the system are conducted at least annually. A commercial vulnerability scanning tool is configured to scan all external IP addresses and internal nodes at least quarterly. The results of vulnerability scans and penetration tests are reviewed by management. Vulnerabilities and threats are assessed, documented in a ticket, and tracked through resolution. **Security Event and Information Monitoring** 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.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
• Using a suitable change management process, known vulnerabilities are tracked until mitigations have been deployed. • You know service provider timescales for implementing mitigations and are happy with them.	**Incident Management** Incidents, including incidents reported directly to a customer's account manager, are recorded through an internal, access-controlled electronic ticketing system. Routing, communication, and escalation of incidents vary depending on several factors, including urgency and impact to customers. Incidents reported through My Oracle Support (MOS) or through the external user incident reporting process are routed to OCI personnel and tracked in the electronic ticketing system in the same manner as an internally identified incident. In the event of a security incident, OCI activates an agreed-upon protocol that includes Global Information Security, Global Product Security, and Privacy & Security Legal, as applicable, to provide specialist subject-matter expertise to respond to the incident. If Oracle determines that it is required to report an incident involving the breach of personal information to a customer, Oracle will promptly notify the affected customer.
You should have confidence that: • The service generates adequate audit events to support effective identification of suspicious activity. • These events are analysed to identify potential compromises or inappropriate use of your service. • The service provider takes prompt and appropriate action to address incidents.	**Intrusion Detection** Oracle employs intrusion-detection systems within the Oracle intranet to provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle uses a network-based monitoring approach to detect attacks on open firewall ports within Oracle's intranet. Events are analysed using signature detection, which is a pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to Oracle's IT security for review and response to potential threats. You are responsible for securely configuring and managing your compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform (database configuration) services. **Monitoring and Protection of Audit Log Information** 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.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	Network Protection Oracle's network protections include solutions designed to provide continuity of service, defending against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Events are analysed using signature detection, which is a pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database frequently. **Monitoring and Event Alerts** Alerts are sent to Oracle's IT security and cloud security operations teams for review and response to potential threats. These alerts are monitored 24x7x365.
You should have confidence that: • Incident management processes are in place for the service and are actively deployed in response to security incidents. • Predefined processes are in place for responding to common types of incident and attack. • A defined process and contact route exist for reporting of security incidents by consumers and external entities. • Security incidents of relevance to you will be reported in acceptable timescales and formats.	Reflecting the recommended practices in prevalent security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets. **Incident Response** OCI has incident response mechanisms and processes designed to detect and respond to (potential) security incidents within the security environment that we implement. Oracle notifies you, the customer, if a security incident was confirmed to have led to a personal information breach, following the terms described in the "Incident Management and Breach Notification" section of the Data Processing Agreement for Oracle Cloud Services. 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. **Audit Service** The Audit service logs calls to the OCI public API, whether those calls originated from the Console, SDK, or CLI. 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. See "Overview of Audit" at 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.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	Notifications Oracle will notify you of a confirmed Personal Information Breach without undue delay but at the latest within 24 hours. As information regarding the breach is collected or otherwise reasonably becomes available to Oracle, Oracle will also provide you with the following information: • A description of the nature and reasonably anticipated consequences of the breach • The measures taken to mitigate any possible adverse effects and prevent a recurrence • Where possible, information about the types of personal information that were the subject of the breach

Cloud Security Principle 6: Personnel Security

Where service provider personnel have access to data and systems, the customer needs a high degree of confidence in the service provider's trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
You should have confidence that: • The level of security screening conducted on service provider staff with access to information, or with ability to affect the service, is appropriate. • The minimum number of people necessary have access to information or could affect the service.	Oracle maintains high standards for ethical business conduct at every level of the organisation and at every location where Oracle does business around the world. These standards apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Oracle requires its employees to receive training in ethics and business conduct every two years. **Emphasis on Personnel Security** Oracle emphasises personnel security strongly. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities. These initiatives include personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions. **Employee Screening** In the US, Oracle uses an external screening agency to perform preemployment background investigations for newly hired US personnel. Personnel screening in other countries varies according to local laws, employment regulations, and local Oracle policy. Learn more about Oracle's global background check practices.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	Commitment to Confidentiality Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. **Segregation of Duties and Need-to-Know Principles** Oracle enforces well-defined roles, allowing for segregation of duties among operations staff. Operations are organised into functional groups, where each function is performed by separate groups of employees. Examples of functional groups include database administrators, system administrators, and network engineers. Learn more about Oracle access controls.

Cloud Security Principle 7: Secure Development

Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise data, cause loss of service or enable other malicious activity.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
You should be confident that: • New and evolving threats are reviewed, and the service improved in line with them. • Development is carried out in line with industry good practice regarding secure design, coding, testing, and deployment. • Configuration management processes are in place to ensure the integrity of the solution through development, testing, and deployment.	**Secure Coding Standards** Oracle has formal programs to guide development of software and hardware solutions. Encompassing every phase of the product development life cycle, Oracle Software Security Assurance is Oracle's methodology for building security into the design, building, testing, and maintenance of its products. Oracle's formal programs also focus on security requirements and operations for Oracle Cloud. **Software Development Lifecycle** All Oracle Cloud Infrastructure software development teams follow requirements of OSSA and Oracle Secure Coding Standards. Teams must document their software development life cycle (SDLC), including secure code development practices, peer review, change management for introducing new code into production, and the requirement for annual secure code development training. OCI software development teams must review and update their respective SDLC at least annually.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	Continuous Integration/Continuous Deployment OCI's Continuous Integration/Continuous Deployment (CICD) team champions the creation of an engineering environment that embodies the best development and testing practices to quantitatively ensure that engineers deliver an IaaS offering of high quality, stability, and performance via a continuous integration and deployment model. CICD partners with software development teams responsible for architecture, design, and implementation of OCI's IaaS solutions to increase the velocity and quality of code releases through the product development lifecycle. **Configuration Management** OCI uses industry-standard configuration management tools to manage packages, system configurations, and service configurations on long-lived hosts. Oracle's colocation facility providers only supply power, physical security, and environmental controls for OCI. Colocation facility providers are not permitted to have access to OCI's services or customer applications, workloads, or data.

Cloud Security Principle 8: Supply Chain Security

The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
You understand and accept: • How your information is shared with, or accessible to, third-party suppliers and their supply chains. • How the service provider's procurement processes place security requirements on third-party suppliers. • How the service provider manages security risks from third-party suppliers.	**Oracle Supply Chain Security and Assurance** Oracle has formal policies and procedures designed to ensure the safety of its supply chain. See Oracle Supply Chain Security and Assurance. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers. Oracle also has formal requirements for its suppliers and partners to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when performing the following actions: • Accessing Oracle and Oracle customers' facilities, networks, or information systems • Handling Oracle confidential information and Oracle hardware assets placed in their custody

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
• How the service provider manages the conformance of their suppliers with security requirements. • How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.	In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. For more information about suppliers, see "Oracle Suppliers" at oracle.com/corporate/suppliers.html. **Supply Chain Risk Management** 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: • 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, and continuity and resiliency in Oracle's hardware supply chain, are addressed through a variety of practices: • Multiple-supplier and 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 or end-of-support-life 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

Cloud Security Principle 9: Secure User Management

Your service provider should make the tools available for you to securely manage your use of the service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of the customer's resources, applications and data.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
You should have sufficient confidence that: • You are aware of all the mechanisms by which the service provider would accept management or support requests from you (telephone, web portal, email etc.). • Only authorized individuals from your organisation can use those mechanisms to affect your use and the service.	Oracle Cloud Infrastructure Identity and Access Management (IAM) service lets you control who has access to your cloud resources. You can control what type of access a group of users has and to which specific resources. **Authentication and Authorisation** The customer controls access to and use of their applications, workloads, and data. IAM is built to address the requirements of enterprises,and it provides authentication and authorisation for all their OCI resources and services. An enterprise can use a single tenancy shared by various business units, teams, and individuals while maintaining security, isolation, and governance. When a customer joins OCI, a tenancy is created. A tenancy is a virtual construct that contains all the OCI resources that belong to the customer. The administrator of the tenancy can create users and groups and assign them least-privileged access to resources that are partitioned into compartments. **Separation and Isolation** A compartment is a group of resources that can be managed as a single logical unit, providing a streamlined way to manage large infrastructure. For example, a customer can create a compartment (HR-Compartment) to host a specific set of cloud network, compute instances, and storage volumes necessary to host its HR applications. Compartments are a fundamental component of OCI for organizing and isolating cloud resources. Customers use compartments to clearly separate resources for the purposes of isolation (separating the resources for one project or business unit from another). A common approach is to create a compartment for each major part of an organisation. Unlike most OCI services that are regionally scoped, IAM resources are global. Customers can have a single tenancy across multiple regions.
You should: • Have confidence that other users cannot access, modify, or otherwise affect your service management. • Manage the risks of privileged access using a system such as the "principle of least privilege".	Access control refers to the policies, procedures, and tools that govern access to and use of resources. Examples of resources include a physical server, a file, a directory, a service running an operating system, a table in a database, or a network protocol. • Least privilege is a system-oriented approach in which users' permissions and system functionality are carefully evaluated and access is restricted to the resources required for use or systems to perform their duties. • Default-deny is a network-oriented approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
• Understand how management interfaces are protected and what functionality they expose.	**User Access Management** Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resource databases. Access privileges are granted based on job roles and require management approval. **Privilege Management** Authorisation depends on successful authentication because controlling access to specific resources depends on establishing an entity's or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • **Need to know**: Does the user require this access for their job function? • **Segregation of duties**: Will the access result in a conflict of interest? • **Least privilege**: Is access restricted to only the resources and information required for a legitimate business purpose? **Period Review of Access Rights** Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. **Network Access Controls** Oracle has implemented and maintained strong network controls to address the protection and control of customer data during its transmission from one end system to another. The Oracle Use of Network Services Policy states that computers, servers, and other data devices connected to the Oracle network must comply with well-established standards for security, configuration, and access method.

Cloud Security Principle 10: Identity and Authentication

All access to service interfaces should be constrained to authenticated and authorised individuals.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
• You should have confidence that identity and authentication controls ensure users are authorised to access specific interfaces.	**Authentication and Authorisation** Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorisation, 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. If you are a regular user (not an administrator) who needs to use the OCI resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using. Administrators: For an example of policy that gives groups access to audit logs, see Required IAM Policy. Only members of the Administrators group can modify the Audit log retention period. See Administrators Group and Policy. **Least-Privilege Access** Unnecessary or out-of-date permissions pose a significant threat. Attackers can gain access to them and use them to move throughout a system. To reduce the risk from overly permissioned users or applications, we use the principle of *least-privilege access* when granting access to production systems. We 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, we 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.

Cloud Security Principle 11: External Interface Protection

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

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
You: • Understand what physical and logical interfaces information is available from, and how access to data is controlled. • Have sufficient confidence that the service identifies and authenticates users to an appropriate level over those interfaces.	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 with 18 points of presence (POPs) on five continents and offers fully redundant DNS constellations and multiple Tier 1 transit providers per POP. The solution 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 over 240 billion data points per day. The DNS service also fully supports the 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.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	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. For more information, see OCI Security Features.

Cloud Security Principle 12: Secure Service Administration

Systems used for administration of a cloud service 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.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
You should: • Understand which service administration model is being used by the service provider to manage the service. • Be content with any risks the service administration model in use brings to data or use of the service.	**Secure Administration of the Underlying Stack by Oracle Personnel** Access to network devices and servers that support the services requires Oracle users to use multifactor authentication (MFA) and traverse three levels of access control. The first step in the authentication path is the Oracle Cloud Network Access (OCNA) VPN. OCNA is a multitiered demilitarised zone (DMZ) environment inside a dedicated extranet that is isolated from Oracle's internal corporate network and VPNs for non-cloud services. It functions as a secure access gateway between the user and the target device. OCNA is composed of a gateway subnet, a tools subnet, and a network subnet located in Oracle's DMZ and is protected by firewalls. Only approved engineers with a valid OCNA account can access OCNA.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
	Two-factor authentication is required to authenticate to OCNA. When a user account is created, attributes are defined to describe the specific entitlements that the user is authorised to access. The user is restricted to these resources when connected. The user's access must be approved by an appropriate approver before access is provisioned, and access is revoked when the user is terminated. Before an endpoint can authenticate to the VPN, OCNA is configured to complete a security posture check to determine whether the endpoint is running up-to-date antivirus software, has a local firewall enabled, and is in line with Oracle policies regarding software updates. The second step in the authentication path is authenticating to the relevant bastion server. Operator access is permitted only from bastion servers. Bastion servers are permitted to accept connections only from OCNA subnets. Access to bastion servers is controlled in the following ways: • **Oracle Identity Manager (OIM)**: Only approved engineers with the required OIM entitlement can access the bastion servers. Before the entitlement can be provisioned, the user's access must be approved by an appropriate approver. • **SSH key**: The public and private SSH key of authorised users is used in conjunction with the user's UNIX username and authenticated via LDAP. The user's private key is stored on a virtual slot on the user's token, which requires two-factor authentication to access. The user's corresponding public key is configured on the appropriate bastion servers during the access provisioning process. Users must meet both prerequisites to authenticate to a bastion server. Access to bastion servers is reviewed on a quarterly basis. Inappropriate access identified during the review is investigated and revoked. **Secure Administration of Cloud Services by the Customer** The customer 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 facilitatesthe 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. For more information, see OCI Security Features.

Cloud Security Principle 13: Audit Information for Users

The customer should be provided with the audit records needed to monitor access to the service and the data held within it. The type of audit information available to the customer will have a direct impact on the ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
You should be: • Aware of the audit information that will be provided, how and when it will be made available, the format of the data, and the retention period associated with it. • Confident that the audit information available will meet needs for investigating misuse or incidents.	The Oracle Cloud Infrastructure Audit service automatically records calls to all supported OCI public API endpoints as log events. Currently, all services support logging by Audit. The Object Storage service supports logging for bucket-related events, but not for object-related events. 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, see OCI Security Features.

Cloud Security Principle 14: Secure Use of the Service

The security of cloud services and the data held within them can be undermined if the customer uses the service poorly. Consequently, the customer will have certain responsibilities when using the service in order for data to be adequately protected.

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
You: • Understand any service configuration options available and the security implications of choices. • Understand the security requirements of your use of the service.	**Documentation for Launching, Configuring, Managing and Using Oracle Cloud Infrastructure** Review the Oracle Cloud Infrastructure Documentation, especially the following topics, for information about launching, configuring, managing, and using Oracle Cloud Infrastructure services. • Key Concepts and Terminology • Security Guide • Security Services and Features • Security Best Practices

CONSIDERATIONS	ORACLE CLOUD INFRASTRUCTURE CONTROL OR FEATURE
• Educate your staff using and managing the service how to do so safely and securely.	**Shared Responsibilities for Security** To securely run workloads in OCI, customer must be aware of their security and compliance responsibilities. By design, Oracle provides security of cloud infrastructure and operations (cloud operator access controls, infrastructure security patching, and so on), and customers are responsible for securely configuring their cloud resources. For more information, see Oracle Cloud Infrastructure Security.

NCSC Cloud Security Principles and Oracle Cloud

NCSC outlined several steps that you can take to gain confidence that the security measures that you and your suppliers put in place are working effectively. The recommended approaches are not mutually exclusive. Many of the steps can be combined to provide higher levels of confidence.

The following sections demonstrate how Oracle Cloud Infrastructure enables your organisation to build confidence in cyber security.

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.

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

Validation by an Independent Third Party

Oracle Cloud Infrastructure engages independent auditors and assessors to test and provide opinions about security, confidentiality, and availability controls that are relevant to data protection laws, regulations, and industry standards.

- Ernst & Young CertifyPoint BV (EYCP) audits OCI's Information Security Management System (ISMS) and has issued an ISO/IEC 27001:2013 certificate. In addition, EYCP has issued an ISO/IEC 27017:2015 certificate addressing information security controls for cloud services and ISO/IEC 27018:2014 certificate addressing relevant aspects of protection for personally identifiable information (PII) in public clouds acting as PII processors. OCI's scope for its ISMS is global in nature for both services and regions. Newly deployed services and regions are brought into the ISMS scope upon deployment and are audited by EYCP within our 6 months audit cadence, producing certificate updates by June and December each year.
- Ernst & Young LLP examines OCI in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements 18 (SSAE 18) and the International Auditing and Assurance Standards Board (IAASB) Internal Standard on Assurance Engagements 3000 (ISAE 3000), and issues a System and Organization Control 2 (SOC 2) Type 2 report covering AICPA Trust Services Criteria for controls relevant to security, confidentiality, and availability. OCI's scope under these assurance programs is global in nature for both services and regions. Newly deployed services and regions are aligned with the appropriate security, confidentiality, and availability requirements upon deployment and are audited by Ernst & Young LLP within our 6 months audit cadence, producing assurance reports by June and December each year.
- In addition, Ernst & Young LLP examines OCI in accordance with ISAE 3000 and issues a report addressing relevant criteria found in the Bundesamt fur Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Controls Catalog (C5). OCI's scope under these assurance programs is global in nature for both services and regions. Newly deployed services and regions are aligned with the appropriate C5 requirements upon deployment and are audited by Ernst & Young LLP within our 6 months audit cadence, producing assurance reports by June and December each year.
- Schellman & Company LLC assesses OCI as a Level 1 service provider in accordance with the Payment Card Industry Data Security Standard (PCI DSS). OCI's PCI DSS Attestation of Compliance (AOC) covers all 12 PCI DSS requirements in relation to in-scope IaaS. OCI's scope under PCI is global in nature for both services and regions. Newly developed services and regions meet all applicable PCI DSS requirements upon deployment and are audited by Schellman & Company LLC within our 6 months audit cadence, producing an AOC by June and December each year.

- Secarma Ltd. performed an independent assessment of OCI's cybersecurity practices and issued a Cyber Essentials certificate. The scope of this certificate covers the services and regions within the UK.

For more compliance information, see Oracle Cloud Compliance.

Compliance with Recognized and Appropriate Standards

Oracle Cloud Infrastructure'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" activities 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.

Independent Testers Validate the Implementation of Controls

Oracle Cloud Infrastructure 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 performs penetration tests and 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. All penetration test results and reports are reviewed by Oracle's corporate security teams to validate that an independent and thorough test has been performed.

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 customer support tools or through Sales.

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 cross-organisation working group focused on security architecture, with the goal of collaboratively guiding security for Oracle Cloud. Participation includes members from Oracle Cloud development, operations, and governance teams.

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 done throughout the project life cycle:

- **Prereview**: The risk management teams in each line of business must perform a preassessment 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.

Documentation Relevant to NCSC Cloud Security Principles and Implementation in Oracle Cloud

For the NCSC's full guidance on Cloud Security Principles, see Implementing the Cloud Security Principles.

The following Oracle Cloud Infrastructure documentation provides technical descriptions and guidance for configuring and managing each service, including information about security features and best practices.

- Oracle Cloud Infrastructure documentation: docs.oracle.com/iaas/Content/home.htm
- "Key Concepts and Terminology": docs.oracle.com/iaas/Content/GSG/Concepts/concepts.htm
- "Security Guide": docs.oracle.com/iaas/Content/Security/Concepts/security_guide.htm
- "Security Services and Features": docs.oracle.com/iaas/Content/Security/Concepts/security_features.htm
- "Security Best Practices": docs.oracle.com/iaas/Content/Security/Reference/configuration_security.htm

Oracle has corporate security practices that encompass all the functions related to security, safety, and business continuity for Oracle's internal operations and its provision of services to customers. They include a suite of internal information security policies and different customer-facing security practices that apply to different services.

Oracle Cloud Security Practices describes Oracle's controls designed to protect the confidentiality, integrity, and availability of customer data and systems that are hosted in Oracle Cloud, accessed when providing cloud services, or both. To find out more, see "Oracle Corporate Security Practices" at oracle.com/corporate/security-practices.

Security in OCI is a shared responsibility between you and Oracle:

- Oracle is responsible for the security of the underlying cloud infrastructure (such as data centre facilities, and hardware and software systems). See "Oracle Corporate Security Practices" at oracle.com/corporate/security-practices.
- You, the customer, are responsible for securing your workloads and securely configuring services (such as compute, network, storage, and database). See "Shared Security Model" at docs.oracle.com/iaas/Content/Security/Concepts/security_overview.htm#Shared_Security_Model.

Oracle complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the EU to the US. Oracle is also responsible for ensuring that third parties who act as an agent on our behalf do the same.

Oracle has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in our privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, visit https://www.privacyshield.gov/list.

For personal information received or transferred pursuant to the Privacy Shield Framework, Oracle is subject to the regulatory enforcement powers of the US Federal Trade Commission.

Oracle continues to adhere to the underlying European privacy principles of the US-Swiss Safe Harbor for the processing of Personal Information received from Switzerland. To learn more about the Safe Harbor program, and to view our certification, visit https://safeharbor.export.gov/swisslist.aspx.

OCI is an IaaS product in which responsibility for data security and data privacy is shared between Oracle and its customers. Oracle defines two broad categories of data in its interactions with customers:

- **Data about our customers**: The contact and related information needed to operate an OCI account and bill for services. The use of any personal information that we gather for purposes of account management is governed by the "Oracle General Privacy Policy" at oracle.com/legal/privacy/privacy-policy.html.
- **Data stored by our customers**: The data that customers store in OCI, such as files, documents, and databases. We don't have insight into the contents of this data. Our handling of this data is described by the "Oracle Services Privacy Policy" at oracle.com/legal/privacy/services-privacy-policy.html and the "Data Processing Agreement" for Oracle Services at oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing.

Oracle Cloud Infrastructure and the GDPR explains how the features and functionality of OCI can help customers meet General Data Protection Regulation (GDPR) requirements.

Oracle has standard contracts and policies that govern the terms, service descriptions, and delivery of cloud services. To find out more, review the following documentation:

- "Data Processing Agreement for Cloud Services" at oracle.com/us/corporate/contracts/cloud-dpa-soc-4261012.pdf
- "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

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