



System and Organization Controls (SOC 3) Report

Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Oracle Cloud Infrastructure System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

For the Period April 1, 2024 to September 30, 2024

Prepared in Accordance with AICPA Attestation Standards

Copyright © 2024, Oracle and/or its affiliates



Table of Contents

Section I – Report of Independent Accountants	3
Section II – Management’s Report of Its Assertions on the Effectiveness of Its Controls Over the Oracle Cloud Infrastructure System Based on the Trust Services Criteria for Security, Availability, and Confidentiality	9
Attachment A – Description of the Oracle Cloud Infrastructure System	14
Oracle Overview	14
Oracle Cloud Infrastructure Overview	14
Relevant Aspects of the Control Environment	39
Information and Communication	42
Risk Assessment	43
Monitoring	43
Attachment B – Principal Service Commitments and System Requirements	45
Overview	45

SECTION I – REPORT OF INDEPENDENT ACCOUNTANTS

To the Management of Oracle Cloud Infrastructure:

Scope:

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertion on the Effectiveness of Its Controls Over the Oracle Cloud Infrastructure System Based on the Trust Services Criteria for Security, Availability, and Confidentiality" (Assertion), that Oracle Cloud Infrastructure's controls over the Oracle Cloud Infrastructure (System) were effective throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Oracle Cloud Infrastructure's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

The System consists of the following services:

- Access Governance
- Account Tracking and Automation Tool
- Accounts Management
- Analytics Cloud
- Anomaly Detection
- API Gateway
- Application Dependency Management
- Application Performance Monitoring
- Archive Storage
- Artifact Registry
- Audit
- Autonomous Database on Dedicated Exadata Infrastructure (ADB-D)
- Autonomous Database on Exadata Cloud at Customer (ADB-C@C)
- Autonomous Database Serverless
- Base Database Service
- Bastion
- Big Data
- Bling
- Block Volume
- Blockchain Platform
- Budgets
- Certificates
- Client Logging
- Cloud Advisor
- Cloud Guard
- Cloud Incident Service
- Identity and Access Management
- Instance Security
- Integration
- Intelligent Advisor
- Inter-Region Latency
- Java Management
- Language
- License Manager
- Load Balancer
- Logging
- Logging Analytics
- Managed Access
- Management Agent
- Marketplace - Consumer
- Media Services
- Monitoring
- MySQL Heatwave
- Netsuite Analytics Warehouse
- NetSuite Health Check
- Network Firewall
- Network Load Balancer
- Network Path Analyzer
- Networking
- NoSQL Database
- Notifications
- Object Storage

- Cloud Shell
- Compute
- Compute Cloud@Customer
- Console Announcements
- Container Engine for Kubernetes
- Container Instances
- Content Management
- Customer Feedback Service
- Data Catalog
- Data Flow
- Data Integration
- Data Labeling
- Data Lake
- Data Safe
- Data Science
- Data Transfer
- Database Autonomous Recovery (formerly known as - Autonomous Recovery Service)
- Database Management
- Database Migration
- Database Tools
- DevOps - Build Pipelines
- DevOps - Code Repositories
- DevOps - Deployment Pipelines
- DevOps - Projects
- Digital Assistant
- Distributed Denial of Service Mitigation
- Document Understanding
- Domain Name System (DNS)
- Email Delivery
- Events
- Exadata Database on Cloud at Customer (ExaDB-C@C)
- Exadata Database on Dedicated Infrastructure (ExaDB-D)
- Exadata Fleet Update
- FastConnect
- File Storage
- Full Stack Disaster Recovery
- Functions
- Fusion Analytics Warehouse
- OCI Cache (formerly known as - Cache with Redis)
- OCI Control Center (formerly known as - Operator Insights)
- OCI Database with PostgreSQL
- Operator Access Control
- Ops Insights
- Oracle Cloud Migrations
- Oracle Database Service for Azure
- Oracle Database@Azure
- Oracle Ksplice
- Oracle Open Data
- Oracle Search Cloud
- OS Management
- OS Management Hub
- Process Automation
- Publisher
- Queue
- Registry
- Resource Manager
- Roving Edge Infrastructure
- Search
- Search with OpenSearch
- Secure Desktops
- Security Assurance System
- Security Zones
- Serverless Kubernetes
- Service Connector Hub
- Service Manager Proxy
- Service Mesh
- Site-to-Site VPN
- Speech
- Stack Monitoring
- Status
- Streaming
- Subscription Pricing Service
- Tagging
- Threat Intelligence
- Vault
- Vision

- Fusion Applications Environment Management
- Generative AI
- Globally Distributed Autonomous Database
- GoldenGate
- Health Checks
- Visual Builder
- Visual Builder Studio
- VMWare Solution
- physical Scanning
- Web Application Acceleration
- Web Application Firewall

supported by availability domains and points of presence in the following regions:

Commercial Regions

- Australia East (Sydney)
- Australia Southeast (Melbourne)
- Brazil East (Sao Paulo)
- Brazil Southeast (Vinhedo)
- Canada Southeast (Montreal)
- Canada Southeast (Toronto)
- Chile Central (Santiago)
- Chile West (Valparaíso)
- Colombia Central (Bogotá)
- France Central (Paris)
- France South (Marseille)
- Germany Central (Frankfurt)
- India South (Hyderabad)
- India West (Mumbai)
- Israel Central (Jerusalem)
- Italy Northwest (Milan)
- Japan Central (Osaka)
- Japan East (Tokyo)
- Mexico Central (Querétaro)
- Mexico Northeast (Monterrey)
- Netherlands Northwest (Amsterdam)
- Saudi Arabia Central (Riyadh)
- Saudi Arabia West (Jeddah)
- Serbia Central (Jovanovac)
- Singapore (Singapore)
- Singapore West (Singapore)
- South Africa Central (Johannesburg)
- South Korea Central (Seoul)
- South Korea North (Chuncheon)
- Spain Central (Madrid)
- Sweden Central (Stockholm)
- Switzerland North (Zurich)
- UAE Central (Abu Dhabi)
- UAE East (Dubai)

- United Kingdom South, London, United Kingdom
- United Kingdom West, Newport, United Kingdom
- United States East, Ashburn, Virginia, United States
- United States Midwest, Chicago, Illinois, United States
- United States West, Phoenix, Arizona, United States
- United States West, San Jose, California, United States

Government Regions

- Australia Government Southeast, Canberra, Australia
- United Kingdom Government South, London, United Kingdom
- United Kingdom Government West, Newport, United Kingdom
- United States Department of Defense East, Ashburn, Virginia, United States
- United States Department of Defense North, Chicago, Illinois, United States
- United States Department of Defense West, Phoenix, Arizona, United States
- United States Government East, Ashburn, Virginia, United States
- United States Government West, Phoenix, Arizona, United States

Sovereign Regions

- EU Sovereign Central, Frankfurt am Main, Federal Republic of Germany
- EU Sovereign South, Madrid, Spain

Multi-tenant Dedicated Regions

- Abu Dhabi, UAE
- Abu Dhabi, UAE 2

Dedicated Regions

- Chiyoda, Japan
- Doha, Qatar
- Dublin, Ireland 1
- Dublin, Ireland 2
- Gazipur, Bangladesh
- Milan, Italy 1
- Milan, Italy 2
- Muscat, Oman
- Osaka, Japan
- Ratingen, Germany 1
- Ratingen, Germany 2
- Zurich, Switzerland

Oracle Alloy

- Hobsonville, Auckland, New Zealand
- Rome, Italy
- Tokyo, Japan

Office facilities and security/network operating centers in the following locations:

- Bangalore, India

- Dublin, Ireland
- Guadalajara, Mexico
- Noida, India
- Seattle, Washington, United States

and Dedicated Transparency Centers:

- Columbia, Maryland, United States
- Denver, Colorado, United States
- Reading, United Kingdom
- North Ryde, Australia

(collectively, the “System”)

Oracle Cloud Infrastructure uses Microsoft Azure (subservice organization) to provide multi-cloud data center hosting services. The description of the boundaries of the system presented at Appendix A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at Oracle Cloud Infrastructure, to provide reasonable assurance that Oracle Cloud Infrastructure’s service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at Microsoft Azure. Our procedures did not extend to the services provided by Microsoft Azure, and we have not evaluated whether the controls management assumes have been implemented at Microsoft Azure have been implemented or whether such controls were suitably designed and operating effectively throughout the period April 1, 2024 to September 30, 2024.

Management’s responsibilities

Oracle Cloud Infrastructure’s management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Oracle Cloud Infrastructure’s service commitments and system requirements were achieved. Oracle Cloud Infrastructure management is also responsible for providing the accompanying assertion about the effectiveness of controls within the System, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and service requirements that are the objectives of the System.

Our responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion, which includes: (1) obtaining an understanding of Oracle Cloud Infrastructure’s relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Oracle Cloud Infrastructure's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of Oracle Cloud Infrastructure and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 - Members in Public Practice of the Code of Professional Conduct established by the AICPA.

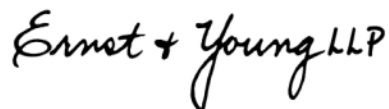
Inherent limitations:

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Oracle Cloud Infrastructure's service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Our examination was not conducted for the purpose of evaluating the performance or integrity of Oracle Cloud Infrastructure's AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Oracle Cloud Infrastructure's AI services.

Opinion:

In our opinion, Oracle Cloud Infrastructure's controls over the System were effective throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.



November 15, 2024

SECTION II – MANAGEMENT’S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER THE ORACLE CLOUD INFRASTRUCTURE SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY, AND CONFIDENTIALITY

We, as management of, Oracle Cloud Infrastructure are responsible for:

- Identifying the Oracle Cloud Infrastructure System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our service commitments and system requirements
- Identifying the risks that would threaten the achievement of our service commitments and service requirements that are the objectives of our System, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirements
- Selecting the trust services categories and associated criteria that are the basis of our assertion

The System consists of the following services:

- | | |
|---|----------------------------------|
| • Access Governance | • Health Checks |
| • Account Tracking and Automation Tool | • Identity and Access Management |
| • Accounts Management | • Instance Security |
| • Analytics Cloud | • Integration |
| • Anomaly Detection | • Intelligent Advisor |
| • API Gateway | • Inter-Region Latency |
| • Application Dependency Management | • Java Management |
| • Application Performance Monitoring | • Language |
| • Archive Storage | • License Manager |
| • Artifact Registry | • Load Balancer |
| • Audit | • Logging |
| • Autonomous Database on Dedicated Exadata Infrastructure (ADB-D) | • Logging Analytics |
| • Autonomous Database on Exadata Cloud at Customer (ADB-C@C) | • Managed Access |
| • Autonomous Database Serverless | • Management Agent |
| • Base Database Service | • Marketplace - Consumer |
| • Bastion | • Media Services |
| • Big Data | • Monitoring |
| • Bling | • MySQL Heatwave |
| • Block Volume | • Netsuite Analytics Warehouse |
| • Blockchain Platform | • NetSuite Health Check |
| • Budgets | • Network Firewall |
| • Certificates | • Network Load Balancer |
| • Client Logging | • Network Path Analyzer |
| • Cloud Advisor | • Networking |
| | • NoSQL Database |
| | • Notifications |

- Cloud Guard
- Cloud Incident Service
- Cloud Shell
- Compute
- Compute Cloud@Customer
- Console Announcements
- Container Engine for Kubernetes
- Container Instances
- Content Management
- Customer Feedback Service
- Data Catalog
- Data Flow
- Data Integration
- Data Labeling
- Data Lake
- Data Safe
- Data Science
- Data Transfer
- Database Autonomous Recovery (formerly known as – Autonomous Recovery Service)
- Database Management
- Database Migration
- Database Tools
- DevOps - Build Pipelines
- DevOps - Code Repositories
- DevOps - Deployment Pipelines
- DevOps - Projects
- Digital Assistant
- Distributed Denial of Service Mitigation
- Document Understanding
- Domain Name System (DNS)
- Email Delivery
- Events
- Exadata Database on Cloud at Customer (ExaDB-C@C)
- Exadata Database on Dedicated Infrastructure (ExaDB-D)
- Exadata Fleet Update
- FastConnect
- File Storage
- Full Stack Disaster Recovery
- Functions
- Object Storage
- OCI Cache (formerly known as - Cache with Redis)
- OCI Control Center (formerly known as - Operator Insights)
- OCI Database with PostgreSQL
- Operator Access Control
- Ops Insights
- Oracle Cloud Migrations
- Oracle Database Service for Azure
- Oracle Database@Azure
- Oracle Ksplice
- Oracle Open Data
- Oracle Search Cloud
- OS Management
- OS Management Hub
- Process Automation
- Publisher
- Queue
- Registry
- Resource Manager
- Roving Edge Infrastructure
- Search
- Search with OpenSearch
- Secure Desktops
- Security Assurance System
- Security Zones
- Serverless Kubernetes
- Service Connector Hub
- Service Manager Proxy
- Service Mesh
- Site-to-Site VPN
- Speech
- Stack Monitoring
- Status
- Streaming
- Subscription Pricing Service
- Tagging
- Threat Intelligence
- Vault
- Vision
- Visual Builder

- Fusion Analytics Warehouse
- Fusion Applications Environment Management
- Generative AI
- Globally Distributed Autonomous Database
- GoldenGate
- Visual Builder Studio
- VMWare Solution
- Vulnerability Scanning
- Web Application Acceleration
- Web Application Firewall

supported by availability domains and points of presence in the following regions:

Commercial Regions

- Australia East (Sydney)
- Australia Southeast (Melbourne)
- Brazil East (Sao Paulo)
- Brazil Southeast (Vinhedo)
- Canada Southeast (Montreal)
- Canada Southeast (Toronto)
- Chile Central (Santiago)
- Chile West (Valparaiso)
- Colombia Central (Bogota)
- France Central (Paris)
- France South (Marseille)
- Germany Central (Frankfurt)
- India South (Hyderabad)
- India West (Mumbai)
- Israel Central (Jerusalem)
- Italy Northwest (Milan)
- Japan Central (Osaka)
- Japan East (Tokyo)
- Mexico Central (Queretaro)
- Mexico Northeast (Monterrey)
- Netherlands Northwest (Amsterdam)
- Saudi Arabia Central (Riyadh)
- Saudi Arabia West (Jeddah)
- Serbia Central (Jovanovac)
- Singapore (Singapore)
- Singapore West (Singapore)
- South Africa Central (Johannesburg)
- South Korea Central (Seoul)
- South Korea North (Chuncheon)
- Spain Central (Madrid)
- Sweden Central (Stockholm)
- Switzerland North (Zurich)
- UAE Central (Abu Dhabi)
- UAE East (Dubai)
- United Kingdom South, London, United Kingdom
- United Kingdom West, Newport, United Kingdom

- United States East, Ashburn, Virginia, United States
- United States Midwest, Chicago, Illinois, United States
- United States West, Phoenix, Arizona, United States
- United States West, San Jose, California, United States

Government Regions

- Australia Government Southeast, Canberra, Australia
- United Kingdom Government South, London, United Kingdom
- United Kingdom Government West, Newport, United Kingdom
- United States Department of Defense East, Ashburn, Virginia, United States
- United States Department of Defense North, Chicago, Illinois, United States
- United States Department of Defense West, Phoenix, Arizona, United States
- United States Government East, Ashburn, Virginia, United States
- United States Government West, Phoenix, Arizona, United States

Sovereign Regions

- EU Sovereign Central, Frankfurt am Main, Federal Republic of Germany
- EU Sovereign South, Madrid, Spain

Multi-tenant Dedicated Regions

- Abu Dhabi, UAE
- Abu Dhabi, UAE 2

Dedicated Regions

- Chiyoda, Japan
- Doha, Qatar
- Dublin, Ireland 1
- Dublin, Ireland 2
- Gazipur, Bangladesh
- Milan, Italy 1
- Milan, Italy 2
- Muscat, Oman
- Osaka, Japan
- Ratingen, Germany 1
- Ratingen, Germany 2
- Zurich, Switzerland

Oracle Alloy

- Hobsonville, Auckland, New Zealand
- Rome, Italy
- Tokyo, Japan

Office facilities and security/network operating centers in the following locations:

- Bangalore, India
- Dublin, Ireland
- Guadalajara, Mexico
- Noida, India

- Seattle, Washington, United States

and Dedicated Transparency Centers:

- Columbia, Maryland, United States
- Denver, Colorado, United States
- Reading, United Kingdom
- North Ryde, Australia

(collectively, the “System”).

Carved-out Unaffiliated Subservice Organization: Oracle Cloud Infrastructure System uses Microsoft Azure to provide multi-cloud data center hosting services. The Description indicates that complementary controls at Microsoft Azure that are suitably designed and operating effectively are necessary, along with controls at Oracle Cloud Infrastructure, to achieve Oracle Cloud Infrastructure’s service commitments and system requirements, based on the applicable trust services criteria. The Description presents Oracle Cloud Infrastructure’s controls and the types of complementary subservice organization controls assumed in the design of Oracle Cloud Infrastructure’s controls. The Description does not disclose the actual controls at Microsoft Azure.

We confirm, to the best of our knowledge and belief, that:

- a. The Description presents the System that was designed and implemented throughout the period April 1, 2024 to September 30, 2024 in accordance with the Description Criteria.
- b. The controls stated in the Description were suitably designed throughout the period April 1, 2024 to September 30, 2024 to provide reasonable assurance that Oracle Cloud Infrastructure service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout April 1, 2024 to September 30, 2024, and the carved-out subservice organization applied the complementary controls assumed in the design of Oracle Cloud Infrastructure’s controls throughout the period April 1, 2024 to September 30, 2024.
- c. The Oracle Cloud Infrastructure controls stated in the Description operated effectively throughout the period April 1, 2024 to September 30, 2024 to provide reasonable assurance that Oracle Cloud Infrastructure’s service commitments and system requirements were achieved based on the applicable trust services criteria, and the complementary carved-out subservice organization controls assumed in the design of Oracle Cloud Infrastructure’s controls operated effectively throughout that period.

Very truly yours,

ORACLE

ATTACHMENT A – DESCRIPTION OF THE ORACLE CLOUD INFRASTRUCTURE SYSTEM

Oracle Overview

Oracle provides products and services that address enterprise information technology (IT) environments. Our products and services include enterprise applications and infrastructure offerings that are delivered worldwide through a variety of flexible and interoperable IT deployment models. These models include on-premise, cloud-based and hybrid deployments (an approach that combines both on-premise and cloud-based deployments), such as Oracle Exadata Cloud at Customer and Dedicated Region offerings (instances of Oracle Cloud in a customer's own data center) and multi-cloud options that enable customers to use Oracle Cloud in conjunction with other public clouds. Accordingly, we offer choice and flexibility to our customers and facilitate the product, service and deployment combinations that best suit our customers' needs. Our customers include businesses of many sizes, government agencies, educational institutions, and resellers that we market and sell to directly through our worldwide sales force and indirectly through the Oracle Partner Network. Using Oracle technologies, our customers build, deploy, run, manage and support their internal and external products, services and business operations.

Oracle Cloud Services offerings, which include Oracle Software-as-a-Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), provide comprehensive and integrated applications and infrastructure services delivered via various cloud delivery models enabling our customers to choose the best option that meets their specific business needs. Oracle Cloud Services integrate the IT components, including software, hardware and services, on a customer's behalf in a cloud-based IT environment that Oracle deploys, manages, supports and upgrades for the customer and that a customer may access utilizing common web browsers via a broad spectrum of devices.

Oracle Cloud Services are designed to be rapidly deployable to enable customers shorter time to innovation; intuitive for casual and experienced users; easily maintainable to reduce upgrade, integration and testing work; connectable among differing deployment models to enable interoperability and extensibility to easily move workloads among the Oracle Cloud and other IT and cloud environments; cost-effective by lowering upfront customer investments and implementing usage-based resource consumption costs; and highly secure, standards-based and reliable.

Oracle cloud license and on-premise license deployment offerings include Oracle Applications, Oracle Database and Oracle Middleware software offerings, among others, which customers deploy using IT infrastructure from the Oracle Cloud or their own cloud-based or on-premise IT environments. Substantially all customers opt to purchase license support contracts when they purchase an Oracle license.

Oracle hardware products include Oracle Engineered Systems, servers, storage and industry-specific products, among others. Customers generally opt to purchase hardware support contracts when they purchase Oracle hardware products. Oracle also offers professional services to assist our customers and partners to maximize the performance of their investments in Oracle products and services. Providing choice and flexibility to Oracle customers as to when and how they deploy Oracle applications and infrastructure technologies is an important element of our corporate strategy. Oracle believes that offering customers broad, comprehensive, flexible and interoperable deployment models for Oracle applications and infrastructure technologies is important to its growth strategy.

Oracle Cloud Infrastructure Overview

Oracle Cloud Infrastructure is a set of complementary cloud services that enable customers to build and run a range of applications and services in a highly available hosted environment. Oracle Cloud Infrastructure provides high-performance capabilities (as physical hardware instances) and storage capacity in a flexible overlay virtual network that is securely accessible from customer's on-premise networks.

Oracle Cloud Infrastructure's [distributed cloud](#) provides customers with the flexibility to choose where and how cloud services are delivered to meet their regulatory, performance, and other needs. The distributed cloud offerings deliver the full functionality and superior economics of Oracle's public cloud to customer data centers and edge locations, with a range of deployment models and operational controls. By design, Oracle Cloud Infrastructure's distributed cloud offerings are all built on the same foundation.

The concepts and terminology described below are critical to understanding Oracle's controls over the Oracle Cloud Infrastructure System.

Physical Architecture Concepts

Regions and Availability Domains

Oracle Cloud Infrastructure is physically hosted in regions and availability domains (ADs). A region is a localized geographic area, and an AD is one or more data centers located within a region. A region is comprised of one or more ADs. Most Oracle Cloud Infrastructure resources are either region-specific, such as a virtual cloud network (VCN), or AD specific, such as a compute instance. Traffic between ADs and between regions is encrypted. ADs are isolated from each other, fault tolerant, and very unlikely to fail simultaneously. Because ADs do not share infrastructure such as power or cooling, or the internal AD network, a failure at one AD within a region is unlikely to impact the availability of the others within the same region.

The ADs within the same region are connected to each other by a low-latency, high-bandwidth network, which makes it possible for customers to provide high-availability connectivity to the internet and on-premises, and to build replicated systems in multiple ADs for both high-availability and disaster recovery.

Regions are independent of each other and can be separated by vast geographical distances. Generally, customers would deploy an application in the region where it is most heavily used, because using nearby resources is faster than using distant resources. However, customers can also deploy applications in different regions for these reasons:

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

The Exadata Database Service on Cloud@Customer service is hosted physically in regions and ADs. The accompanying Exadata Database Machine is hosted at the customer's designated data center.

Fault Domains

A fault domain is a grouping of hardware and infrastructure within an AD. Each AD contains three fault domains. Fault domains provide anti-affinity: they let customers distribute their instances so that the instances are not on the same physical hardware within a single AD. A hardware failure or Compute hardware maintenance event that affects one fault domain does not affect instances in other fault domains.

To control the placement of compute instances, bare metal DB system instances, or virtual machine DB system instances, customers can optionally specify the fault domain for a new instance or instance pool at launch time. If the customer doesn't specify the fault domain, the system selects one automatically. Oracle Cloud Infrastructure makes a best-effort anti-affinity placement across different fault domains, while optimizing for available capacity in the AD.

Realms

A realm is a logical collection of regions. Realms are isolated from each other and do not share any data. A customer tenancy exists in a single realm and has access to the regions that belong to that realm. Oracle Cloud Infrastructure offers realms for the following:

- Commercial - A secure, high performance cloud platform for all workloads
- US Government - Cloud regions for the US government.
- UK Government - A sovereign, dedicated dual-region cloud for UK government and defense customers.
- Australian Government - Cloud region for the Australian government.
- EU Sovereign - Cloud regions in the European Union to help customers control their data and applications in alignment with data residency and sovereignty requirements. Regions are physically and logically separated from other public cloud regions.
- Dedicated Region - Region for a single customer. There is also a multi-tenancy functionality within a dedicated region, allowing a single customer to have multiple completely isolated tenancies within their region.
- Oracle Alloy - A complete cloud infrastructure platform that enables partners to become cloud providers and offer a full range of cloud services to expand their businesses.

The following table lists the regions in the commercial realms included in the scope of the System:

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY	AVAILABILITY DOMAINS
Australia East (Sydney)	ap-sydney-1	Sydney, Australia	SYD	OC1	1
Australia Southeast (Melbourne)	ap-melbourne-1	Melbourne, Australia	MEL	OC1	1
Brazil East (Sao Paulo)	sa-saopaulo-1	Sao Paulo, Brazil	GRU	OC1	1
Brazil Southeast (Vinhedo)	sa-vinhedo-1	Vinhedo, Brazil	VCP	OC1	1
Canada Southeast (Montreal)	ca-montreal-1	Montreal, Canada	YUL	OC1	1
Canada Southeast (Toronto)	ca-toronto-1	Toronto, Canada	YYZ	OC1	1
Chile Central (Santiago)	sa-santiago-1	Santiago, Chile	SCL	OC1	1
Chile West (Valparaiso)	sa-valparaiso-1	Valparaiso, Chile	VAP	OC1	1
Colombia Central (Bogota)	sa-bogota-1	Bogota, Colombia	BOG	OC1	1
France Central (Paris)	eu-paris-1	Paris, France	CDG	OC1	1
France South (Marseille)	eu-marseille-1	Marseille, France	MRS	OC1	1
Germany Central (Frankfurt)	eu-frankfurt-1	Frankfurt, Germany	FRA	OC1	3
India South (Hyderabad)	ap-hyderabad-1	Hyderabad, India	HYD	OC1	1
India West (Mumbai)	ap-mumbai-1	Mumbai, India	BOM	OC1	1
Israel Central (Jerusalem)	il-jerusalem-1	Jerusalem, Israel	MTZ	OC1	1
Italy Northwest (Milan)	eu-milan-1	Milan, Italy	LIN	OC1	1
Japan Central (Osaka)	ap-osaka-1	Osaka, Japan	KIX	OC1	1
Japan East (Tokyo)	ap-tokyo-1	Tokyo, Japan	NRT	OC1	1
Mexico Central (Queretaro)	mx-queretaro-1	Queretaro, Mexico	QRO	OC1	1
Mexico Northeast (Monterrey)	mx-monterrey-1	Monterrey, Mexico	MTY	OC1	1
Netherlands Northwest (Amsterdam)	eu-amsterdam-1	Amsterdam, Netherlands	AMS	OC1	1
Saudi Arabia Central (Riyadh)	me-riyadh-1	Riyadh, Saudi Arabia	RUH	OC1	1 – from July 31 st , 2024
Saudi Arabia West (Jeddah)	me-jeddah-1	Jeddah, Saudi Arabia	JED	OC1	1
Serbia Central (Jovanovac)	eu-jovanovac-1	Jovanovac, Serbia	BEG	OC20	1

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY	AVAILABILITY DOMAINS
Singapore (Singapore)	ap-singapore-1	Singapore, Singapore	SIN	OC1	1
Singapore West (Singapore)	ap-singapore-2	Singapore, Singapore	XSP	OC1	1 – from June 28 th , 2024
South Africa Central (Johannesburg)	af-johannesburg-1	Johannesburg, South Africa	JNB	OC1	1
South Korea Central (Seoul)	ap-seoul-1	Seoul, South Korea	ICN	OC1	1
South Korea North (Chuncheon)	ap-chuncheon-1	Chuncheon, South Korea	YNY	OC1	1
Spain Central (Madrid)	eu-madrid-1	Madrid, Spain	MAD	OC1	1
Sweden Central (Stockholm)	eu-stockholm-1	Stockholm, Sweden	ARN	OC1	1
Switzerland North (Zurich)	eu-zurich-1	Zurich, Switzerland	ZRH	OC1	1
UAE Central (Abu Dhabi)	me-abudhabi-1	Abu Dhabi, UAE	AUH	OC1	1
UAE East (Dubai)	me-dubai-1	Dubai, UAE	DXB	OC1	1
UK South (London)	uk-london-1	London, UK	LHR	OC1	3
UK West (Newport)	uk-cardiff-1	Newport, UK	CWL	OC1	1
US East (Ashburn)	us-ashburn-1	Ashburn, Virginia, US	IAD	OC1	3
US Midwest (Chicago)	us-chicago-1	Chicago, IL	ORD	OC1	3
US West (Phoenix)	us-phoenix-1	Phoenix, Arizona, US	PHX	OC1	3
US West (San Jose)	us-sanjose-1	San Jose, California, US	SJC	OC1	1

The following table lists the regions in the United States Government Cloud realm (with FedRAMP authorization) included in the scope of the System:

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY	AVAILABILITY DOMAINS
US Gov East (Ashburn)	us-langley-1	Ashburn, Virginia, US	LFI	OC2	1
Us Gov West (Phoenix)	us-luke-1	Phoenix, Arizona, US	LUF	OC2	1

The following table lists the regions in the United States Federal Cloud realm (with DISA Impact Level 5 authorization) included in the scope of the System:

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY	AVAILABILITY DOMAINS
US DoD East (Ashburn)	us-gov-ahsburn-1	Ashburn, Virginia, US	RIC	OC3	1
US DoD North (Chicago)	us-gov-chicago-1	Chicago, Illinois, US	PIA	OC3	1

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY	AVAILABILITY DOMAINS
US DoD West (Phoenix)	us-gov-phoenix-1	Phoenix, Arizona, US	TUS	OC3	1

The following table lists the regions in the United Kingdom Government Cloud realm included in the scope of the System:

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY	AVAILABILITY DOMAINS
UK Gov South (London)	uk-gov-london-1	London, UK	LTN	OC4	1
UK Gov West (Newport)	uk-gov-cardiff-1	Newport, UK	BRS	OC4	1

The following table lists the region in the Australian Government Cloud realm included in the scope of the System:

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY	AVAILABILITY DOMAINS
Australia Government Southeast (Canberra)	ap-canberra-1	Canberra, Australia	WGA	OC10	1

The following table lists the regions in the EU Sovereign Cloud realm included in the scope of the System:

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY	AVAILABILITY DOMAINS
EU Sovereign Central (Frankfurt)	eu-frankfurt-2	Frankfurt, Germany	STR	OC19	1
EU Sovereign South (Madrid)	eu-madrid-2	Madrid, Spain	VLL	OC19	1

The following table lists the Dedicated Regions included in the scope of the System:

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY
NJA Dedicated Region	ap-chiyoda-1	Chiyoda, Japan	NJA	OC8
UKB Dedicated Region	ap-ibaraki-1	Osaka, Japan	UKB	OC8
MCT Dedicated Region	me-dcc-muscat-1	Muscat, Oman	MCT	OC9
BGY Dedicated Region	eu-dcc-milan-1	Milan, Italy	BGY	OC14
DTM Dedicated Region	eu-dcc-rating-2	Ratingen, Germany	DTM	OC14
DUS Dedicated Region	eu-dcc-rating-1	Ratingen, Germany	DUS	OC14
MXP Dedicated Region	eu-dcc-milan-2	Milan, Italy	MXP	OC14
ORK Dedicated Region	eu-dcc-dublin-1	Dublin, Ireland	ORK	OC14
SNN Dedicated Region	eu-dcc-dublin-2	Dublin, Ireland	SNN	OC14
DAC Dedicated Region	ap-dcc-gazipur-1	Gazipur, Bangladesh	DAC	OC15 – from April 8 th , 2024

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY
DOH Dedicated Region	me-dcc-doha-1	Doha, Qatar	DOH	OC21
AVZ Dedicated Region	eu-dcc-zurich-1	Zurich, Switzerland	AVZ	OC24
AHU Multi-Tenant Dedicated Region	me-abudhabi-3	Abu Dhabi, UAE	AHU	OC26 – from April 15 th , 2024
RKT Multi-Tenant Dedicated Region	me-abudhabi-2	Abu Dhabi, UAE 2	RKT	OC29 – from July 12 th , 2024

The following table lists the Oracle Alloys included in the scope of the System:

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY
NAP Alloy Region	eu-dcc-rome-1	Rome, Italy	NAP	OC22
TYO Alloy Region	ap-dcc-tokyo-1	Tokyo, Japan	TYO	OC25
IZQ Alloy Region	ap-hobsonville-1	Hobsonville, Auckland	IZQ	OC31 – from July 17 th , 2024

Account and Access Concepts

Console

The Console is an intuitive, graphical interface to create and manage instances, cloud networks, and storage volumes, as well as users and permissions. Oracle Alloy partners and Multi-tenant Dedicated Regions operators have their own operator consoles, enabling them to manage both their cloud region's services and business operations. The Alloy operating team can customize branding, including logos, color themes, and terms of use. They can configure their customers' front-end experience, including notifications and announcements.

Tenancy

When a customer signs up or subscribes to Oracle Cloud services, Oracle creates a tenancy for the customer. The customer can think of the tenancy as their account, but it is also a secure and isolated partition with Oracle Cloud Infrastructure where they can create, organize, and administer their cloud resources. When a customer signs up, the customer's tenancy is created in a home region designated by the customer, but the customer can subscribe their tenancy to as many regions as needed. Large organizations can have multiple tenancies.

Compartment

Compartments allow the customer to organize and control access to their cloud resources. A compartment is a collection of related resources (such as instances, VCNs, and block volumes) that can be accessed only by groups that have been given permission by an administrator. A compartment should be thought of as a logical group and not a physical container. When working with resources in the Console, the compartment acts as a filter for what each customer can view.

When a customer signs up for Oracle Cloud Infrastructure, Oracle creates the customer's tenancy, which is the root compartment that holds all cloud resources for the customer. The customer then creates additional compartments within the tenancy (root compartment) and corresponding policies to control access to the resources in each compartment. When a customer creates a cloud resource such as an instance, block volume, or cloud network, the customer must specify to which compartment they want the resource to belong. Each person has access to only the resources they need.

Identity Domains and Policies

An identity domain is a container for managing users and roles, federating and provisioning of users, secure application integration through Oracle Single Sign-On (SSO) configuration, and OAuth administration. It represents a user population in Oracle Cloud Infrastructure and its associated configurations and security settings (such as MFA).

A policy is a document that specifies who can access which resources and how. Customers can write policies to control access to their [services](#) within Oracle Cloud Infrastructure. Access is granted at the group and compartment level, which means customers can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If a customer gives a group access to the tenancy, the group automatically gets the same type of access to all the compartments inside the tenancy.

Oracle Cloud Identifier (OCID)

Every Oracle Cloud Infrastructure resource has an Oracle-assigned unique ID called an Oracle Cloud Identifier (OCID). This ID is included as part of the resource's information in both the Console and API.

Security Zone

Security Zones allow customers to be confident that their Compute, Networking, Object Storage, Database, and other resources comply with Oracle security principles and best practices. A security zone is associated with one or more compartments and a security zone recipe. When a customer creates and updates resources in a security zone, Oracle Cloud Infrastructure validates these operations against security zone policies in the zone's recipe. If any security zone policy is violated, then the operation is denied.

Core Service Concepts

Virtual Cloud Network

A VCN is a virtual version of a traditional network—including subnets, route tables, and gateways—on which the customer's instances run. A cloud network resides within a single region but includes all the region's ADs. Each subnet that is defined by the customer in the cloud network can either be in a single AD or span all the ADs in that region. At least one cloud network needs to be set up before instances can be launched. Customers may configure their cloud network with an optional internet gateway to handle public traffic, and an optional IPSec connection or FastConnect to securely extend their on-premises network.

Instance

An instance is a compute host running in the cloud. An Oracle Cloud Infrastructure compute instance allows customers to utilize hosted physical hardware, as opposed to the traditional software-based virtual machines, ensuring a high level of security and performance.

The image is a template on a virtual hard drive that defines the operating system and other software for an instance, for example, Oracle Linux. When a customer launches an instance, they can define its characteristics by choosing its image. Oracle provides a set of platform images that customers can use. Customers can also save an image from an instance that they have already configured to use as a template to launch more instances with the same software and customizations.

In Compute, the shape specifies the number of CPUs and amount of memory allocated to the instance. Oracle Cloud Infrastructure offers shapes to fit various computing requirements.

Block Volume

A block volume is a virtual disk that provides persistent block storage space for Oracle Cloud Infrastructure instances. A block volume is used in the same way as a physical hard drive on a computer, for example, to store data and applications. Block volumes can be detached from one instance and attached to another instance without loss of data.

Service Essentials

Security Credentials

When working with Oracle Cloud Infrastructure, customers may use the following credentials: console password when accessing their console; API signing key when using API; instance SSH key for accessing a compute instance; and Auth Token for authenticating with third-party APIs that do not support Oracle Cloud Infrastructure's signature-based authentication.

IP Address Ranges

There are public IP address ranges for services that are deployed in Oracle Cloud Infrastructure. Customers need to allow traffic to these Classless Inter-Domain Routing (CIDR) blocks to access the services.

Resource Monitoring

Customers can monitor the health, capacity, and performance of their Oracle Cloud Infrastructure resources as required using queries or on a passive basis using alarms. Queries and alarms rely on metrics emitted by their resource to the Monitoring service.

Resource Tags

Tags allow customers to define keys and values and associate them with resources. Customers can then use the tags to help organize and list resources based on business needs. There are two types of tags:

- Defined tags are set up in a customer's tenancy by an administrator. Only users granted permission to work with the defined tags can apply them to resources.
- Free-form tags can be applied by any user with permissions on the resource.

Service Limits

A set of service limits are configured for each tenancy, as established when a customer purchases Oracle Cloud Infrastructure. The service limit is the quota or allowance set on a resource. These limits may be increased automatically based on the resource usage and account standing, but customers can also request a service limit increase.

Service Logs

Customers can enable service logs for some resources. Service logs provide diagnostic information about the resources in a tenancy. When customers enable logging on resources, they receive information about the resource in a log file. This information allows customers to analyze, optimize, and troubleshoot their resources.

Tenancy Explorer

Tenancy explorer allows customers to obtain a cross-region view of all resources in a compartment.

Work Requests

Work requests allow customers to monitor long-running operations such as database backups or provisioning of compute instances. When such an operation is launched, the service spawns a work request. A work request is an activity log that enables customers to track each step in the operation's process. Each work request has an OCID that allows the customer to interact with it programmatically and use it for automation.

Service Descriptions

The scope of this report includes the controls placed in operation specifically for the following Oracle Cloud Infrastructure services to meet the Trust Services Criteria related to security, availability, and confidentiality and excludes the controls performed by the subservice organization. These criteria are set forth in TSP section 100, of the 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Services available to customers may include, but are not limited to, the offerings described below. The actual services provided by Oracle depends on the contractual agreement with and the services provisioned by each individual customer, as well as the availability of the service within a region or realm. Customers can refer to the publicly available Infrastructure Regions list to find out where a service is available.

Access Governance

Access Governance is an Identity Governance and Administration (IGA) solution that provides insights-based access reviews, identity analytics, and intelligence capabilities for businesses.

Account Tracking and Automation Tool

The Account Tracking and Automation Tool (ATAT) maintains metadata about resources it creates for ATAT Portfolio resources. It provides a cost tracking and reporting.



Accounts Management

Accounts Management provides various billing and cost management tools that make it easy for customers to manage service costs. Customers can estimate costs, create budgets to set spending thresholds, view usage, and visualize spending with charts and reports. Customers can also view subscription details, invoices, payment history, manage payment method, and earn rewards.

Analytics Cloud

Analytics Cloud empowers business analysts and consumers with modern, AI-powered, self-service analytics capabilities for data preparation, visualization, enterprise reporting, augmented analysis, and natural language processing.

Anomaly Detection

Anomaly Detection provides customers with a rich set of tools to identify undesirable events or observations in business data in real time so that customers can take action to avoid business disruptions.

API Gateway

API Gateway allows customers to create governed HTTP/S interfaces for other services, including Functions, Container Engine for Kubernetes, and Container Registry. API Gateway also provides policy enforcement such as authentication and rate-limiting to HTTP/S endpoints.

Application Dependency Management

Application Dependency Management (ADM) detects security vulnerabilities in application dependencies. It is a reporting and management service integrated with Oracle Cloud Infrastructure services to detect and remediate security vulnerabilities in the applications' dependencies. It relies on vulnerabilities reported by community sources including the National Vulnerability Database (NVD).

Application Performance Monitoring

Application Performance Monitoring provides a comprehensive set of features to monitor applications and diagnose performance issues.

Archive Storage

Archive Storage allows customers to store data that is accessed infrequently and requires long retention periods. It is ideal for storing data that is seldom accessed but requires long retention periods. Archive Storage data retrieval is not instantaneous. By default, Archive Storage encrypts data on the server with Advanced Encryption Standard (AES) 256-bit encryption. The customer has the option to encrypt Archive Storage with keys that the customer owns and manages via the Vault service.

Artifact Registry

Artifact Registry is a repository service for storing, sharing, and managing software development packages. An artifact is a software package, library, zip file, or any other type of file used for deploying applications. Examples are Python or Maven libraries. Artifacts are grouped into repositories, which are collections of related artifacts.

Audit

The Audit service provides visibility into activities related to a customer's Oracle Cloud Infrastructure resources and tenancy. Audit log events can be used for security audits, to track usage of and changes to Oracle Cloud Infrastructure resources. Audit 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. 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), custom clients, or other Oracle Cloud Infrastructure services. Information in the logs includes the following: time the API activity occurred, source of the activity, target of the activity, type of action, and type of response.

Bastion

Bastion provides restricted and time-limited access to target resources that don't have public endpoints. Bastions let authorized users connect from specific IP addresses to target resources using Secure Shell (SSH) sessions. When connected, users can interact with the target resource by using any software or protocol supported by SSH.

Big Data

Big Data Service provisions fully configured, secure, highly available, and dedicated Hadoop and Spark clusters on demand. Customers can scale the cluster to fix their big data and analytics workloads by using a range of Oracle Cloud Infrastructure compute shapes that support small test and development clusters to large production clusters.

Bling

Bling is an Oracle internal service that provides the cost and usage reports for customers. Cost reports indicate the cost of resource consumption, and usage reports indicate the quantity of what is consumed.

Block Volume

Block Volume allows customers to dynamically provision and manage block storage volumes. The customer can create, attach, connect, and move volumes as needed to meet storage, performance, and application requirements. By default, Block Volume service encrypts block volumes, boot volumes, and volume backups at rest using AES 256-bit encryption. The customer has the option to encrypt volumes at rest with keys that the customer owns and manages via the Vault service.

Blockchain Platform

Blockchain Platform is a network consisting of validating nodes (peers) that update the ledger and respond to queries by executing smart contract code – the business logic that runs on the blockchain. External applications invoke transactions or run queries through client SDKs or REST API calls, which prompts selected peers to run the smart contracts. Multiple peers endorse (digitally sign) the results, which are then verified and sent to the ordering service. After consensus is reached on the transaction order, transaction results are grouped into cryptographically secured, tamper-proof data blocks and sent to peer nodes to be validated and appended to the ledger.

Budgets

A budget is a feature that customers can use to set soft limits on their Oracle Cloud Infrastructure spending. Customers can set alerts on their budget to be informed when they may exceed their budget and can view all their budgets and spending from one single place in the Oracle Cloud Infrastructure console.

Certificates

Certificates lets customers create and manage TLS certificates, certificate authorities (CAs), and CA bundles. It provides customers with certificate issuance, storage, and management capabilities, including revocation and automatic renewal.

Client Logging

Client Logging is a multi-tenant service that accepts trace logs from the client part of the product, validates requests, augments with additional data, and routes to persistent store in the Oracle Cloud Infrastructure platform. Client Logging is an internal Oracle service.

Cloud Advisor

Cloud Advisor allows customers to find potential inefficiencies in their tenancy and offers guided solutions that explain how to address them. The recommendations help optimize the performance, security, and availability of the customer's tenancy. It complements and cross-sells Cloud Guard and Data Safe, displays summary Cloud Guard data, and redirects customers directly to Cloud Guard for all security issues.

Cloud Guard

Cloud Guard allows customers to monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud. Customers can examine their Oracle Cloud Infrastructure resources for security weakness related to configuration, and their operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist, or take corrective actions, based on their configurations.

Cloud Incident Service

Cloud Incident Service provides the Support Center feature access in the Oracle Cloud Infrastructure console. It enables customers to browse and create tickets for technical and billing requests, including service limit increases.

Cloud Shell

Cloud Shell is a web browser-based terminal accessible from the Oracle Cloud Console. It provides access to a Linux shell, with a pre-authenticated Oracle Cloud Infrastructure Command Line Interface (CLI), a pre-authenticated Ansible installation, and other useful tools to follow Oracle Cloud Infrastructure service tutorials and labs.

Compute

Compute allows customers to provision and manage compute hosts, known as instances. Oracle Cloud Infrastructure offers both bare metal and virtual machine compute instances.

Bare metal compute instances give customers dedicated physical server access for the highest performance and strong isolation.

Virtual machine (VM) instances are independent computing environments that run on top of physical bare metal hardware. Virtualization makes it possible to run multiple VMs that are isolated from each other. VMs are useful for running applications that do not require the performance and resources (CPU, memory, network bandwidth, storage) of an entire physical machine.

When the customer creates a Compute instance, they can select the most appropriate type of instance for their applications based on characteristics such as the number of CPUs, amount of memory, and network resources. Oracle Cloud Infrastructure offers a variety of instances features, shape types, and capacity types that are designed to meet a range of compute and application requirements.

Compute Cloud@Customer

Compute Cloud@Customer is Oracle-owned and remotely managed cloud infrastructure that is installed on-premises. The Compute Cloud@Customer rack is installed in the customer's data center, connected to their Oracle Cloud Infrastructure tenancy. It allows customers to run scalable Oracle Cloud Infrastructure compute, storage, and networking services while enabling data residency requirements and the need for low-latency connections to existing data center assets and real-time operations.

Console Announcements

Announcements are displayed in the Console to communicate timely, important information about service status. Customers can also view a list of past and ongoing announcements. Announcement types currently include the following: required action, emergency change, emergency maintenance extended, emergency maintenance reschedule, recommended action, planned change, planned change extended, planned change rescheduled, event notification, schedule maintenance, emergency maintenance completed, planned change completed, and information.

Container Engine for Kubernetes

Container Engine for Kubernetes allows customers to enable the deployment, scaling, and management of containerized applications. The service uses Kubernetes, the open-source system for automating deployment, scaling, and management of containerized applications across clusters of hosts. Kubernetes groups the containers that make up an application into logical units (called pods) for easy management and discovery.

Container Instances

Container Instances is a serverless compute service that enables customers to run containers quickly and easily without managing any servers. Container Instances service runs a customers' containers on serverless compute optimized for container workloads that provides the same isolation as virtual machines.

Content Management

Content Management is a content hub used to drive omni-channel content management and accelerate experience delivery. Content Management allows customers to rapidly collaborate internally and externally on any device to approve content and create contextualized experiences. Built-in business-friendly tools allow for easy building of new web experiences. Customers can drive digital engagement with their stakeholders using the same content platform and the same processes.

Customer Feedback Service

Customer Feedback Service enables customers to provide feedback on a product or service. It is available to customers as part of the user interface within the Oracle Cloud Infrastructure console.

Data Catalog

Data Catalog is a metadata management service that helps data consumers discover data and improve governance in the Oracle ecosystem. Data analysts, data scientists, data engineers, and data stewards have a single self-service environment to discover the data that's available in the cloud sources. Data Catalog data providers create a data dictionary comprising of technical and business metadata. Data consumers can easily assess the suitability of data for analytics and data science projects.

Data Flow

Data Flow is running for Apache Spark applications. It allows developers to focus on their applications and provides an easy runtime environment to execute them. It has an easy and simple user interface with API support for integration with applications and workflows.

Data Integration

Data Integration is a multi-tenant service that helps data engineers and developers with data movement and data loading tasks. Powered by Spark Extract, Transform, and Load (ETL) or Extract, Load, and Transform (ELT) processes, a large volume of data can be ingested from a variety of data assets; cleansed; transformed and reshaped; and efficiently loaded to Oracle Cloud Infrastructure target data assets.

Data Labeling

Data labeling is the process of identifying properties (labels) of documents, text, and images (records), and annotating (labeling) them with those properties. The topic of a news article, the sentiment of a tweet, the caption of an image, important words spoken in an audio recording, the genre of a video are all examples of a data label. Many machine learning techniques require labeled data before they can be used to train machines to complete an autonomous task. Data labeling is thus an integral part of an Artificial Intelligence (AI) or Machine Learning (ML) project. Data Labeling enables customers to create and browse datasets, view data records (documents, text, and images), and apply labels to build AI/ML models.

Data Lake

Data Lake provides centralized storage and unified access control for structured and unstructured data. It helps secure and govern data stored in Object Storage and other Oracle databases.

Data Safe

Data Safe is an integrated service that provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases. Features include Security Assessment, User Assessment, Data Discovery, Data Masking, and Activity Auditing.

Data Science

Data Science is a serverless platform for data science teams to build, train, and manage machine learning models using Oracle Cloud Infrastructure.

Data Transfer

Data Transfer allows customers to migrate data to Oracle Cloud Infrastructure. Customers can also export data currently residing in Oracle Cloud Infrastructure to the data center offline. Customers can transfer data as files on encrypted USB 2.0/3.0 disk to an Oracle transfer site; as files on secure, high-capacity, Oracle-supplied storage appliances to an Oracle transfer site or customers can export their data from Object Storage bucket to their data center using an Oracle-provided appliance. Data Transfer uses the following encryption methods: data at rest is encrypted with AES-256 encryption, node-to-node communication is encrypted with GCM-AES-128, console and API are using TLS and will default to AES-256.

Database

Customers can use the Database service to create and manage Oracle Database instances and database system infrastructure.

Autonomous Database on Dedicated Exadata Infrastructure (ADB-D)

Autonomous Database provides a fully autonomous database that scales elastically, delivers fast query performance, and requires no database administration. Autonomous Database on Dedicated Exadata Infrastructure is a highly automated, managed database environment running in Oracle Cloud Infrastructure with committed hardware and software resources. It is a private dedicated database within a public cloud that completely isolates the customer's data and operations. These isolated resources enable customers to meet stringent security, availability, and performance requirements while reducing cost and complexity. Customers can configure their database in two different modes based on the workload type as Autonomous Data Warehouse or Autonomous Transaction Processing.

Autonomous Database on Exadata Cloud@Customer (ADB-C@C)

Autonomous Database on Exadata Cloud@Customer combines the benefits of a self-driving, self-securing, and self-repairing database management system and the security and control offered by having it deployed securely on-premise behind the customer's firewall. It is a database in the customer's data center to meet regulator, data sovereignty, or network latency requirements for workloads that cannot move to the public cloud. This deployment option enables IT to deliver self-service databases to business users and developers while ensuring the security and governance of data.

Autonomous Database Serverless

Autonomous Database Serverless handles provisioning the database, backing up the database, patching and upgrading the database, and growing or shrinking the database. Customers do not need to configure or manage any hardware or install any software. Autonomous Database is a completely elastic service.

Base Database

Oracle Base Database Service enables the customer to maintain control over their data while using the combined capabilities of Oracle Database and Oracle Cloud Infrastructure. Oracle Base Database Service offers database systems (DB systems) on virtual machines. They are available as single-node DB systems and multi-node RAC DB systems on Oracle Cloud Infrastructure (OCI). Customers can manage these DB systems by using the OCI Console, the OCI API, the OCI CLI, the Database CLI (DBCLI), Enterprise Manager, or SQL Developer.

Database Autonomous Recovery Service

Oracle Database Autonomous Recovery Service protects Oracle databases from accidental or malicious damage. With backup automation and enhanced data protection capabilities for databases, users can offload all backup processing and storage requirements. The Oracle Cloud Console provides a unified interface to configure the user's backup strategy. The options available in the Console centralize backup administration and monitoring for Oracle Cloud databases in user tenancies.

Exadata Database Machine

Exadata racks are "engineered systems" provisioned as dedicated hardware with embedded software, as though the customer had an on-premises rack. There are several system and shape configuration options available for Exadata. An Exadata consists of a base rack, quarter rack, half rack, or full rack of compute and storage servers. Exadata rack maintenance, security, and the embedded software development practices are not in the scope of the Oracle Cloud Infrastructure System.

Exadata Database on Cloud@Customer (ExaDB-C@C)

Exadata Database on Cloud@Customer allows customers to maintain control over their data while leveraging the combined capabilities of Exadata (data plane) and Oracle Cloud Infrastructure managed by Oracle, inside the customer's data center (control plane). Customers have full access to the features and capabilities of Oracle Database along with the intelligent performance and scalability of Exadata, but with Oracle owning and managing the Exadata infrastructure. Customers can use the Oracle Cloud Infrastructure console and APIs to manage ExaDB-C@C just as with any other cloud resource, while maintaining sovereignty over their data. Each Exadata Database on Cloud@Customer system configuration contains Exadata database servers and Exadata storage servers that are interconnected using a high-speed, low-latency RDMA fabric network, and intelligent Exadata software. Oracle also manages other ExaDB-C@C infrastructure components, including network switches, power distribution units (PDUs), and integrated lights-out management (ILOM) interfaces.

The ExaDB-C@C rack contains all the components of a standard Exadata, including a hypervisor equivalent referred to as Dom0, and two Control Plane Servers (CPS), in a highly available (HA) configuration that connect to an Oracle Cloud Infrastructure region. CPS is equivalent to a bastion plus other cloud tolling components running inside the ExaDB-C@C

environment that resides at the customer's data center. Access to CPS and Dom0 is restricted to Oracle and the access workflow is as follows in a sequential order: SSH to an Oracle Cloud Infrastructure bastion host, ExaDB-C@C Management Server within a region, CPS, Dom0. A Rest API runs in each region to connect to each rack and acts as a proxy to collect and send audit logs to the Oracle Cloud Infrastructure Security Information and Event Monitoring (SIEM) tool.

Exadata Database on Dedicated Infrastructure (ExaDB-D)

Exadata Database on Dedicated Infrastructure leverages the combined capabilities of Oracle Exadata and Oracle Cloud Infrastructure. Customers can provision flexible systems that allow them to add database compute services and storage services to their systems as their needs grow. For Exadata Cloud Infrastructure instances, customers can configure automatic backups, optimize different workloads, and scale the CPU and storage allocations as needed. Customers are responsible for the virtual machine operating system, Grid Infrastructure, and the database software maintenance. Oracle is responsible for the base operating system and hardware.

Database Management

Database Management provides comprehensive database performance diagnostics and management capabilities for Oracle Databases and MySQL HeatWave Database systems. In addition, customers can use Database Management to discover and monitor on-premises Oracle Database System components and Exadata Storage Infrastructure.

Database Migration

Database Migration helps database administrators move databases in real-time, at scale, from one or more source databases to Oracle Cloud databases. Configure, run, and monitor database migrations in a single interface.

Database Tools

Database Tools enables customers to create connections to any Oracle or MySQL HeatWave service in Oracle Cloud Infrastructure that can be reused by multiple users, resources, and services. The database connections can then be used with the SQL Worksheet to provide direct SQL access to those databases. Sensitive information such as passwords and Autonomous Database client credentials (wallet files) are stored securely and encrypted in the Oracle Cloud Infrastructure vault.

DevOps

DevOps is an end-to-end, continuous integration and continuous delivery (CI/CD) platform for developers. Using this service a DevOps engineer can easily build, test, and deploy software and applications on Oracle Cloud. The DevOps build and deployment pipelines reduce change-driven errors and decreases the time customers spend on building and deploying releases. The service also provides private Git repositories to store customers' code and supports connections to external code repositories.

DevOps - Build Pipelines

A build pipeline contains the stages that define the build process for successfully compiling, testing, and running software applications before deployment.

DevOps - Code Repositories

In the DevOps service, customers can create their own private code repositories or connect to external code repositories such as GitHub, GitLab, Bitbucket Cloud, Visual Builder Studio, Bitbucket Server, and GitLab Server.

DevOps - Deployment Pipelines

A deployment pipeline holds the requirements that must be satisfied to deliver a set of artifacts to the target environment. Deployment pipelines contain different stages for automated deployment. Each stage is associated with certain actions in the pipeline.

DevOps - Projects

A project logically groups the DevOps resources needed to implement a CI/CD workflow.

Digital Assistant

Digital Assistant is a cloud-based AI service that allows customers to create and deploy digital assistants, which are AI-driven interfaces that help users accomplish a variety of tasks in natural language conversations.

Distributed Denial of Service Mitigation

Oracle provides a Layer 7 Distributed Denial of Service (DDoS) Mitigation service to help mitigate layer 7 DDoS attacks. A layer 7 DDoS attack is a DDoS attack that sends HTTP/S traffic to consume resources and hamper a website's ability to deliver content or to harm the owner of the site. The Web Application Firewall (WAF) service can protect layer 7 HTTP-based resources from layer 7 DDoS and other web application attack vectors. DDoS Mitigation Specialists are trained members of Oracle Cloud Customer Support team who help mitigate layer 7 DDoS attacks.

Document Understanding

Document Understanding is an AI service that lets developers extract text, tables, and other key data from document files through APIs and CLI tools. With Document Understanding, customers can automate tedious business processing tasks with prebuilt AI models and customize document extraction to fit industry-specific needs.

Domain Name System (DNS)

Domain Name System (DNS) service helps customers [create and manage DNS zones](#). Customers can create zones, add records to zones, and allow Oracle Cloud Infrastructure's edge network to handle a domain's DNS queries. DNS translates human-readable domain names to machine-readable IP addresses. A DNS nameserver stores the DNS records for a zone and responds with answers to queries against its database.

Email Delivery

Email Delivery is an email sending service and SMTP relay that provides a fast and reliable managed solution for sending both high volume bulk and transactions emails that need to reach the inbox.

Events

Events allows customers to create automation based on the state changes of resources throughout their tenancy. Customers can use Events to enable their development teams to automatically respond when a resource changes its state.

Exadata Fleet Update

Exadata Fleet Update provides a way to automate database cloud fleet updates without customer development. It also orchestrates updates across the stack in a single maintenance window. It leverages fleet update capabilities of Fleet Patching and Provisioning (FPP). Exadata Fleet Update offers a simple and uniform "look and feel" for operations across multiple database versions, multiple database types, and dynamic runtime environments.

FastConnect

FastConnect provides an easy way to create a dedicated, private connection between the customer's data center and Oracle Cloud Infrastructure. FastConnect provides higher-bandwidth options, and a more reliable and consistent networking experience compared to internet-based connections. With FastConnect, customers can choose to use private peering or public peering. With FastConnect, there are different connectivity models to choose from including Oracle Partners, Third-Party Provider, or Colocation with Oracle in an Oracle Cloud Infrastructure FastConnect location. FastConnect private connection is also used as a connection between Oracle Cloud Infrastructure and Microsoft Azure, also known as the Oracle Interconnect for Azure.

File Storage

File Storage provides a durable, scalable, secure, enterprise-grade network file system. Customers can connect to a File Storage service file system from any bare metal, VM, or container instance in their VCN. Customers can also access a file system from outside the VCN using VCN Peering, FastConnect, and Internet Protocol security (IPSec) virtual private network (VPN). The File Storage service encrypts all file system and snapshot data at rest using AES 256-bit encryption. By default, all file systems are encrypted using Oracle-managed encryption keys. The customer has the option to encrypt File Storage with keys that the customer owns and manages via the Vault service.

Full Stack Disaster Recovery

Full Stack Disaster Recovery is a disaster recovery orchestration and management service that provides comprehensive disaster recovery capabilities for all layers of an application stack, including infrastructure, middleware, database, and application.

Functions

Functions is a serverless platform that enables customers to create, run, and scale business logic without managing any infrastructure.

Fusion Analytics Warehouse

Fusion Analytics Warehouse provides analytics for Oracle Applications Cloud, powered by Autonomous Data Warehouse and Oracle Analytics. The service extracts and loads data from Oracle Fusion Cloud Applications into an instance of Oracle Autonomous Data Warehouse. Users can then create and customize dashboards in Oracle Analytics Cloud.

Fusion Applications Environment Management

The Oracle Cloud Console provides self-service management of the environments where customers provision, run, and maintain their Fusion Applications. Databases supporting Fusion Applications are managed by Oracle and utilize the ExaDB-D service.

When a customer subscribes to Fusion Applications, they are allotted one production environment and one test environment. The customer has the option of purchasing development environments. Before the customer provisions these environments, they need to set up an environment family. The environment family ensures that the applications on all the customers environments are maintained, upgraded, and patched at the same levels. An environment is the platform where applications are provisioned. The environment provides a single management interface for the installed applications.

Generative AI

Generative AI provides a set of state-of-the-art, customizable large language models (LLMs) that cover a wide range of use cases for text generation. Use the playground to try out the ready-to-use pretrained models or create and host fine-tuned customer models based on data on dedicated AI clusters.

Globally Distributed Autonomous Database – From April 23rd, 2024

Oracle Globally Distributed Autonomous Database is a cloud-based database service that enables the sharding of data across globally distributed converged databases. It is designed to support large-scale, mission-critical applications. It is a highly available, fault-tolerant, and scalable database service that enables organizations to store and process massive amounts of data with high performance and reliability.

GoldenGate

GoldenGate helps data engineers move data in real-time, at scale, from one or more data management systems to Oracle Cloud databases. Users can design, run, orchestrate, and monitor data replication tasks in a single interface without having to allocate or manage any compute environments.

Health Checks

Health Checks provides users with high frequency external monitoring to determine the availability and performance of any publicly facing service, including hosted websites, API endpoints, or externally facing load balancers.

Identity and Access Management

Identity and Access Management (IAM) provides identity and access management features such as authentication, single sign-on (SSO), and identity lifecycle management for Oracle Cloud as well as for Oracle and non-Oracle applications, whether SaaS, cloud-hosted, or on-premises. Employees, business partners, and customers can access applications at any time, from anywhere, and on any device in a secure manner. IAM allows users to control who has access to their cloud resources. They can control what type of access a group of users has and to what specific resources. IAM can be used with or without identity domains.

Instance Security

Instance Security provides runtime security for workloads in Compute virtual and bare metal hosts. Instance Security expands Cloud Guard from cloud security posture management to cloud workload protection. It ensures that security needs are met in one place with consistent visibility and holistic understanding of the security state of infrastructure.

Integration

Integration allows customers to integrate their cloud and on-premises applications, automate business processes, develop visual applications, use a Secure File Transfer Protocol (SFTP) compliance file server to store and retrieve files, and exchange business documents with a B2B trading partner.

Intelligent Advisor

Intelligent Advisor is designed to deliver consistent and auditable advice across channels and business processes by capturing rules in natural language and building interactive customer service experiences called interviews around those rules.

Inter-Region Latency

The Inter-Region Latency dashboard in the Console provides the average network round-trip latency for all pairs of regions in an Oracle Cloud Infrastructure realm. The dashboard shows a current snapshot view and lets the user view historic snapshots including up to a 30-day history.

Java Management

Java Management Service is a reporting and management infrastructure integrated with Oracle Cloud Infrastructure Platform services to observe and manage the use of Java in the user's environment.

Language

Language is a cloud-based AI service that allows users to perform sophisticated text analysis at scale. Using the pretrained and custom models, users can process unstructured text to extract insights without data science expertise. Pretrained models include sentiment analysis, key phrase extraction, text classification, and named entity recognition. Users can also train custom models for named entity recognition and text classification with domain specific datasets. Additionally, text can be translated across numerous languages.

License Manager

License Manager allows users to bring their own licenses (BYOL) into Oracle Cloud Infrastructure.

Load Balancer

Load Balancer provides automated traffic distribution from one entry point to multiple servers reachable from a virtual cloud network (VCN). The service offers a load balancer with the user's choice of a public or private IP address, and provisioned bandwidth.

Logging

Logging is a highly scalable single pane of glass for all the logs in a user's tenancy. Logging provides access to logs from Oracle Cloud Infrastructure resources. These logs include critical diagnostic information that describes how resources are performing and being accessed.

Logging Analytics

Logging Analytics allows users to index, enrich, aggregate, explore, search, analyze, correlate, visualize and monitor all log data from their applications and system infrastructure.

Managed Access

Oracle Managed Access lets users manage requests for temporary access to their organization's cloud resources from Oracle Cloud Infrastructure authorized operators. Occasionally, authorized operators need to access resources to troubleshoot or help resolve an issue. Oracle Managed Access provides a secure workflow through which operators request access to the customer's cloud environment. The customer can approve or deny the access requests.

Management Agent

Management Agent provides low latency interactive communication and data collection between Oracle Cloud Infrastructure and any other targets. Users can deploy management agents to collect data from services and sources that they want to monitor. It manages the lifecycle of the management agent and the plug-ins for the services.

Marketplace – Consumer

Marketplace is an online store that offers a catalog of listings offered by approved and registered publishers. Use Marketplace to find an image, stack, container image, and helm chart and seamlessly deploy it on Oracle Cloud Infrastructure.

Media Services

Media Services processes media (video) source content. It provides scalable distribution and origination for just-in-time packaged adaptive bitrate (ABR) video content. Media Services includes two components, Media Flow, and Media Streams, which can be used independently or together and operate on the content stored in Object Storage.

Monitoring

Monitoring allows users to monitor query metrics and alarms. Metrics and alarms help monitor the health, capacity, and performance of cloud resources.

MySQL Heatwave

MySQL Heatwave is a database service, powered by the integrated HeatWave in-memory query accelerator. It combines transactions, analytics, and machine learning services into MySQL Heatwave, delivering real-time, secure analytics without the complexity, latency, and cost of ETL duplication.

NetSuite Analytics Warehouse

NetSuite Analytics Warehouse (NSAW) is an analytical application solution that extracts data from NetSuite and makes it available for analytic consumption through Fusion Analytics Warehouse (FAW) on Oracle Cloud Infrastructure. NSAW enables businesses to analyze historical data from multiple sources and determine how to improve their business.

NetSuite Health Check

NetSuite Health Check is an Oracle internal service that provides the reporting capability of the performance of a NetSuite environment, by checking and grading Backend, Integrations, Customizations and Events against NetSuite Leading Practices. NetSuite customers do not have direct access to the health check tool. NetSuite performance reports can be provided by customer requests.

Network Firewall

Network Firewall is a network firewall and intrusion detection and prevention service for Oracle Cloud Infrastructure VCNs, powered by Palo Alto Networks®. The Network Firewall service gives visibility into traffic entering cloud environments as well as traffic between subnets.

Network Load Balancer

Network Load Balancer provides automated traffic distribution from one entry point to multiple servers in a backend set. Network Load Balancers ensure that services remain available by directing traffic only to healthy servers based on Layer 3/Layer 4 (IP protocol) data.

Network Path Analyzer

Network Path Analyzer (NPA) provides a unified and intuitive capability users can use to identify virtual network configuration issues that impact connectivity. NPA collects and analyzes the network configuration to determine how the paths between the source and the destination function or fail. No actual traffic is sent, instead the configuration is examined and used to confirm reachability.

Networking

Networking uses virtual versions of traditional network components:

Virtual Cloud Network

A virtual cloud network (VCN) is a virtual private network that users set up in Oracle data centers. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that users can choose to use. A VCN resides in a single Oracle Cloud Infrastructure region and covers one or more CIDR blocks (IPv4 and IPv6, if enabled).

Subnets

Subnets are subdivisions defined in a VCN. Subnets contain virtual network interface cards (VNICs), which attach to instances. Each subnet consists of a contiguous range of IP addresses that do not overlap with other subnets in the VCN. Subnets can be designated to exist in either a single AD or across an entire region.

Virtual Network Interface Card

A virtual network interface card (VNIC) attaches to an instance and resides in a subnet to enable a connection to the subnet's VCN. The VNIC determine how the instance connects with endpoints inside and outside of the VCN.

Private IP

A private IPv4 address and related information for addressing an instance. Each VNIC has a primary private IP, and users can add and remove secondary private IPs.

Public IP

A public IPv4 address and related information. Users can optionally assign a public IP to their instances or other resource that have a private IP. Public IPs can be either ephemeral or reserved.

IPv6

An IPv6 address and related information. IPv6 addressing is supported for all commercial and government regions.

Dynamic Routing Gateway

Dynamic Routing Gateway (DRG) is an optional virtual router that users can add to their VCN. It provides a path for private network traffic between the user's VCN and on-premises network.

Internet Gateway

Internet Gateway is an optional virtual router that users can add to their VCN for direct Internet access.

Network Address Translation Gateway

Network Address Translation (NAT) Gateway is an optional virtual router that users can add to their VCN to give cloud resources without public IP addresses access to the internet without exposing those resources to incoming internet connections.

Service Gateway

Service Gateway is an optional virtual router that users can add to their VCN to provide a path for private network traffic between their VCN and supported Oracle Cloud Infrastructure services.

Local Peering Gateway

Local Peering Gateway (LPG) is an optional virtual router that users can add to their VCN to allow peering one VCN with another VCN in the same region.

Remote Peering Connection

Remote Peering Connection (RPC) is a component users can add to a DRG that allows peering of one VCN with another VCN in a different region.

Route Tables

Virtual route tables for user's VCN that have rules to route traffic from subnets to destinations outside the VCN by way of gateways or specially configured instances.

Security Rules

Virtual firewall rules, ingress and egress, for user's VCN that specify the types of traffic (protocol and port) allowed in and out of the instances. The user can designate whether a given rule is stateful or stateless. To implement security rules, users can use network security groups or security lists.

Dynamic Host Configuration Protocol (DHCP) Options

Configuration information that is automatically provided to the instances when they boot up.

NoSQL Database

NoSQL Database is designed for database operations that require predictable, single digit millisecond latency responses to simple queries. NoSQL Database allows developers to focus on application development rather than setting up cluster servers, or performing system monitoring, tuning, diagnosing, and scaling. NoSQL Database is suitable for applications such as Internet of Things, user experience personalization, instant fraud detection, and online display advertising.

Notifications

Notifications lets users know when something happens with their resources in Oracle Cloud Infrastructure. Using alarms, event rules, and connectors, users can get human-readable messages through supported endpoints, including email and text messages (SMS). Users can also automate tasks through custom HTTPS endpoints and Oracle Cloud Infrastructure Functions.

Object Storage

Object Storage can store an unlimited amount of unstructured data of any content type, including analytic data and rich content, like images and video. Customers can safely and securely store or retrieve data directly from the internet or from within the cloud platform. Object Storage is a regional service and is not tied to any specific compute instance. By default, Object Storage encrypts object data on the server with AES 256-bit encryption at rest. The customer has the option to encrypt Object Storage with keys that the customer owns and manages via the Vault service.

OCI Cache (formerly known as Cache with Redis)

OCI Cache is a managed service that enables customers to build and manage Redis clusters, which are memory-based storage solutions for their applications. Cache with Redis handles the management and operations of clusters, including operations such as security updates.

OCI Control Center (formerly known as Operator Insights)

OCI Control Center is only applicable for Dedicated Region customers. OCI Control Center (OCC) enables customers to monitor region-level cloud consumption and manage capacity requests, in realms where OCI Control Center is available.

OCI Database with PostgreSQL

PostgreSQL-compatible service leads with intelligent sizing, tuning, and high durability. The service automatically scales storage as database tables are created and dropped, making management easier and optimizing storage spend. Data is encrypted both in-transit and at rest.

Operator Access Control

Oracle Operator Access Control enables customers to grant, audit, and revoke the access Oracle has to their Exadata Infrastructure, Exadata Infrastructure hosting an Oracle Autonomous Database on Exadata Cloud@Customer, and Autonomous Exadata VM Cluster (client virtual machines deployed on Oracle Autonomous Database on Exadata Cloud@Customer) administered by Oracle, and to obtain audit reports of the actions taken by a human operator, in a near real-time manner.

Ops Insights

Ops Insights provides comprehensive information about the resource use and capacity of databases and hosts. Use this service to analyze CPU and storage resources, forecast capacity issues, and proactively identify SQL performance issues across a database fleet.

Oracle Cloud Migrations

Oracle Cloud Migrations service provides an end-to-end comprehensive self-service experience for migrating existing VMware virtual machine-based workloads from on-premises to Oracle Cloud Infrastructure.

Oracle Database Service for Azure

Oracle Database Service for Azure delivers Oracle Database services in Oracle Cloud Infrastructure directly to Microsoft Azure customers through the Oracle Cloud Infrastructure Azure Interconnect (also known as FastConnect), a capability available between the two cloud environments in regions located around the world. Oracle Database Service for Azure uses a service-based approach and is an alternative to manually creating complex cross-cloud deployments using FastConnect. Oracle Database Service for Azure offers the following types of database systems: Oracle Exadata Database Service on Dedicated Infrastructure, Autonomous Database Serverless, Base Database, and MySQL Heatwave.

Oracle Database@Azure

Oracle Database@Azure is an Oracle Cloud database service that runs Oracle Database workloads in a customer's Azure environment. Oracle Database@Azure offers Oracle Exadata Database Service and Oracle Autonomous Database. This service allows customers to monitor database metrics, audit logs, events, logging data, and telemetry natively in Azure. It runs on infrastructure managed by Oracle's Cloud Infrastructure operations team who performs software patching, infrastructure updates, and other operations through a connection to Oracle Cloud. While the service requires that customers have an Oracle Cloud Infrastructure tenancy, most service activities take place in the Azure environment.

The Oracle Database@Azure documentation is also available in the Azure documentation at [Oracle Database@Azure Overview](#).

Subservice Organization

The Oracle Database@Azure service uses a subservice organization, Microsoft Azure, to support the physical and environmental components of the service. All infrastructure for Oracle Database@Azure is co-located in Azure's physical data centers and uses Azure Virtual Network for networking, managed within the Azure environment. Federated identity and access management for Oracle Database@Azure is provided by Microsoft Entra ID. Azure Virtual Network and Microsoft Entra ID are not within the scope of the System.

Oracle Ksplice

Use Oracle Ksplice to apply critical security patches to Linux kernels on Oracle Cloud Infrastructure instances without requiring a reboot. On Oracle Linux, Ksplice also updates the glibc and OpenSSL user space libraries, applying critical security patches without disrupting workloads.

Oracle Open Data

Oracle Open Data is a free repository of scientifically relevant data sets from trusted sources for researchers, educators, data scientists, analysts and anyone interested in data. Purpose-built tools enable users to concentrate on using large data sets and metadata to achieve the results they need. This repository includes public-domain data for Life Sciences, Geo-spatial and AI/ML for users to find, consume and use to discoveries that matter.

Oracle Search Cloud

Oracle has its own internal search service that can provide a high performing search engine with near real-time capabilities to power Cloud Services. It enables the business to ingest, query, and analyze data efficiently. Oracle Search Cloud is an internal Oracle service.

OS Management

OS Management allows users to manage and monitor updates and patches for the operating system environments, including Oracle Autonomous Linux, and discover and monitor resources on their instances.

OS Management Hub

Oracle OS Management Hub is the next generation management solution for operating system environments. It provides a centralized management console to monitor and manage updates across customers' entire environments.

OS Management Hub monitors available Oracle Linux and Microsoft Windows Server environments at scale. From a single view, customers gain control of updates over their entire environment, reducing administration and improving efficiency. OS Management Hub is delivered as an Oracle Cloud Infrastructure (OCI) service. It can manage instances in OCI, supported third-party clouds, or on premises in a customer data center.

Process Automation

Process Automation allows users to rapidly design, automate, and manage business processes in the cloud. With Process Automation design-time (Designer) and the runtime (Workspace) environments, users can create, develop, manage, test, and monitor process applications and their components.

Publisher

The Publisher service is an extension of the Oracle Cloud Marketplace Partner Portal service. Users can create and publish listings and artifacts in Marketplace.

Queue

Queue is a serverless service that helps decouple system and enable asynchronous operations. Queue handles high-volume transactional data that requires independently processed messages without loss or duplication.

Registry

Registry, also known as Container Registry, enables users to store, share, and manage container images (such as Docker images) in an Oracle-managed registry.

Resource Manager

Resource Manager automates deployment and operations for Oracle Cloud Infrastructure resources. Using the infrastructure-as-code (IaC) model, the service is based on Terraform, an open-source industry standard that lets DevOps engineers develop and deploy their infrastructure anywhere.

Roving Edge Infrastructure

Roving Edge Infrastructure is a cloud-integrated service that puts fundamental Oracle Cloud Infrastructure services where data is generated and consumed. Roving Edge Infrastructure devices provide high-performance computing, such as analytics, machine learning, and location-based services, and storage capabilities that operate with intermittent or no internet connectivity.

Search

Search allows users to find resources within a tenancy, Console pages in services, and documentation within the Oracle Cloud Infrastructure Getting Started Guide and User Guide.

Search with OpenSearch

Search with OpenSearch enables users to build in-application search solutions based on OpenSearch to search large datasets and return results in milliseconds, without having to focus on managing infrastructure. Search with OpenSearch handles all the management and operations of search clusters, including operations such as security updates, upgrades, resizing, and scheduled backups.

Security Assurance System

The Security Assurance System provides infrastructure and support services that facilitate Oracle's delivery of security services. Within this system, Gateways mediate data flows and Oracle conducts various analyses of traffic that passes through Gateways based on use-cases that align with assurance objectives related to the understanding and monitoring of network traffic. The security assurance system also includes components that facilitate access control and the collection of performance data and logs. Additionally, the system includes facilities called Dedicated Transparency Centers that enable Oracle to provide specific software assurance services.

Secure Desktops

Secure Desktops allows an administrator to create a set of identically configured virtual desktops, which individual users can then securely access. An administrator can create pools of desktops in their tenancy, based on existing compute shapes or custom images.

Security Zones

Security Zones lets users be confident that their resources in Oracle Cloud Infrastructure, including Compute, Networking, Object Storage, and Database resources, comply with their security principles.

Serverless Kubernetes

Virtual nodes provide a serverless Kubernetes experience, enabling users to run containerized applications at scale without the operational overhead of managing, scaling, upgrading, and troubleshooting the node infrastructure. Virtual nodes provide granular pod-level elasticity and pay-per-use pricing. As a result, users can scale deployments without taking into consideration the cluster's capacity, simplifying the execution of scalable workloads such as high-traffic web applications and data-processing jobs. Users create virtual nodes by creating virtual node pools in enhanced clusters.

Service Connector Hub

Service Connector Hub is a cloud message bus platform that offers a single pane of glass for describing, executing, and monitoring interactions when moving data between Oracle Cloud Infrastructure services.

Service Manager Proxy

Service Manager Proxy is used to obtain information about SaaS environments provisioned by Service Manager. Customers can get information such as service types and service environment URLs.

Service Mesh

Service Mesh allows users to add a set of capabilities that enable microservices within a cloud native application to communicate with each other in a centrally managed and secure manner. Service Mesh includes standardized patterns around observability, security, and traffic management for communication between microservices.

Site-to-Site VPN

Site-to-Site VPN provides site-to-site IPSec connection between users' on-premises network and virtual cloud network (VCN). The IPSec protocol suite encrypts IP traffic before the packets are transferred from the source to the destination and decrypts the traffic when it arrives.

Speech

Speech is a cloud-based AI service that can transcribe customer service calls, automate subtitling, and generate metadata for media assets to create a fully searchable archive.

Stack Monitoring

Stack Monitoring allows users to proactively monitor an application and its underlying application stack, including application servers and databases. It starts by discovering all components of the application, including the application topology. Once discovered, it automatically collects status, load, response, error, and utilization metrics for all application components.

Status

Status allows users to view the status of Oracle Cloud Infrastructure services in a region on a dashboard, and query service status programmatically.

Streaming

Streaming provides a scalable and durable storage solution for ingesting and consuming high-volume streams in real time. It can be used for any use case in which data is produced and processed continually and sequentially in a publish-subscribe messaging model.

Subscription Pricing Service

Subscription Pricing Service is responsible for maintaining product, price list, subscription configurations, and pricing rules information in an Alloy realm. Subscription service generates rate cards and make them available for metering for cost computation purposes.

Tagging

Tagging allows users to add metadata to resources, which enables them to define keys and values and associate them with resources. Tags can be used to organize resources based on business needs.

Threat Intelligence

Threat Intelligence allows users to search for information about known threat indicators, including suspicious IP addresses, domain names, and other digital fingerprints.

Vault

Vault is an encryption management service that stores and manages encryption keys and secrets to securely access resources. Vaults securely store master encryption keys and secrets that might otherwise be stored in configuration files or in code. Specifically, depending on the protection mode, keys are either stored on the server or they 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.

The key encryption algorithms that the Vault service supports includes the Advanced Encryption Standard (AES), the Rivest-Shamir-Adleman (RSA) algorithm, and the elliptic curve digital signature algorithm (ECDSA). Customers can create and use AES symmetric keys and RSA asymmetric keys for encryption and decryption. Customers can also use RSA or ECDSA asymmetric keys for signing digital messages.

Customers can use the Vault service to create and manage vaults, keys, and secrets:

- Vaults – logical entities where the Vault service creates and durably stores keys and secrets
- Keys – logical entities that represent one or more key versions, each of which contains cryptographic material
- Secrets – credentials such as passwords, certificates, SSH keys, or authentication tokens

In addition, integration with IAM allows customers to control who and what services can access which keys and secrets and what they can do with those resources. Audit integration allows customers to monitor key and secret usage. Audit tracks administrative actions on vaults, keys, and secrets.

For a list of Oracle Cloud Infrastructure services that integrate with the Vault service to support the use of customer-managed keys to encrypt data in their respective, specified resources, see the [Vault Overview](#).

Customers also have the ability to Bring Your Own Keys (BYOK) to Oracle Cloud Infrastructure, create them in Oracle Cloud Infrastructure, or Hold Your Own Keys (HYOK) external to Oracle Cloud Infrastructure.

Vision

Vision is a serverless, multi-tenant AI based service, accessible using the Console, or over REST APIs. Users can upload images to detect and classify objects in them. If a user has lots of images, they can process them in batch using asynchronous API endpoints.

Visual Builder

Visual Builder is a cloud-based software development platform and a hosted environment for application development infrastructure. IT provides an open-source standards-based solution to develop, collaborate on, and deploy applications within Oracle Cloud.

Visual Builder Studio

Visual Builder Studio is an application development platform that helps users plan and manage work throughout all stages of the application development lifecycle: design, build, test, and deploy.

VMware Solution

VMware Solution is used to create and manage VMware enabled software-defined data centers (SDDCs) in Oracle Cloud Infrastructure.

Vulnerability Scanning

Vulnerability Scanning helps improve security posture by routinely checking hosts for potential vulnerabilities. The service gives developers, operations, and security administrators comprehensive visibility into misconfigured or vulnerable resources and generates reports with metrics and details about these vulnerabilities including remediation information.

Web Application Acceleration

Web Application Acceleration is used to speed up traffic on load balancers by applying a combination of caching and compression.

Web Application Firewall

Web Application Firewall (WAF) is a regional-based and edge enforcement service that is attached to an enforcement point, such as a load balancer or a web application domain name. It protects applications from malicious and unwanted internet traffic. WAF can be configured to protect any internet facing endpoint, providing consistent rule enforcement across the customer's applications.

Relevant Aspects of the Control Environment

The control environment is embodied by the organization's awareness of the need for controls and the emphasis given to the appropriate controls as demonstrated by the organization's policies, procedures, organizational structure, and management actions. The primary elements of the control environment include commitment to integrity and ethical values, oversight responsibility of the Board of Directors, assignment of authority and responsibility, commitment to competence, and accountability.

Commitment to Integrity and Ethical Values

Oracle has a reputation for secure and reliable product offerings and related services, and it has invested a great deal of time and resources in protecting the integrity and security of products, services, and the internal and external data managed therein.

Oracle has a Compliance and Ethics Program that includes a Code of Ethics and Business Conduct (CEBC), which defines and implements the Company's core values, that applies to all Oracle entities. Core values include integrity, ethics, compliance, mutual respect, teamwork, communication, innovation, customer satisfaction, quality, and fairness. The CEBC supplements and, in many cases, exceeds what is required to comply with laws and regulations. The Oracle CEBC applies to all personnel employed by or engaged to provide services to Oracle, including, but not limited to, Oracle's employees, officers, temporary employees, workers (including agency workers), casual staff, and independent contractors ("employees"). Oracle also requires its partners and suppliers to adhere to the Partner Code of Ethics and Business Conduct and its suppliers to adhere to the Supplier Code of Ethics and Business Conduct as well as the Oracle Supply Chain Security and Assurance guidance, which are available on the Oracle website.

The Global Anti-Corruption Policy and Business Courtesy Guidelines (ACP), which also applies to all employees, supplements the CEBC. These documents are posted on both internal and external corporate websites.

Each new employee is required to complete and sign an employment agreement or equivalent and a Proprietary Information Agreement prior to or on the day of hire (or as otherwise required under applicable law), in accordance with local procedures, laws, and regulations. Additionally, all employees are required to take an Ethics and Business Conduct training upon hire and every two years thereafter.

A confidential ethics helpline has been established for Oracle employees and non-Oracle employees, such as business partners, customers, and other stakeholders, to field concerns, questions, or to report violations of the CEBC. The reporting site allows employees to report compliance and ethics situations confidentially and/or anonymously, where allowed by local law. A summary of items communicated via the ethics helpline, including fraud, are presented to the Finance and Audit Committee with specific reference to items impacting the financial statements.

Oversight Responsibility of the Board of Directors

A corporate governance framework is in place at Oracle for continuity and quality monitoring of the control environment. The control environment at Oracle Cloud Infrastructure originates with, and is the responsibility of, the Oracle Board of Directors. The Board of Directors provides oversight of Oracle Cloud Infrastructure operations and activities including oversight of the Finance and Audit Committee.

Oracle Legal reviews the profiles of Board members to ensure the board and committee members meet current regulatory and internal requirements, including independence and expertise.

Oracle maintains, and distributes externally via its website, its Corporate Governance Guidelines as well as charters for its Finance and Audit Committee, Independent Committee, Compensation Committee, and Nomination and Governance Committee.

Assignment of Authority and Responsibility

Executive management recognizes its responsibility for directing and controlling operations, managing risks, and establishing, communicating, and monitoring control policies and procedures. Management recognizes its responsibility for establishing and maintaining sound internal control and promoting integrity and ethical values to all personnel on a day-to-day basis. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. Oracle Cloud Infrastructure has developed an organizational structure to meet its needs in support of its control obligations. Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel supporting system design, development, implementation, security, operation, maintenance, and monitoring. The current management structure has adequate diversification and segregation of responsibility across executive management to ensure no overriding influence exists within the current reporting structure. In addition, Oracle provides IT security oversight to identify and implement security controls and processes in the IT control environment that align with organizational objectives.

Oracle is supported by the following security groups, which provide oversight of internal IT resources and suppliers.

SECURITY GROUP	ROLES AND RESPONSIBILITIES
Global Information Security	Global Information Security (GIS) is responsible for security oversight, compliance and enforcement, and conducting information assessments leading the development of information security policy and strategy, as well as training and awareness at the corporate level. This organization serves as the primary contact for security incident response, providing overall direction for incident prevention, identification, investigation, and resolution.
Global Product Security	Under the leadership of Oracle's Chief Security Officer, Global Product Security promotes the use of Oracle Software Security Assurance standards throughout Oracle, acts as a central resource to help development teams improve the security of their products, and handles specialized security functions.
Global Physical Security	Responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets.

SECURITY GROUP	ROLES AND RESPONSIBILITIES
Global Trade Compliance	Responsible for import and export oversight, guidance, and enforcement to enable worldwide trade compliant business processes across Oracle, to uphold and protect Oracle's global trade privileges and ensure the success of Oracle's business.
Security Architecture	The Oracle 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.
Business Assessment and Audit	Oracle's Business Assessment & Audit (BA&A) is an independent global audit organization which performs global process and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards and select laws and regulations across Oracle's Lines of Business and business units. Any key risks or control gaps identified by BA&A during these reviews are tracked through remediation. These reviews, identified risks or control gaps are confidential and shared with executive leadership and Oracle's Board of Directors.

Commitment to Competence

Oracle Cloud Infrastructure's commitment to employee competence begins with formal hiring practices designed to help ensure that new employees are qualified for their job responsibilities. The hiring process also includes a robust background check, performed on candidates selected for hire, in accordance with local laws and regulations, and local Oracle policy.

New employees are supported by a new hire web site and orientation courses. Ongoing training is available to all employees through a variety of courses delivered through web learning and external courses. Training for each employee is tailored to support his or her job role.

Employees are required to complete the Ethics and Business Conduct, Information Protection Awareness, and the Anti-Corruption & Foreign Corrupt Practices Act online courses upon hire. All Oracle employees are required to complete Information Protection Awareness training every two years. The Human Resources (HR) Training team runs exception reports monthly to identify any employees or managers not in compliance with these courses and follows up with those individuals by email.

Oracle Cloud Infrastructure employees must complete security awareness training specific to the services annually. This training includes Oracle Cloud Infrastructure requirements, the process to report and respond to potential incidents and specific security training tailored to the System. Additionally, employees with access to source code are required to complete annual secure code training. The Oracle Cloud Infrastructure Security Training team runs exception reports on a periodic basis to identify employees not in compliance with the requirement to complete the annual training and follows up with those individuals' managers by email.

Critical information is disseminated via email throughout the company. Employees are also informed about company events, security updates and other matters through the company website "In the Know".

In addition, Oracle conducts annual appraisal and performance management process for all Oracle employees. The performance management process follows a performance evaluation framework and clarifies how employees are expected to perform, how they will be measured, and how their work fits into the larger business context.

Accountability

Oracle Cloud Infrastructure's commitment to an effective system of internal control begins with the Oracle Board of Directors and Finance and Audit Committee. The primary functions of the Finance and Audit Committee (the "Committee") are to assist the Board of Directors (the "Board") of Oracle Corporation with the Board's oversight of: management's conduct of the

Corporation's financial accounting and reporting processes; the integrity of the Corporation's financial statements; the Corporation's compliance with legal and regulatory requirements; its independent registered public accounting firm's qualifications, performance and independence; the performance of the Corporation's internal audit function; and the evaluation of merger and acquisition transactions and investment transactions proposed by the Corporation's management. The Finance and Audit Committee holds regular meetings as necessary, but not less than quarterly, and special meetings as may be called by the Chairman of the Committee.

Oracle has developed internal policies outlining corporate requirements to hold individuals accountable for their internal control responsibilities. The policies are managed centrally, reviewed at least annually and are available to all personnel. Per the Authority, Enforcement, Exceptions, and Violations Policy, Oracle employees and contingent workers are required to comply with all laws, regulations, contractual obligations, and Oracle policies. Non-compliance with laws, regulations, and Oracle policies may result in disciplinary action up to and including termination. Requests for an exception to an information security policy must be made as directed in the Corporate Security Exception Management Process.

In addition to corporate policies, Oracle Cloud Infrastructure has designed and implemented a set of robust internal controls and standards outlining detailed requirements for various processes undertaken and managed by Oracle personnel and provide direction for all activities performed. The standards are managed centrally, reviewed at least annually, and made available to all personnel.

Services must successfully complete the Customer Readiness Program Process prior to inclusion in compliance assessments. This process requires security and privacy reviews performed by Oracle Cloud Infrastructure Release Management, Compliance Onboarding, Privacy, Enterprise Risk Management, and Resilience & Crisis Management.

Information and Communication

MyOracle Support

Oracle customers can access information online through MyOracle Support (MOS), which is Oracle Corporation's portal for technical support services, the primary means of logging electronic Service Requests (SRs), and the source of a variety of support services and information for Oracle customers.

Oracle Cloud Infrastructure customers may use MOS to view the knowledge base and technical support services information; search for updates, alerts, and other information about products and releases; and set automated notification preferences regarding newly available information.

Customers may use MOS to log electronic SRs, or they can report incidents to their customer account manager, who is responsible for opening a SR ticket within the Oracle Cloud Infrastructure system tool for tracking and resolution.

Operator Console Support

For Oracle Alloy and multi-tenant DRCC, the Fusion support portal in the operator console provides an interface to search for and create SRs regarding the System.

External Communication

Oracle Cloud Infrastructure maintains a description of services, Oracle commitments and obligations, and detailed information relating to customer responsibilities and customer support guides on the Oracle public website. The process for external parties to report incidents to Oracle is also outlined on the Oracle public website. Customers have access to information about Oracle corporate security via Oracle's publicly available Security Practices document, Cloud Hosting and Delivery Policies, Global Customer Support Security Practices, Consulting Security Practices, and Advanced Customer Services Security Practices.

Oracle has standard terms and conditions that govern the use of Cloud Services that are publicly available and indicates the date of its most recent update. During the customer order process, customers are required to acknowledge the Oracle Cloud Services Agreement, which outlines customer responsibilities and Oracle's responsibilities, objectives, and commitments. Amendments to the standard Oracle Cloud Services Agreement require advanced approval.

Oracle Cloud Infrastructure service release notes are publicly available. Incidents that cause a customer outage, as well as system decommission or replacement events that will result in customer downtime, are reviewed and communicated to the impacted customer. Oracle Cloud Infrastructure investigates and responds, as appropriate, to actual, attempted or threatened unauthorized use or violation of the confidentiality, integrity, or availability of Oracle Cloud Infrastructure assets. In accordance with Oracle policies and procedures, Oracle Cloud Infrastructure reports confirmed security incidents with customer impact to Oracle Global Information Security and Oracle Legal, who are responsible for notices or disclosures to the public, customers, affected individuals, and law enforcement authorities.

Security 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. These security practices include a suite of internal information security policies as well as customer-facing security practices that apply to different service lines.

Oracle's security practices are designed to protect the confidentiality, integrity, and availability of both customer and Oracle data. Oracle continually works to strengthen and improve the security controls and practices for Oracle internal operations and services offered to customers.

Data Classification

When new service offerings are available to customers, the data gathered by the service is classified and documented according to the Oracle corporate policy. The [Data Processing Agreement for Oracle Services](#), which is publicly available, defines how to handle personal data. Additionally, the [Oracle Services Privacy Policy](#) describes the conditions under which Oracle may access, collect, and/or use services data, which includes customers' development, test, or production environments. The policy is publicly available and indicates the date of the most recent update.

Risk Assessment

Oracle values the necessary balance between risk and control, and that the intent of risk management is to reduce risk to an acceptable level. Risk is integral to the pursuit of value, which is a function of risk and return. Oracle seeks to manage risk exposures to incur just enough of the right kinds of risk to effectively pursue strategic goals.


Oracle Business Assessment & Audit (BA&A) conducts an annual Global Risk Assessment of key business processes at Oracle. Upon request, members of management across the company update their risk assessment of each process against two factors: likelihood of control/process issues and importance to business strategy. In addition, BA&A meets with senior management, Executive Committee members, the Finance and Audit Committee Chair, and the Board Chair to discuss company risk.

The Oracle Cloud Infrastructure Global Enterprise Risk team is responsible for identifying, analyzing, measuring, mitigating/responding to, and monitoring risk specific to the Oracle Cloud Infrastructure organization. In accordance with the Cloud Compliance Standard for Risk Management, risk assessments are performed annually across Oracle Cloud Infrastructure to identify threats and risks that could impact the security, confidentiality, or availability of the system. The risk assessment is modeled after National Institute of Standards and Technology (NIST) Special Publication 800-30 Rev. 1 guidelines and incorporates risk assessment requirements from the ISO/IEC 27001:2022 standard.

Risks are reviewed, assigned an owner, and remediated in line with the Oracle Cloud Infrastructure risk management assessment program. The results of internal audits, external audits, customer audits, and other compliance activities are collated and form inputs into Oracle Cloud Infrastructure's risk assessment process.

Monitoring

At least annually, Oracle Cloud Infrastructure completes an internal and external audit of the System. The internal audit is conducted by qualified auditors and as per the requirements set out in Clause 9 of ISO/IEC 27001:2022. Oracle Cloud Infrastructure evaluates and communicates internal control findings in a timely manner to those parties responsible for taking corrective action. Findings are reviewed and tracked through resolution. In addition, BA&A evaluates Oracle's operational controls for effectiveness and compliance with policy.



The Oracle Database@Azure service uses a subservice organization to support the physical and environmental components of the service. Oracle Cloud Infrastructure reviews in-scope data center, subservice organization, and PoP site's provider attestation reports or internationally recognized certifications, at least annually. Identified issues are evaluated and tracked.

Oracle designed control activities in its day-to-day operations to support the Oracle Cloud Infrastructure environment. The sections below describe different control activities in various processes within Oracle Cloud Infrastructure.

ATTACHMENT B – PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Overview

Oracle designs its processes and procedures to meet its objectives for the Oracle Cloud Infrastructure System. Those objectives are based on the service commitments that Oracle makes to user entities, the laws and regulations that govern the provision of the Oracle Cloud Infrastructure System, and the financial, operational and compliance requirements that Oracle has established for the services.

The Oracle Cloud Infrastructure services are subject to relevant regulations, as well as privacy security laws and regulations in the jurisdictions in which Oracle operates.

Security, Availability and Confidentiality commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided on the Oracle website. Security, Availability and Confidentiality commitments are standardized and include, but are not limited to, the following:

- Security and confidentiality principles inherent to the fundamental design of the Oracle Cloud Infrastructure System are intended to permit Oracle users to access the information and resources they need on the infrastructure supporting the system based on their role in the system while restricting them from accessing information not needed for their role.
- Security and confidentiality principles inherent to the fundamental design of the Oracle Cloud Infrastructure System are designed to prevent Oracle users from accessing user entity servers and storage once the instance has been provisioned.
- Availability principles inherent to the fundamental design of the Oracle Cloud Infrastructure System are designed to provide fault tolerance related to the infrastructure supporting the service and to isolate incidents to within a fault zone or availability domain.

Oracle Cloud Infrastructure establishes operational requirements that support the achievement of security, availability and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Oracle Cloud Infrastructure's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Oracle Cloud Infrastructure System.

The Oracle Cloud Infrastructure System is designed based on a shared responsibility model where both Oracle and the user entities (or "customers") are responsible for aspects of security, availability, and confidentiality. Details of the responsibilities of user entities can be found on the Oracle [website](#) and in the customer contract.