ORACLE
Cloud Infrastructure

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

Oracle Cloud Infrastructure

January 2019

ORACLE

ORACLE CONFIDENTIAL

Terms of Use

The information in this document is provided on an “AS-IS” basis without warranty, is subject to change, and is confidential information under the terms of your contract with Oracle by which you have acquired the product or services related to this document. In the absence of such a contract with Oracle, your use and disclosure of the information in this document is protected by intellectual property laws. Notwithstanding anything to the contrary, you are restricted from disclosing any information contained within this document to any third party. However, you may disclose such information to your employees and external auditors only as necessary, provided that such employees and auditors protect the confidentiality of the information.

By using this document, you are agreeing to the Terms of Use located at http://www.oracle.com/us/legal/terms/index.html.

For the purpose of such Terms of Use, the information in this document shall be treated as Content (as defined in the Terms of Use) provided on or through an Oracle Web Site.

Table of Contents

I. Introduction to Using the Cloud Security Principles

National Cyber Security Centre (NCSC) guidance summarises 14 essential security principles (the NCSC Cloud Security Principles) to consider when evaluating cloud services and provides context on why these may be important to an organisation.

Customers should decide which of the NCSC Cloud Security Principles are important and how much (if any) assurance they require in the implementation of these principles.

Providers of cloud services should consider NCSC Cloud Security Principles when presenting their offerings to consumers. This will allow them to make informed choices about which services are appropriate for their needs.

This whitepaper is intended to provide the reader and customers with an understanding of:

- How Oracle Cloud Infrastructure's administrative, physical and technical safeguards relevant to security, confidentiality and availability align with NCSC Cloud Security Principles.
- How the responsibilities for security and implementation of the NCSC guidance are shared between Oracle Cloud Infrastructure (*provider* of cloud services) and the customer (*consumer* of cloud services).
- How the customer can approach information security risk management and implementation of the NCSC Cloud Security Principles guidance using Oracle Cloud Infrastructure services.

II. Overview of Oracle Cloud Infrastructure Services

Oracle Cloud Infrastructure combines the elasticity and utility of public cloud with the granular control, security, and predictability of on-premises infrastructure to deliver high-performance, high-availability and cost-effective infrastructure as a service (IaaS).

As a result, customers can provision elastic, self-service and pay-as-you-go bare metal cloud servers. Oracle's next-generation infrastructure will also allow running bare metal servers side-by-side with any class of system from virtual machines (VMs) to engineered systems.

Services include:

- Archive Storage
- Audit
- Block Volumes
- Cloud Access Security Broker (CASB) Cloud Service
- Compute
- Container Engine for Kubernetes
- Data Transfer
- Database
- Database – 2-node Real Application Clusters (RAC)
- Database – Autonomous Data Warehouse
- Database – Autonomous Transaction Processing
- Database – Exadata
- Distributed Denial of Service (DDoS) Protection
- Domain Name System (DNS)
- Email Delivery
- FastConnect
- File Storage Service (FSS)
- Identity and Access Management (IAM)
- Key Management Service (KMS)
- Load Balancing
- Object Storage
- Registry
- Storage Gateway
- Virtual Cloud Network (VCN)

Oracle Cloud Infrastructure maintains its head office in Seattle, Washington, USA, and Operations Command Centres in Seattle, Washington, USA and Dublin, Ireland. Data centres, which house the hardware supporting the services listed above, are located in Ashburn, Virginia, USA; Phoenix, Arizona, USA; Frankfurt am Main, Federal Republic of Germany, and London, United Kingdom.

III. National Cyber Security Centre (NCSC) Cloud Security Principles and Oracle Cloud Infrastructure

To assist customers with evaluating Oracle Cloud Infrastructure services, the following statements address topics used in the guidance supplementary to the National Cyber Security Centre (NCSC) Cloud Security Principles, NCSC's "*Having confidence in cyber security*":

1. 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 Hosting and Delivery Policies and Pillar Documents describe how Oracle will deliver cloud services, including how Oracle addresses security, change management, and backups.

2. 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 which are relevant to data protection laws, regulations and industry standards.

Ernst & Young CertifyPoint (EYCP), a Certification Body accredited by the Dutch Accreditation Council (Raad voor Accreditatie or RvA), audits and certifies Oracle Cloud Infrastructure's Information Security Management System (ISMS). EYCP first issued an ISO/IEC 27001:2013 certificate in 2017. EYCP performs annual surveillance audits of Oracle Cloud Infrastructure's ISMS to verify compliance with the international standard.

Secarma Limited, a Certification Body accredited by QG Business Solutions, assesses and certifies Oracle Cloud Infrastructure in accordance with the Cyber Essentials scheme promulgated by the National Cyber Security Centre (NCSC). Secarma first issued a Cyber Essentials Plus certificate in 2018 and performs annual assessments to verify ongoing compliance with the scheme.

Ernst & Young LLP examines Oracle Cloud Infrastructure every six months in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements 18 (SSAE 18) and International Auditing and Assurance Standards Board (IAASB) International Standard on Assurance Engagements 3000 (ISAE 3000) and issues a Service Organization Control 2 (SOC 2) Type 2 attestation covering AICPA Trust

Services Principles and Criteria for controls relevant to security, confidentiality and availability in relation to in-scope infrastructure as a service (IaaS).

Schellman & Company, LLC, assesses Oracle Cloud Infrastructure annually in accordance with Payment Card Industry Data Security Standard (PCI DSS). Oracle Cloud Infrastructure's Attestation of Compliance (AOC) for a Service Provider covers all 12 PCI DSS requirements in relation to in-scope IaaS.

3. Compliance with a Recognised and Appropriate Standard

Oracle Cloud Infrastructure's ISO/IEC 27001:2013 certification covers its Information Security Management System (ISMS). The ISMS is centrally managed from Oracle Cloud Infrastructure's main office in Seattle, Washington, USA. In-scope applications, systems, people and processes are globally implemented and operated by teams located in Seattle, Washington, USA, and Dublin, Ireland, and regions including North America and Europe, Middle East and Africa.

Oracle Cloud Infrastructure's Cyber Essentials Plus certification provides independent verification of cyber security safeguards from an accredited Certification Body. The National Cyber Security Centre (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.

Oracle Cloud Infrastructure'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 Oracle Cloud Infrastructure's in-scope services, tests of controls and results of testing outlined in the report provide customers with assurance that Oracle Cloud Infrastructure's service commitments and requirements were achieved based on the applicable AICPA Trust Services Principles and Criteria.

Oracle Cloud Infrastructure has implemented PCI DSS into "business-as-usual" activities as part of its overall security strategy. This enables Oracle Cloud Infrastructure to continuously monitor the effectiveness of security controls and designed to maintain a PCI DSS compliant environment in between annual PCI DSS assessments.

4. Independent Testers Validate the Implementation of Controls

Oracle Cloud Infrastructure engages an independent third party to perform periodic external vulnerability scans of its public IP address ranges. Oracle Cloud Infrastructure also maintains a staff of qualified information security professionals who perform periodic internal vulnerability scans of its non-public IP address ranges as well as internal and external penetration tests of both public and non-public IP address ranges.

5. Security Architecture Review

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

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

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

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

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience.

IV. Documentation Relevant to National Cyber Security Centre (NCSC) Cloud Security Principles and Implementation in the Oracle Cloud

For the NCSC's full guidance on Cloud Security Principles, please review the following documentation.

- Implementing the Cloud Security Principles

The following Oracle Cloud Infrastructure documentation provides technical descriptions and guidance for configuring and managing each service including information on security features and best practices, which are used below in section V, mapping Oracle Cloud Infrastructure controls and features to the NCSC Cloud Security Principles.

- Oracle Cloud Infrastructure Documentation
  - Key Concepts and Terminology
  - Security Guide
  - Security Features
  - Security Best Practices

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 as well as 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 the Oracle Cloud and/or accessed when providing cloud services. This information is also used below in section V, aligning Oracle Cloud Infrastructure controls and features to the NCSC Cloud Security Principles.

To find out more, please review the following documentation.

- Oracle Corporate Security Practices

Oracle Cloud Infrastructure is an infrastructure as a service (IaaS) product, in which responsibility for security is shared between Oracle Cloud Infrastructure and the customer.

To securely run workloads in Oracle Cloud Infrastructure, the customer must be aware of its 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, please review the following documentation.

- Oracle Cloud Infrastructure Security

Likewise, privacy compliance is also a shared responsibility between Oracle Cloud Infrastructure and the customer. The following documentation explains how the features and functionality of Oracle Cloud Infrastructure can help customers meet General Data Protection Regulation (GDPR) requirements.

- Oracle Cloud Infrastructure and the GDPR

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

- Oracle's New Data Processing Agreement for Cloud Services
- Oracle Cloud Services Contracts
- Cloud Services Hosting and Delivery Policies

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

The following section includes the detailed breakdown of each of the 14 Cloud Security Principles described by the NCSC.

Information on both customer considerations and Oracle Cloud Infrastructure implementation can be found 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" which the user (customer) should be confident in when analyzing 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 user (customer) to enable secure architecture specific to the nature of each Cloud Security Principle.

Depending on the considerations for each given Cloud Security Principle, the Oracle Cloud Infrastructure control or feature will focus on the service(s) as applicable where the security features are implemented.

Cloud Security Principle 1: Data in Transit Protection

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

Considerations	Oracle Cloud Infrastructure Control or Feature
The customer should consider how: - 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).	Oracle Cloud Infrastructure provides the customer with multiple forms of encryption for data in transit. **Application Programming Interface (API) Encryption** All Oracle Cloud Infrastructure Application Programming Interface (API) requests must support HTTPS and SSL protocol TLS 1.2. **Virtual Private Networks (VPNs)** Oracle Cloud Infrastructure 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 VPN. **Private Connections** Oracle Cloud Infrastructure FastConnect offers a dedicated, private connection between the customer's data centre and Oracle Cloud Infrastructure. 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 Oracle Cloud Infrastructure (e.g., to implement a hybrid cloud, or a lift-and-shift scenario). Communication across the connection is with IPv4 private addresses (typically RFC 1918).

Cloud Security Principle 1: Data in Transit Protection

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

Considerations	Oracle Cloud Infrastructure Control or Feature
	• Public peering: To access public services in Oracle Cloud Infrastructure without using the Internet. For example, Object Storage, the Oracle Cloud Infrastructure 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 of 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 a customer to run its 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 type of VCN external connectivity whether internet, on-premises network, peered VCN, or 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.

Cloud Security Principle 1: Data in Transit Protection

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

Considerations	Oracle Cloud Infrastructure Control or Feature
	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 the customer's instances. A security list is configured at the subnet level and enforced at the instance level. The customer can apply multiple security lists to a subnet. A network packet is allowed if it matches any rule in the security lists. Gateways let resources in a VCN communicate with destinations outside the VCN. The gateways include: • **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 Oracle Cloud Infrastructure services such as Object Storage • **Local peering gateway (LPG):** for connectivity to a peered VCN in the same region

Cloud Security Principle 1: Data in Transit Protection

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

Considerations	Oracle Cloud Infrastructure Control or Feature
	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: • Virtual Cloud Network Overview and Deployment Guide • NAT Instance Configuration • Deploying VPN IPSec Tunnels with Cisco ASA/ASAv VTI on Oracle Cloud Infrastructure • 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 consider: - in which countries its data will be stored, processed and managed. - how the customer's use of cloud services affects compliance with relevant legislation (e.g., the Data Protection Act 2018 and the General Data Protection Regulation) and whether the legal jurisdiction(s) within which the service provider operates are acceptable.	**Jurisdiction Control** In its capacity as data controller, the customer determines which regions or availability domains it will deploy services in and where it will store its data. In its capacity as data processor, Oracle Cloud Infrastructure does not have a direct relationship with the customer's data subjects, nor does it have insight into the data that the customer has collected from data subjects. For additional information on data protection principles and compliance, see Oracle Cloud Infrastructure and the GDPR. **Data Centre Assurance** Co-location facilities have their own ISO/IEC 27001:2013 certifications and/or SOC 2 Type 2 attestations. Oracle Cloud Infrastructure performs an annual review of available certifications and assurance reports from each facility and periodic on-site compliance inspections. Oracle Cloud Infrastructure's independent auditors conduct periodic on-site walkthroughs to ensure data centre controls are in place and operating.

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
- whether storage media containing data are protected from unauthorised access. - whether data is erased when resources are moved or re-provisioned, when the customer leaves the service or when the customer requests it to be erased. - whether storage media which has held customer data is sanitised or securely destroyed at the end of its life.	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. **Data at Rest Protection: Encryption by Default** By default, Oracle Cloud Infrastructure Block Volumes and associated backups are encrypted at rest using AES-256. The customer can also encrypt data volumes using tools like dm-crypt, veracrypt, and Bit-Locker. All data in Oracle Cloud Infrastructure Object Storage is encrypted at rest by using AES-256. Encryption is on by default and cannot be turned off. Each object is encrypted with its encryption key, and the object encryption keys are encrypted with a master encryption key. In addition, the customer can use client-side encryption to encrypt objects with encryption keys before storing them in object store buckets. User-created tablespaces are encrypted by default in Oracle Cloud Infrastructure Database. In these databases, ENCRYPT_NEW_TABLESPACES parameter is set to CLOUD_ONLY where tablespaces created in a Database Cloud Service (DBCS) database are transparently encrypted with the AES128 algorithm unless a different algorithm is specified. Oracle Cloud Infrastructure File Storage exposes an NFSv3 endpoint as a mount target in each customer's VCN subnet. All file-system data is encrypted at rest using AES-128.

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
- whether equipment potentially containing customer data, credentials, or configuration information for the service is identified at the end of its life (or prior to being recycled). - whether any components containing sensitive data are sanitised, removed or destroyed as appropriate. - whether availability commitments of the	**Data at Rest Protection: Crypto-key Management** Oracle Cloud Infrastructure Key Management provides the customer with centralised management of the encryption of data. The customer can use Key Management to create master encryption keys and data encryption keys, rotate keys to generate new cryptographic material, enable or disable keys for use in cryptographic operations, assign keys to resources, and use keys for encryption and decryption. Oracle Cloud Infrastructure Object Storage and Oracle Cloud Infrastructure Block Volume integrate with Key Management to support encryption of data in buckets and block or boot volumes. Integration with Oracle Cloud Infrastructure Identity and Access Management (IAM) lets the customer control who and what services can access which keys and what they can do with those keys. Oracle Cloud Infrastructure Audit integration gives the customer a way to monitor key usage. Audit tracks administrative actions on keys and vaults. Keys are stored on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification. Key Management uses the Advanced Encryption Standard (AES) as its encryption algorithm and its keys are AES symmetric keys. **Data Sanitisation and Equipment Disposal** Oracle's *Media Sanitization and Disposal Policy* sets forth the requirements for removal of information from electronic storage media including sanitization 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.

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
service, including their ability to recover from outages, meets business needs.	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 sanitization. **Physical Resilience and Availability** Oracle Cloud Infrastructure is hosted in regions and availability domains. A region is a localised geographic area, and an availability domain is one or more data centres located within a region. A region is composed of several availability domains. Most Oracle Cloud Infrastructure resources are either region-specific, such as a VCN, or availability domain-specific, such as a compute instance. Availability domains are isolated from each other, fault tolerant, and designed against failing simultaneously. Because availability domains do not share infrastructure such as power or cooling or the internal availability domain network, a failure at one availability domain is designed to not impact the availability of the others. All the availability domains in a region are connected to each other by a low-latency, high-bandwidth network, which makes it possible for the customer to provide high-availability connectivity to the Internet and customer premises, and to build replicated systems in multiple availability domains for both high availability and disaster recovery. Regions are completely independent of other regions and can be separated by vast distances— across countries or even continents. Generally, the customer would deploy an application in the region where it is most heavily

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
	used since using nearby resources is faster than using distant resources. However, the customer can also deploy applications in different regions to: • Mitigate the risk of region-wide events, such as large weather systems or earthquakes • Meet varying requirements for legal jurisdictions, tax domains, and other business or social criteria The customer is responsible for designing and implementing high availability and disaster recovery capabilities according to business needs, internal policies and industry or regulatory compliance requirements. For more information, see Best Practices for Deploying High Availability Architecture on Oracle Cloud Infrastructure and Best Practices for Disaster Recovery in Oracle Cloud Infrastructure.

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
The customer needs to consider: - the types of user it shares the service or platform with. - whether the service provides sufficient separation of customer data and service from other users of the service. - how management of the customer's instances of the service are kept separate from other users.	Security of an Oracle Cloud Infrastructure tenancy is based on a combination of factors. The following steps provide high-level guidelines for configuring security of a tenancy. **User authentication and authorization** The initial step in securely configuring a tenancy is to create mechanisms for authenticating users and authorizing users to access tenancy resources in a least-privilege manner. This step comprises creating Oracle Cloud Infrastructure Identity and Access Management (IAM) users, creating IAM groups, formulating authentication mechanisms (for example, Console access using password, API access using API keys, and auth token for object store) for the IAM users created, grouping customer tenancy resources into logical groups using compartments, and 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 polices, and federation mechanisms. **Network security architecture** After formulating IAM user authentication and authorization, 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. VCN is a software-

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
	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 type of VCN external connectivity whether internet, on-premises network, peered VCN, or 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 (BM) instances, Virtual Machine (VM) instances and GPUs. Compute instances are the basic compute building blocks. Bare metal instances have no Oracle-managed software running on them, with the result that the instances and data stored (in memory and local drives) are completely controlled by the customer. 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 BM and VM instances,

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
	to run their application workloads in their tenancy. It is imperative to securely configure compute instances, to maintain 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, Oracle Cloud Infrastructure offers multiple data storage services such as Block Volume, Object Storage, Database, and File Storage. In order 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. 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 can't be turned off. These logs are available to customers for 90 days, with 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 OCI API Audit logs to ensure they are in accordance with actions they took on their tenancy resources. See Oracle Cloud Infrastructure Security Features for more information.

Cloud Security Principle 4: Governance

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
The customer needs to consider: - whether the service has a governance framework and processes which are appropriate.	Oracle provides IT security oversight and governance to identify and globally implement security controls and processes aligned with organizational objectives. Oracle is supported by the following security groups. **Oracle Security Oversight Committee (OSOC)** Oracle's Security Oversight Committee (OSOC) brings together senior management from Lines of Business and security organizations and provides an opportunity to communicate security strategy across the global Oracle organization. OSOC: • Identifies and addresses corporate security requirements across the global organization. • Nominates and delegates Lines of Business (LOBs), organizations and teams to deliver worldwide security standards, practices and policies. • Communicates recommendations and action plans to senior management across all LOBs. **Oracle Global Information Security (GIS)** Oracle Global Information Security (GIS) is responsible for security oversight; compliance; enforcement; conducting information security assessments; leading the development of information security policy and strategy, as well as training and awareness at the corporate level. GIS security policies are available to

	employees on the GIS Policy Portal. GIS also serves as the primary contact for security incident response, providing overall direction for incident prevention, identification, investigation, and resolution. **Oracle Cloud Infrastructure Chief Security Officer** Oracle Cloud Infrastructure has appointed a Chief Security Officer who directs the Security organization and the information security management system (ISMS) within the LOB. Within the LOB, the Chief Security Officer oversees the following functions: • Security Architecture • Offensive Security • Detection and Response Team (DART) • Security Services Development • Access Control Ecosystem • Security Products • Threat and Vulnerability Management (TVM) • Continuous Security Integration Services (CSIS) **Oracle Cloud Infrastructure Risk Management** Oracle Cloud Infrastructure Risk Management is responsible for incorporating risk management practices into governance and operations; communicating current, strategic, and emerging risks to operational and leadership teams; risk discovery and management; advising on best practices; evaluating and advising on risk to relevant teams; design of security strategy; architectural review of systems and solutions; threat intelligence, and 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
The customer needs to consider: - configuration and change management – ensuring that changes to the system have been properly tested and authorised and that changes should not unexpectedly alter security properties. - vulnerability management – identifying and mitigating security issues in constituent components.	**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 minimum, and outlines the processes and procedures to be followed for each change. The process incorporates segregation of duties (SoD) 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 which 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. Oracle Cloud Infrastructure has implemented an emergency change process which requires all changes that are to be implemented within 24 hours or during a change freeze to require the approval of a member of the Operations Team and Senior Manager prior to the change being implemented.

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
- protective monitoring – putting measures in place to detect attacks and unauthorised activity on the service. - incident management – ensuring the ability to respond to incidents and recover a secure, available service.	**Vulnerability Management** 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** Oracle Cloud Infrastructure has deployed a security information and event monitoring (SIEM) solution which ingests and stores security-related logs and alerts from networking devices, hosts and other components within the infrastructure. Oracle Cloud Infrastructure's Detection and Response Team (DART) monitors the SIEM for event correlations and other relevant detection scenarios on a 24x7x365 basis designed to defend and protect against unauthorised intrusions and activity in the production environment. **Incident Management** Incidents, including incidents reported directly to a customer's account manager, are recorded via an internal access-controlled electronic ticketing system. Routing, communication, and escalation of incidents vary depending on a number of factors including urgency and impact to customers. The severity definitions are detailed below. Incidents reported via My Oracle Support (MOS) or through the external user incident reporting

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
	process are routed to Oracle Cloud Infrastructure personnel and tracked in the electronic ticketing system in the same manner as an internally identified incident. In the event of a security incident, Oracle Cloud Infrastructure activates an agreed protocol which includes GIS, Global Product Security, and Privacy & Security Legal, as applicable, to provide specialist subject matter expertise to respond to the incident. In the event that 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.

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
The customer needs to consider: - 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.	**Access to Customer Data** Oracle Cloud Infrastructure does not have access to the customer's Virtual Cloud Network (VCN), applications, workloads or data. The customer controls access to and the use of its data during the time it uses Oracle Cloud Infrastructure services. **Oracle Human Resources** Human Resources (HR) is a corporate function at Oracle. The controls in this section are applicable to the global employee population including Oracle Cloud Infrastructure employees. HR representatives are assigned to the business areas within Oracle. HR utilises a number of Oracle Human Resources Management Systems and tools (HR systems) for their operations. Personnel procedures vary according to local Oracle policy, laws, and regulations. There are formal procedures for hiring new employees (traditional new hire or through a merger or acquisition), which follow corporate directives and in-country regulations and processes. A manager, with a need for a new employee, accesses a HR self-service application, creates the job requisition, and forwards it to the Recruitment Team for review and approval in accordance with the local process.

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
	Résumés or curricula vitae (CVs) are reviewed before selecting candidates for interviews. The hiring manager and a recruiter, if requested by the manager, initially interview potential candidates. The candidate then continues the interview process with multiple interviewers selected based on their experience, role, and subject matter expertise. After a candidate has been successfully identified, the offer process is initiated. For Oracle candidates, there is a formal approval matrix which indicates the level of approval required for offers and transfers based on the terms of the transaction (e.g., position, salary, etc.). **Background Checks** Background checks are performed on candidates selected for hire in accordance with local laws and regulations and local Oracle policy. Oracle's supplier agreements require the suppliers of contract personnel to perform background screening of non-direct Oracle workers (sub-contractors) before assigning an individual to Oracle to the extent permitted by local laws and regulations and local Oracle policy. In the event a non-direct worker is hired as a direct Oracle employee, they are subject to the mandatory Oracle background checks for their location. **Training**

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
	New employees are supported by a new-hire web site and orientation courses. Orientations are available in a number of formats. Depending on the location, orientations may take place via on-line e-course, live web broadcast, or during face-to-face onboarding sessions. Ongoing training is available to all employees through a variety of courses delivered through web learning, Oracle University and external courses. Training for each employee is tailored to support his or her job role.

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
The customer needs to consider: - 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	**Secure Coding Standards** Oracle has documented *Secure Coding Standards* that provide software developers specific guidance on how to avoid introducing known types of security flaws when writing code. The Secure Coding Standards are part of the wider Oracle Software Security Assurance (OSSA) program and are based on Software Engineering Institute Computer Emergency Response Team (SEI CERT) rules and Oracle internal directives. **Software Development Lifecycle** All Oracle Cloud Infrastructure software development teams follow requirements of OSSA and Oracle *Secure Coding Standards* and must document their software development lifecycle (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. Oracle Cloud Infrastructure software development teams must review and update their respective SDLC at least annually. **Continuous Integration/Continuous Deployment** Oracle Cloud Infrastructure'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

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
development, testing and deployment.	continuous integration and deployment model. CICD partners with software development teams responsible for architecture, design, and implementation of Oracle Cloud Infrastructure's IaaS solutions to increase the velocity and quality of code releases through the product development lifecycle. **Configuration Management** Oracle Cloud Infrastructure uses industry-standard configuration management tools to manage packages, system configurations, and service configurations on long-lived hosts.

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
The customer needs to consider: - how 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's co-location facility providers only supply power, physical security and environmental controls for Oracle Cloud Infrastructure. Co-location facility providers are not permitted to have access to Oracle Cloud Infrastructure's services or customer applications, workloads or data. Oracle's Supplier Security Program is aligned with ISO 27000 series and is designed to identify, manage and mitigate information security risk for suppliers used by Oracle. Supplier security assessments are performed as part of the Supplier Security Program in order to review suppliers' compliance with Oracle's information and physical security standards, identify gaps and advise on remediation. **Co-location Facility Security** Each co-location facility has its own ISO/IEC 27001:2013 certification and/or SOC 2 Type 2 attestation. Oracle Cloud Infrastructure performs an annual review of available assurance reports from each facility and periodic on-site compliance inspections. Oracle cloud Infrastructure'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.

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
- 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.	**Hardware Security** Oracle Cloud Infrastructure sources hardware from well-known hardware vendors including Oracle (Sun), Arista, Juniper, Cavium and other well-known vendors. Hardware vendors are required to implement and maintain appropriate technical and organizational measures designed to protect personal information against any misuse, accidental, unlawful or unauthorised destruction, loss, alteration, disclosure, acquisition or access. In addition, Suppliers to Oracle are required to comply with the IT, physical and environmental and human resources security, confidentiality, training, compliance and audit, business continuity and disaster recovery, and security incident and reporting requirements set forth in *Oracle Supplier Information and Physical Security Standards (OSSS)* and the *Oracle Supplier Code of Ethics and Business Conduct (OSCoE).* To address evolving business risks, security standards and regulatory compliance requirements, Oracle reviews the OSSS and OSCoE at least annually and makes updates as needed at any point in time.

Cloud Security Principle 9: Secure User Management

The service provider should make the tools available for the customer to securely manage 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
The customer needs to consider: - authentication of users to management interfaces and support channels. - separation and access control within management interfaces.	**Authentication and Authorization** The customer controls access to and use of its applications, workloads and data. The Oracle Cloud Infrastructure Identity and Access Management (IAM) service is built to meet the requirements of enterprises, and it provides authentication and authorization for all their Oracle Cloud Infrastructure 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 Oracle Cloud Infrastructure, a tenancy is created. A tenancy is a virtual construct that contains all of the Oracle Cloud Infrastructure 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.

Cloud Security Principle 9: Secure User Management

The service provider should make the tools available for the customer to securely manage 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
	Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating cloud resources. Customers use them 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 organization. Unlike most Oracle Cloud Infrastructure services that are regionally scoped, the IAM service resources are global. Customers can have a single tenancy across multiple regions. The following are key IAM: • **Resource:** A cloud object that a company's employees create and use when interacting with Oracle Cloud Infrastructure services, for example, compute instances, block storage volumes, virtual cloud networks (VCNs), subnets, and route tables. • **Policy:** A set of authorization rules that define access to resources within a tenancy. • **Compartment:** A heterogeneous collection of resources for the purposes of security isolation and access control. • **Tenancy:** The root compartment that contains all of an organization's resources. Within a tenancy, administrators can create one or more compartments, create more users and groups, and assign policies that grant groups the ability to use resources within a compartment.

Cloud Security Principle 9: Secure User Management

The service provider should make the tools available for the customer to securely manage 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
	• **User:** A human being or system that needs access to manage their resources. Users must be added to groups in order to access resources. Users have one or more credentials that must be used to authenticate to Oracle Cloud Infrastructure services. Federated users are also supported. • **Group:** A collection of users who share a similar set of access privileges. Administrators can grant access policies that authorise a group to consume or manage resources within a tenancy. All users in a group inherit the same set of privileges. • **Identity Provider:** A trusted relationship with a federated identity provider. Federated users who attempt to authenticate to the Oracle Cloud Infrastructure console are redirected to the configured identity provider. After successfully authenticating, federated users can manage Oracle Cloud Infrastructure resources in the console just like a native IAM user. Currently, Oracle Cloud Infrastructure supports the Oracle Identity Cloud Service and Microsoft Active Directory Federation Service (ADFS) as identity providers. Federated groups are mapped to native IAM groups to define the policies apply to a federated user. All customer calls to access Oracle Cloud Infrastructure resources are first authenticated by the IAM service (or federated provider) and then authorised based on IAM policies. A customer can create a policy that gives a set of users permission to access the infrastructure resources (network, compute, storage, and so on) within a

Cloud Security Principle 9: Secure User Management

The service provider should make the tools available for the customer to securely manage 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
	compartment in the tenancy. These policies are flexible and are written in a human-readable form that is easy to understand and audit. **Authentication Credentials** Each user has one or more of the following credentials to authenticate themselves to Oracle Cloud Infrastructure. Users can generate and rotate their own credentials. In addition, a tenancy security administrator can reset credentials for any user within their tenancy. • **Console password:** Used to authenticate a user to the Oracle Cloud Infrastructure Console. • **API key:** All API calls are signed using a user-specific 2048-bit RSA private key. The user creates a public key pair, and uploads the public key in the Console. • **Auth token:** Auth tokens are Oracle-generated token strings that the customer can use to authenticate with third-party APIs that do no support Oracle Cloud Infrastructure's signature-based authentication. For example, use an auth token to authenticate with an OpenStack Swift client. To ensure sufficient complexity, the token is created by the IAM service and cannot be provided by a customer. • **Customer secret key:** Used by Amazon S3 clients to access the Object Storage service's S3-compatible API. To ensure sufficient complexity, the password is created by the IAM service and cannot be provided by a customer.

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
The customer needs to consider: - whether identity and authentication controls ensure users are authorised to access specific interfaces.	**Authentication and Authorization** The customer controls access to and use of its applications, workloads and data. The Oracle Cloud Infrastructure Identity and Access Management (IAM) service is built to meet the requirements of enterprises, and it provides authentication and authorization for all their Oracle Cloud Infrastructure 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 Oracle Cloud Infrastructure, a tenancy is created. A tenancy is a virtual construct that contains all of the Oracle Cloud Infrastructure 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 Oracle Cloud Infrastructure for organizing and isolating cloud resources.

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
	Customers use them 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 organization. Unlike most Oracle Cloud Infrastructure services that are regionally scoped, the IAM service resources are global. Customers can have a single tenancy across multiple regions. The following are key IAM concepts: • **Resource:** A cloud object that a company's employees create and use when interacting with Oracle Cloud Infrastructure services, for example, compute instances, block storage volumes, virtual cloud networks (VCNs), subnets, and route tables. • **Policy:** A set of authorization rules that define access to resources within a tenancy. • Compartment: A heterogeneous collection of resources for the purposes of security isolation and access control. • **Tenancy:** The root compartment that contains all of an organization's resources. Within a tenancy, administrators can create one or more compartments, create more users and groups, and assign policies that grant groups the ability to use resources within a compartment. • **User:** A human being or system that needs access to manage their resources. Users must be added to groups in order to access resources. Users have one or more credentials that must be used to authenticate to Oracle Cloud Infrastructure services. Federated users are also supported.

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
	• **Group:** A collection of users who share a similar set of access privileges. Administrators can grant access policies that authorise a group to consume or manage resources within a tenancy. All users in a group inherit the same set of privileges. • **Identity Provider:** A trusted relationship with a federated identity provider. Federated users who attempt to authenticate to the Oracle Cloud Infrastructure console are redirected to the configured identity provider. After successfully authenticating, federated users can manage Oracle Cloud Infrastructure resources in the console just like a native IAM user. Currently, Oracle Cloud Infrastructure supports the Oracle Identity Cloud Service and Microsoft Active Directory Federation Service (ADFS) as identity providers. Federated groups are mapped to native IAM groups to define the policies apply to a federated user. All customer calls to access Oracle Cloud Infrastructure resources are first authenticated by the IAM service (or federated provider) and then authorised based on IAM policies. A customer can create a policy that gives a set of users permission to access the infrastructure resources (network, compute, storage, and so on) within a compartment in the tenancy. These policies are flexible and are written in a human-readable form that is easy to understand and audit.

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
	Authentication Credentials Each user has one or more of the following credentials to authenticate themselves to Oracle Cloud Infrastructure. Users can generate and rotate their own credentials. In addition, a tenancy security administrator can reset credentials for any user within their tenancy. • **Console password:** Used to authenticate a user to the Oracle Cloud Infrastructure Console. • **API key:** All API calls are signed using a user-specific 2048-bit RSA private key. The user creates a public key pair, and uploads the public key in the Console. • **Auth token:** Auth tokens are Oracle-generated token strings that the customer can use to authenticate with third-party APIs that do no support Oracle Cloud Infrastructure's signature-based authentication. For example, use an auth token to authenticate with a OpenStack Swift client. To ensure sufficient complexity, the token is created by the IAM service and cannot be provided by a customer. • **Customer secret key:** Used by Amazon S3 clients to access the Object Storage service's S3-compatible API. To ensure sufficient complexity, the password is created by the IAM service and cannot be provided by a customer.

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
The customer needs to consider: - what physical and logical interfaces information is available from, and how access to data is controlled. - whether the service identifies and authenticates users to an appropriate level over those interfaces.	The customer is responsible for physical security of computing resources within its 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 analyzes 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 its 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 type of VCN external connectivity whether internet, on-premises network, peered VCN, or combination of these

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
	• 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. The customer's Virtual Cloud Network (VCN) can be partitioned into subnets, each mapped to an availability domain. Instances inside private subnets cannot have public IP addresses. Instances inside public subnets can optionally have public IP addresses at the customer's discretion. Security lists provide stateful and stateless firewall capability to control network access to the customer's instances. A security list is configured at the subnet level and enforced at the instance level. The customer can apply multiple security lists to a subnet. A network packet is allowed if it matches any rule in the security lists. Gateways let resources in a VCN communicate with destinations outside the VCN. The gateways include: • 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 Oracle Cloud Infrastructure services such as Object Storage • Local peering gateway (LPG): for connectivity to a peered VCN in the same region

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
	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. See Oracle Cloud Infrastructure Security Features for more information.

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
The customer needs to consider: - which service administration model is being used by the service provider to manage the service. - 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, servers supporting the services requires Oracle users to use multi-factor authentication 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 multi-tiered 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 comprised of a gateway subnet, tools subnet and network subnet located in Oracle's DMZ and is protected by firewalls. Only approved engineers with a valid OCNA account can access OCNA. Two-factor authentication is required to authenticate to OCNA. At the time of user account creation, 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 prior to access being provisioned and access is revoked when the user is terminated. OCNA is configured to complete a security posture check to determine whether the endpoint is running up-to-date anti-virus software, has a local firewall enabled and is in line with Oracle policies regarding software updates prior to permitting the endpoint to authenticate to the VPN. The second step in the authentication path is authenticating to the relevant bastion server. Operator access is only permitted from bastion servers. The bastion servers are only permitted to accept connections from OCNA subnets. Access to bastion severs is controlled in two ways.

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
	• Oracle Identity Manager (OIM) – Only approved engineers with the required OIM entitlement can access the bastion servers. The user's access must be approved by an appropriate approver prior to the entitlement being provisioned. • SSH Key – The public/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 severs 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: • Oracle Cloud Infrastructure Console: The Console is an intuitive, graphical interface that facilitates the creation and management of instances, cloud networks, and storage volumes, as well as users and permissions.

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
	• Oracle Cloud Infrastructure Application Programming Interfaces (APIs): The Oracle Cloud Infrastructure APIs are typical REST APIs that use HTTPS requests and responses. • Software Development Kits (SDKs): SDKs are available for easy integration with the Oracle Cloud Infrastructure APIs, including SDKs for Java, Ruby, and Python. • Command Line Interface (CLI): The customer can use a CLI with some services. See Oracle Cloud Infrastructure Security Features for more information.

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
The customer needs to consider: - 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. - the audit information available will meet needs for investigating misuse or incidents.	Oracle Cloud Infrastructure Audit service automatically records calls to all supported Oracle Cloud Infrastructure public Application Programming Interface (API) endpoints as log events. Currently, all services support logging by Audit. 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 Oracle Cloud Infrastructure Console, Command Line Interface (CLI), Software Development Kits (SDK), the customer's own custom clients, or other Oracle Cloud Infrastructure 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 resource(s), time stamp 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, as well as analyze events or store them separately. Data from events can be used to perform diagnostics, track resource usage, monitor compliance, and collect security-related events. See Oracle Cloud Infrastructure Security Features for more information.

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

The customer needs to consider:
 	
- any service configuration options available and the security implications of choices.
 	
- the security requirements of the customer's use of the service.
 	
- how to ensure the customer's staff using and managing the
	Documentation for Launching, Configuring, Managing and Using Oracle Cloud Infrastructure
	
	Please review the following documentation for information on launching, configuring, managing and using Oracle Cloud Infrastructure services.
	
	• Oracle Cloud Infrastructure Documentation
	  ○ Key Concepts and Terminology
	  ○ Security Guide
	  ○ Security Features
	  ○ Security Best Practices
	
	Shared Responsibilities for Security
	
	To securely run workloads in Oracle Cloud Infrastructure, the customer must be aware of its 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.

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
service in how to do so safely and securely.	For more information, please review the following documentation. • Oracle Cloud Infrastructure Security

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services