ORACLE

System and Organization Controls (SOC 1) Type 2 Report

Description of the Oracle Cloud Infrastructure System

For the Period January 1, 2025 to December 31, 2025

Prepared in Accordance with AICPA Attestation Standards and IAASB Standard ISAE No. 3402

TABLE OF CONTENTS

World Headquarters
2300 Oracle Way
Austin, TX 78741
Phone +1.737.867.1000
oracle.com

SECTION I – ORACLE CLOUD INFRASTRUCTURE'S MANAGEMENT ASSERTION

We have prepared the description of Oracle Cloud Infrastructure's system entitled "Description of the Oracle Cloud Infrastructure System" (Description), which consists of a description of the following services:

- Access Governance
- Account Tracking and Automation Tool
- Analytics Cloud
- Anomaly Detection
- API Gateway
- Application Dependency Management
- Application Performance Monitoring
- Archive Storage
- Artifact Registry
- Audit
- Autonomous AI Database on Dedicated Exadata Infrastructure (ADB-D)
- Autonomous AI Database on Exadata Cloud at Customer (ADB-C@C)
- Autonomous AI Database Serverless
- Base Database Service
- Bastion
- Big Data
- Billing and Cost Management
- Block Volume
- Blockchain Platform
- Budgets
- Certificates
- Client Logging
- Cloud Advisor
- Cloud Guard
- Cloud Incident Service
- Cloud Shell
- Compute
- Compute Cloud@Customer
- Connector Hub
- Console Announcements
- Container Instances
- Intelligent Advisor
- Inter-Region Latency
- Java Management
- Kubernetes Engine
- Language
- License Manager
- Load Balancer
- Log Analytics
- Logging
- Managed Access
- Managed Services for Mac
- Management Agent
- Marketplace - Consumer
- Media Services
- Monitoring
- MySQL Heatwave
- NetSuite Analytics Warehouse
- NetSuite Health Check
- Network Firewall
- Network Health Intelligence
- Network Load Balancer
- Network Path Analyzer
- Networking
- NoSQL Database
- Notifications
- Object Storage
- OCI Cache
- OCI Control Center
- OCI Database with PostgreSQL
- Operator Access Control
- Ops Insights
- Oracle AI Data Platform
- Oracle Clinical Control Plane

World Headquarters
2300 Oracle Way
Austin, TX 78741
Phone +1.737.867.1000
oracle.com

- Content Management
- Customer Feedback Service
- Data Catalog
- Data Flow
- Data Integration
- Data Labeling
- Data Lake
- Data Safe
- Data Science
- Database Autonomous Recovery
- 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@Customer (ExaDB-C@C)
- Exadata Database on Dedicated Infrastructure (ExaDB-D)
- Exadata Database Service on Exascale Infrastructure (ExaDB-XS)
- Exadata Fleet Update
- FastConnect
- File Storage
- Fleet Application Management
- Full Stack Disaster Recovery
- Functions
- Fusion Data Intelligence
- Fusion Applications Environment Management
- Generative AI
- Oracle Cloud Migrations
- Oracle Database@AWS
- Oracle Database Service for Azure
- Oracle Database@Azure
- Oracle Database@Google Cloud
- Oracle Ksplice
- Oracle Search Cloud
- OS Management Hub
- Process Automation
- Publisher
- Query Service
- Queue
- Raw Metal Cloud
- Registry
- Resource Manager
- Resource Scheduler
- Roving Edge Infrastructure
- Search
- Search with OpenSearch
- Secure Desktops
- Security Assurance System
- Security Zones
- Serverless Kubernetes
- Service Manager Proxy
- Service Mesh
- Site-to-Site VPN
- Speech
- Stack Monitoring
- Status
- Streaming
- Streaming with Apache Kafka
- Subscription Pricing Service
- Tagging
- Threat Intelligence
- Vault
- Vision
- Visual Builder
- Visual Builder Studio

World Headquarters
2300 Oracle Way
Austin, TX 78741
Phone +1.737.867.1000
oracle.com

- Generative AI Agents
- Globally Distributed Autonomous AI Database
- GoldenGate
- Health Checks
- Identity and Access Management
- Instance Security
- Integration
- VMWare Solution
- Vulnerability Scanning
- Web Application Acceleration
- Web Application Firewall
- WebLogic Management Service
- Zero Trust Packet Routing

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

Commercial Regions

- Australia East, Sydney, Australia
- Australia Southeast, Melbourne, Australia
- Brazil East, Sao Paulo, Brazil
- Brazil Southeast, Vinhedo, Brazil
- Canada Southeast, Montreal, Canada
- Canada Southeast, Toronto, Canada
- Chile Central, Santiago, Chile
- Chile West, Valparaiso, Chile
- Colombia Central, Bogota, Colombia
- France Central, Paris, France
- France South, Marseille, France
- Germany Central, Frankfurt am Main, Federal Republic of Germany
- India South, Hyderabad, India
- India West, Mumbai, India
- Ireland East, Dublin, Ireland
- Israel Central, Jerusalem, Israel
- Italy Northwest, Milan, Italy
- Japan Central, Osaka, Japan
- Japan East, Tokyo, Japan
- Mexico Central, Queretaro, Mexico
- Mexico Northeast, Monterrey, Mexico
- Netherlands Northwest, Amsterdam, Netherlands
- Saudi Arabia Central, Riyadh, Saudi Arabia
- Saudi Arabia West, Jeddah, Saudi Arabia
- Serbia Central, Jovanovac, Serbia
- Singapore, Singapore
- Singapore West, Singapore
- South Africa Central, Johannesburg, South Africa
- South Korea Central, Seoul, South Korea
- South Korea North, Chuncheon, South Korea
- Spain Central, Madrid, Spain
- Sweden Central, Stockholm, Sweden

World Headquarters
2300 Oracle Way
Austin, TX 78741
Phone +1.737.867.1000
oracle.com

- Switzerland North, Zurich, Switzerland
- UAE Central, Abu Dhabi, UAE
- UAE East, Dubai, UAE
- 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 Midwest, Des Moines, Iowa, United States
- United States South, Dallas, Texas, United States
- United States South Central, Abilene, Texas, United States
- United States West, Boardman, Oregon, United States
- United States West, Phoenix, Arizona, United States
- United States West, Salt Lake City, Utah, 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, Germany
- EU Sovereign South, Madrid, Spain

Multi-tenant Dedicated Regions

- Abu Dhabi, UAE 2 (RKT)
- Abu Dhabi, UAE 3 (AHU)
- Abu Dhabi, UAE 4 (SHJ)
- Al Ain, UAE (RBA)
- Chuncheon, South Korea 2 (BNO)
- Seoul, South Korea 2 (DTZ)
- Suwon, South Korea (DLN)

Dedicated Regions

- Ashburn, Virginia, United States 2 (YXJ)
- Chiyoda, Japan (NJA)
- Crissier, Switzerland (AVF)
- Doha, Qatar (DOH)
- Dublin, Ireland 1 (ORK)

World Headquarters
2300 Oracle Way
Austin, TX 78741
Phone +1.737.867.1000
oracle.com

- Dublin, Ireland 2 (SNN)
- Gazipur, Bangladesh (DAC)
- Ibaraki, Japan (UKB)
- Milan, Italy 1 (BGY)
- Milan, Italy 2 (MXP)
- Muscat, Oman (MCT)
- Ratingen, Germany 1 (DUS)
- Ratingen, Germany 2 (DTM)
- Zurich, Switzerland (AVZ)

Oracle Alloy

- Dubai, UAE 2 (ABR)
- Dubai, UAE 3 (PCZ)
- Hobsonville, Auckland, New Zealand (IZQ)
- Milan, Italy 2 (PBV)
- Osaka, Japan (UKY)
- Osaka, Japan 2 (IBG)
- Pathum Thani, Thailand (MEZ)
- Rome, Italy (NAP)
- Silverdale, Auckland, New Zealand (JJT)
- Tatebayashi, Japan (JBB)
- Tokyo, Japan (TYO)

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

- Bengaluru, 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") for cloud infrastructure services throughout the period January 1, 2025 to December 31, 2025 for user entities of the System during some or all of the period January 1, 2025 to December 31, 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Carved-out Unaffiliated Subservice Organization: Oracle Cloud Infrastructure uses subservice organizations to provide multi-cloud services and large language model services. The Description includes only the control objectives and related controls of Oracle Cloud Infrastructure and excludes the control objectives and related controls of the

World Headquarters
2300 Oracle Way
Austin, TX 78741
Phone +1.737.867.1000
oracle.com

subservice organizations. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The Description does not extend to controls of the subservice organizations.

Complementary User Entity Controls: The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Oracle Cloud Infrastructure's controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to controls of the user entities.

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

a. The Description fairly presents the System made available to user entities of the System during some or all of the period January 1, 2025 to December 31, 2025 for cloud infrastructure services as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:

(1) Presents how the System made available to user entities of the System was designed and implemented, including, if applicable:

- The types of services provided.
- The procedures, within both automated and manual systems, by which those services are provided for user entities of the System.
- The information used in the performance of the procedures and supporting information; this includes the correction of incorrect information and how information is transferred to the reports prepared for user entities.
- How the System captures and addresses significant events and conditions.
- The process used to prepare reports and other information for user entities.
- Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
- The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.
- Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

(2) Includes relevant details of changes to the System during the period covered by the Description.

(3) Does not omit or distort information relevant to the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors, and may not, therefore, include every aspect of the System that each individual user entity of the System and its user auditor may consider important in the user entity's own particular environment.

b. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period January 1, 2025 to December 31, 2025 to achieve those control objectives, if the subservice organizations applied the complementary subservice organization controls and user entities applied the complementary user entity controls assumed in the design of Oracle Cloud Infrastructure's controls throughout the period January 1, 2025 to December 31, 2025. The criteria we used in making this assertion were that

World Headquarters
2300 Oracle Way
Austin, TX 78741
Phone +1.737.867.1000
oracle.com

(1) The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the service organization.

(2) The controls identified in the Description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved.

(3) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Very truly yours,

Shape the future with confidence

Ernst & Young LLP
Suite 1600
560 Mission Street
San Francisco, CA
94105-2907

Tel: +1 415 894 8000
Fax: +1 415 894 8099

SECTION II – INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

To the Management of Oracle Cloud Infrastructure

Scope
We have examined Oracle Cloud Infrastructure's description entitled "Description of the Oracle Cloud Infrastructure System" (Description) throughout the period January 1, 2025 to December 31, 2025 which consists of the following services:

- Access Governance
- Account Tracking and Automation Tool
- Analytics Cloud
- Anomaly Detection
- API Gateway
- Application Dependency Management
- Application Performance Monitoring
- Archive Storage
- Artifact Registry
- Audit
- Autonomous AI Database on Dedicated Exadata Infrastructure (ADB-D)
- Autonomous AI Database on Exadata Cloud at Customer (ADB-C@C)
- Autonomous AI Database Serverless
- Base Database Service
- Bastion
- Big Data
- Billing and Cost Management
- Block Volume
- Blockchain Platform
- Budgets
- Certificates
- Client Logging
- Cloud Advisor
- Cloud Guard
- Cloud Incident Service
- Cloud Shell
- Compute
- Compute Cloud@Customer
- Connector Hub
- Intelligent Advisor
- Inter-Region Latency
- Java Management
- Kubernetes Engine
- Language
- License Manager
- Load Balancer
- Log Analytics
- Logging
- Managed Access
- Managed Services for Mac
- Management Agent
- Marketplace - Consumer
- Media Services
- Monitoring
- MySQL Heatwave
- NetSuite Analytics Warehouse
- NetSuite Health Check
- Network Firewall
- Network Health Intelligence
- Network Load Balancer
- Network Path Analyzer
- Networking
- NoSQL Database
- Notifications
- Object Storage
- OCI Cache
- OCI Control Center
- OCI Database with PostgreSQL
- Operator Access Control

- Console Announcements
- Container Instances
- Content Management
- Customer Feedback Service
- Data Catalog
- Data Flow
- Data Integration
- Data Labeling
- Data Lake
- Data Safe
- Data Science
- Database Autonomous Recovery
- 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@Customer (ExaDB-C@C)
- Exadata Database on Dedicated Infrastructure (ExaDB-D)
- Exadata Database Service on Exascale Infrastructure (ExaDB-XS)
- Exadata Fleet Update
- FastConnect
- File Storage
- Fleet Application Management
- Full Stack Disaster Recovery
- Functions
- Fusion Data Intelligence
- Fusion Applications Environment Management
- Ops Insights
- Oracle AI Data Platform
- Oracle Clinical Control Plane
- Oracle Cloud Migrations
- Oracle Database@AWS
- Oracle Database Service for Azure
- Oracle Database@Azure
- Oracle Database@Google Cloud
- Oracle Ksplice
- Oracle Search Cloud
- OS Management Hub
- Process Automation
- Publisher
- Query Service
- Queue
- Raw Metal Cloud
- Registry
- Resource Manager
- Resource Scheduler
- Roving Edge Infrastructure
- Search
- Search with OpenSearch
- Secure Desktops
- Security Assurance System
- Security Zones
- Serverless Kubernetes
- Service Manager Proxy
- Service Mesh
- Site-to-Site VPN
- Speech
- Stack Monitoring
- Status
- Streaming
- Streaming with Apache Kafka
- Subscription Pricing Service
- Tagging
- Threat Intelligence
- Vault
- Vision

- Generative AI
- Generative AI Agents
- Globally Distributed Autonomous AI Database
- GoldenGate
- Health Checks
- Identity and Access Management
- Instance Security
- Integration
- Visual Builder
- Visual Builder Studio
- VMWare Solution
- Vulnerability Scanning
- Web Application Acceleration
- Web Application Firewall
- WebLogic Management Service
- Zero Trust Packet Routing

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

Commercial Regions

- Australia East, Sydney, Australia
- Australia Southeast, Melbourne, Australia
- Brazil East, Sao Paulo, Brazil
- Brazil Southeast, Vinhedo, Brazil
- Canada Southeast, Montreal, Canada
- Canada Southeast, Toronto, Canada
- Chile Central, Santiago, Chile
- Chile West, Valparaiso, Chile
- Colombia Central, Bogota, Colombia
- France Central, Paris, France
- France South, Marseille, France
- Germany Central, Frankfurt am Main, Federal Republic of Germany
- India South, Hyderabad, India
- India West, Mumbai, India
- Ireland East, Dublin, Ireland
- Israel Central, Jerusalem, Israel
- Italy Northwest, Milan, Italy
- Japan Central, Osaka, Japan
- Japan East, Tokyo, Japan
- Mexico Central, Queretaro, Mexico
- Mexico Northeast, Monterrey, Mexico
- Netherlands Northwest, Amsterdam, Netherlands
- Saudi Arabia Central, Riyadh, Saudi Arabia
- Saudi Arabia West, Jeddah, Saudi Arabia
- Serbia Central, Jovanovac, Serbia
- Singapore, Singapore
- Singapore West, Singapore
- South Africa Central, Johannesburg, South Africa
- South Korea Central, Seoul, South Korea
- South Korea North, Chuncheon, South Korea
- Spain Central, Madrid, Spain

- Sweden Central, Stockholm, Sweden
- Switzerland North, Zurich, Switzerland
- UAE Central, Abu Dhabi, UAE
- UAE East, Dubai, UAE
- 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 Midwest, Des Moines, Iowa, United States
- United States South, Dallas, Texas, United States
- United States South Central, Abilene, Texas, United States
- United States West, Boardman, Oregon, United States
- United States West, Phoenix, Arizona, United States
- United States West, Salt Lake City, Utah, 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, Germany
- EU Sovereign South, Madrid, Spain

Multi-tenant Dedicated Regions

- Abu Dhabi, UAE 2 (RKT)
- Abu Dhabi, UAE 3 (AHU)
- Abu Dhabi, UAE 4 (SHJ)
- Al Ain, UAE (RBA)
- Chuncheon, South Korea 2 (BNO)
- Seoul, South Korea 2 (DTZ)
- Suwon, South Korea (DLN)

Dedicated Regions

- Ashburn, Virginia, United States 2 (YXJ)
- Chiyoda, Japan (NJA)
- Crissier, Switzerland (AVF)
- Doha, Qatar (DOH)
- Dublin, Ireland 1 (ORK)

- Dublin, Ireland 2 (SNN)
- Gazipur, Bangladesh (DAC)
- Ibaraki, Japan (UKB)
- Milan, Italy 1 (BGY)
- Milan, Italy 2 (MXP)
- Muscat, Oman (MCT)
- Ratingen, Germany 1 (DUS)
- Ratingen, Germany 2 (DTM)
- Zurich, Switzerland (AVZ)

Oracle Alloy

- Dubai, UAE 2 (ABR)
- Dubai, UAE 3 (PCZ)
- Hobsonville, Auckland, New Zealand (IZQ)
- Milan, Italy 2 (PBV)
- Osaka, Japan (UKY)
- Osaka, Japan 2 (IBG)
- Pathum Thani, Thailand (MEZ)
- Rome, Italy (NAP)
- Silverdale, Auckland, New Zealand (JJT)
- Tatebayashi, Japan (JBB)
- Tokyo, Japan (TYO)

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

- Bengaluru, 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") for providing cloud infrastructure services to user entities and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in "Oracle Cloud Infrastructure's Management Assertion" (Assertion). The Control Objectives and controls included in the Description are those that management of Oracle Cloud Infrastructure believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

Complementary user entity controls: The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of Oracle Cloud Infrastructure's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Carved-out Unaffiliated Subservice Organizations: Oracle Cloud Infrastructure uses Amazon Web Services (AWS) and Microsoft Azure to provide multi-cloud data center hosting services. Oracle Cloud Infrastructure also uses Google, OpenAI and xAI to provide large language model services. The Description includes only the Control Objectives and related controls of Oracle Cloud Infrastructure and excludes the control objectives and related controls of AWS, Microsoft Azure, Google, OpenAI and xAI (subservice organizations). The description also indicates that certain Control Objectives specified by Oracle Cloud Infrastructure can be achieved only if complementary subservice organization controls assumed in the design of Oracle Cloud Infrastructure's controls are suitably designed and operating effectively, along with the related controls at Oracle Cloud Infrastructure. Our examination did not extend to such complementary controls of AWS, Microsoft Azure, Google, OpenAI and xAI, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Other Information Provided by Service Organization: The information included in "Additional Information Provided by Oracle Cloud Infrastructure" is presented by management of Oracle Cloud Infrastructure to provide additional information and is not a part of Oracle Cloud Infrastructure's Description. Information about Oracle Cloud Infrastructure's Documentation, Security Practice, General Data Protection Regulation and Contracts and Policies has not been subjected to the procedures applied in our examination of the description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related Control Objectives, and accordingly we express no opinion on it.

Oracle Cloud Infrastructure's responsibilities

Oracle Cloud Infrastructure has provided the accompanying Assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives. Oracle Cloud Infrastructure is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the Control Objectives and stating them in the Description, identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related Control Objectives.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period January 1, 2025 to December 31, 2025. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related Control Objectives, based on the criteria in management's Assertion.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related Control Objectives.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved.
- Evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the Assertion.

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.

We are required to be independent of Oracle Cloud Infrastructure and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement 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.

We apply International Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services engagements*, which requires that we design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in providing cloud infrastructure services. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related Control Objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of tests *of* controls

The specific controls tested, and the nature, timing, and results of those tests are listed in the accompanying "Oracle Cloud Infrastructure Controls, Test Procedures and Results of Testing" (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the criteria described in Oracle Cloud Infrastructure's Assertion:

a. The Description fairly presents the System that was designed and implemented throughout the period January 1, 2025 to December 31, 2025.
b. The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period January 1, 2025 to December 31, 2025, and the subservice organizations and user entities applied the

complementary controls assumed in the design of Oracle Cloud Infrastructure's controls throughout the period January 1, 2025 to December 31, 2025.

c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period January 1, 2025 to December 31, 2025, if complementary subservice organizations and user entity controls assumed in the design of Oracle Cloud Infrastructure's controls operated effectively throughout the period January 1, 2025 to December 31, 2025.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of Oracle Cloud Infrastructure, user entities of Oracle Cloud Infrastructure's System during some or all of the period January 1, 2025 to December 31, 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

February 10, 2026

SECTION III – DESCRIPTION OF THE ORACLE CLOUD INFRASTRUCTURE SYSTEM

Oracle Overview

Oracle provides products and services that address enterprise information technology (IT) needs. 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-premises, cloud-based and hybrid deployments. It is an important element of Oracle's corporate strategy to provide choice and flexibility to Oracle customers as to when and how they deploy Oracle applications and infrastructure technologies. Oracle believes that offering customers broad, comprehensive, flexible, and interoperable deployment models for Oracle applications and infrastructure technologies is important to Oracle's growth strategy and addresses customer needs.

Oracle Cloud Services offers comprehensive and integrated applications and infrastructure services, enabling Oracle customers to choose the best option that meets their specific business needs. Oracle Cloud Services integrate IT components in a cloud-based IT environment that Oracle deploys and manages for customers and is accessible by 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 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-premises license deployment offerings include Oracle applications, Oracle Database and Middleware software offerings, among others, which customers deploy using IT infrastructure from the Oracle Cloud or their own 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.

Oracle customers include businesses of many sizes, government agencies, educational institutions, and resellers that Oracle markets and sells to directly through the Oracle worldwide sales force and indirectly through the Oracle Partner Network. Using Oracle technologies, customers build, deploy, run, manage and support their internal and external products, services and business operations.

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-premises 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 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 database (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.
- US Defense – Cloud regions for applications that require Impact Level 5 (IL5) data.
- UK Sovereign - Formerly known as Oracle Cloud for UK Government and Defence, a dedicated dual-region cloud for UK government and defence customers.
- Australian Government and Defence - Cloud region for the Australian government and defense.
- 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 offers 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
Ireland East (Dublin)	eu-dublin-3	Dublin, Ireland	ZQO	OC1	1 – from July 22, 2025
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
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 1	SIN	OC1	1
Singapore West (Singapore)	ap-singapore-2	Singapore, Singapore 2	XSP	OC1	1
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 1	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, Illinois, US	ORD	OC1	3
US Midwest (Des Moines)	us-desmoines-1	Des Moines, Iowa, US	KQQ	OC1	1 – from July 23, 2025
US South Central (Abilene)	us-abilene-1	Abilene, Texas, US	ABL	OC1	1 – from May 1, 2025
US South (Dallas)	us-dallas-1	Dallas, Texas, US	DFW	OC1	1 – from May 1, 2025
US West (Boardman)	us-boardman-1	Boardman, Oregon, US	NHJ	OC1	1 – from June 30, 2025
US West (Phoenix)	us-phoenix-1	Phoenix, Arizona, US	PHX	OC1	3
US West (Salt Lake)	us-saltlake-2	Salt Lake City, Utah, US	AGA	OC1	1
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 Defense 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
US DoD West (Phoenix)	us-gov-phoenix-1	Phoenix, Arizona, US	TUS	OC3	1

The following table lists the regions in the United Kingdom Sovereign 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 and Defence 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	Ibaraki, Japan	UKB	OC8
MCT Dedicated Region	me-dcc-muscat-1	Muscat, Oman	MCT	OC9
BGY Dedicated Region	eu-dcc-milan-1	Milan, Italy 1	BGY	OC14
MXP Dedicated Region	eu-dcc-milan-2	Milan, Italy 2	MXP	OC14
DTM Dedicated Region	eu-dcc-rating-2	Ratingen, Germany 2	DTM	OC14

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY
DUS Dedicated Region	eu-dcc-rating-1	Ratingen, Germany 1	DUS	OC14
ORK Dedicated Region	eu-dcc-dublin-1	Dublin, Ireland 1	ORK	OC14
SNN Dedicated Region	eu-dcc-dublin-2	Dublin, Ireland 2	SNN	OC14
DAC Dedicated Region	ap-dcc-gazipur-1	Gazipur, Bangladesh	DAC	OC15
DOH Dedicated Region	me-dcc-doha-1	Doha, Qatar	DOH	OC21
AVF Dedicated Region	eu-crissier-1	Crissier, Switzerland	AVF	OC24
AVZ Dedicated Region	eu-dcc-zurich-1	Zurich, Switzerland	AVZ	OC24
AHU Multi-Tenant Dedicated Region	me-abudhabi-3	Abu Dhabi, UAE 3	AHU	OC26
RBA Multi-Tenant Dedicated Region	me-alain-1	Al Ain, UAE	RBA	OC26
RKT Multi-Tenant Dedicated Region	me-abudhabi-2	Abu Dhabi, UAE 2	RKT	OC29
SHJ Multi-Tenant Dedicated Region	me-abudhabi-4	Abu Dhabi, UAE 4	SHJ	OC29
BNO Multi-Tenant Dedicated Region	ap-chuncheon-2	Chuncheon, South Korea	BNO	OC35
DTZ Multi-Tenant Dedicated Region	ap-seoul-2	Seoul, South Korea 2	DTZ	OC35
DLN Multi-Tenant Dedicated Region	ap-suwon-1	Suwon, South Korea	DLN	OC35
YXJ Multi-Tenant Dedicated Region	us-ashburn-2	Ashburn, Virginia, United States 2	YXJ	OC42 – from June 30, 2025

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
PBV Alloy Region	eu-milan-2	Milan, Italy 2	PBV	OC22 – from June 9, 2025
UKY Alloy Region	ap-dcc-osaka-1	Osaka, Japan	UKY	OC25
TYO Alloy Region	ap-dcc-tokyo-1	Tokyo, Japan	TYO	OC25
IZQ Alloy Region	ap-hobsonville-1	Hobsonville, Aukland, New Zealand	IZQ	OC31
JJT Alloy Region	ap-silverdale-1	Silverdale, Aukland, New Zealand	JJT	OC31
IBG Alloy Region	ap-osaka-2	Osaka, Japan 2	IBG	OC40 – from June 16, 2025

REGION NAME	REGION IDENTIFIER	REGION LOCATION	REGION KEY	REALM KEY
JBB Alloy Region	ap-tatebayashi-1	Tatebayashi, Japan	JBB	OC40 – from March 19, 2025
ABR Alloy Region	me-dubai-2	Dubai, United Arab Emirates 2	ABR	OC41 – from June 27, 2025
PCZ Alloy Region	me-dubai-3	Dubai, United Arab Emirates 3	PCZ	OC41 – from June 10, 2025
MEZ Alloy Region	ap-pathumthani-1	Pathum Thani, Thailand	MEZ	OC43 – from April 25, 2025

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 Services 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 and which may be relevant to a customer's or user entity's internal controls over financial reporting (ICFR).

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.

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, Kubernetes Engine, 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.

Billing and Cost Management

Billing and Cost 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.

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.

Connector Hub

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.

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 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.

Database

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

Autonomous AI Database on Dedicated Exadata Infrastructure (ADB-D)

Autonomous AI Database provides a fully autonomous database that scales elastically, delivers fast query performance, and requires no database administration. Autonomous AI 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 customers' 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 AI Lakehouse or Autonomous AI Transaction Processing.

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

Autonomous AI 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-premises 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 AI Database Serverless

Autonomous AI 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 AI 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

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 Remote Direct Memory Access (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.

Exadata Database Service on Exascale Infrastructure (ExaDB-XS)

Oracle Exadata Exascale further empowers Exadata to meet the most demanding corporate and cloud computing requirements by decoupling Oracle Database and Grid Infrastructure (GI) clusters from the underlying Exadata storage servers. Exascale software services can manage a large fleet of Exadata storage servers connected by the Exadata RDMA Network Fabric, providing storage services to multiple GI clusters and databases while enabling:

- Secure sharing of storage resources with strict data isolation, allowing different users and databases to share a large pool of storage while ensuring that data is inaccessible to users without the appropriate privileges;
- Flexible and dynamic storage provisioning for many users and databases;
- Increased storage utilization and efficiency while reducing storage costs; and
- Sharing of otherwise idle storage processing resources to improve performance.

Globally Distributed Autonomous AI Database

Oracle Globally Distributed Autonomous AI 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.

Below are the Oracle Multi-cloud database service offerings:

Oracle Database@AWS

Oracle Database@AWS is an Oracle Cloud database service that runs Oracle Database workloads in a customer's Amazon Web Services (AWS) environment. When a customer implements this solution, they deploy resources in two cloud environments: database resources are in AWS, while the database administration control plane is in Oracle Cloud Infrastructure. This allows them to deploy Oracle Database products in their AWS environment while Oracle Cloud Infrastructure maintains the administration capabilities. The customer AWS-based applications access Oracle Databases directly from within their AWS environment. Customers perform most database administrative operations in the AWS Console as well. Maintaining the database control plane in Oracle Cloud Infrastructure allows Oracle Database@AWS to be easily managed and upgraded with the latest operational and administrative capabilities. The service benefits from the simplicity, security, and low latency of a single operating environment within AWS. Oracle Database@AWS service documentation is also available in the AWS documentation at Oracle Database@AWS Overview. For additional information, please refer to the Complementary Subservice Organization Controls (CSOCs) section.

Oracle Database@Azure

Oracle Database@Azure is an Oracle Cloud Database service that runs Oracle Database workloads in a customer's Azure environment. All hardware for Oracle Database@Azure is collocated in Azure's data centers and uses Azure networking. The service benefits from the simplicity, security, and low latency of a single operating environment within Azure. Federated identity and access management for Oracle Database@Azure is provided by Microsoft Entra ID. Oracle Database@Azure documentation is also available in the Azure documentation at Oracle Database@Azure Overview. For additional information, please refer to the Complementary Subservice Organization Controls (CSOCs) section.

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 the Interconnect.

Oracle Database@Google Cloud

Oracle Database@Google Cloud is an Oracle Cloud Database service that runs Oracle Database workloads in a customer's Google Cloud environment. When the customer implements this solution, they deploy resources in two cloud environments: database resources are in Google Cloud, while the database administration control plane is in Oracle Cloud Infrastructure. This allows the customer to deploy Oracle Database products in their Google Cloud environment while Oracle Cloud Infrastructure maintains the administration capabilities. Google Cloud-based applications access Oracle Databases directly from within the customer's Google Cloud environment. The customer performs most database administrative operations in the Google Cloud Console as well. Maintaining the database control plan in Oracle Cloud Infrastructure allows Oracle Database@Goole Cloud be easily managed and upgraded with the latest operational and administrative capabilities. All hardware for Oracle

Database@Google Cloud uses Google Cloud networking. Oracle's responsibility for monitoring the data center control environments is included within the scope of the System. Oracle Database@Google Cloud uses Google's Identity and Access Management integration to manage user and group access for the customer's Oracle database resources. Google Cloud networking and Identity and Access Management are not within the scope of the System. Oracle Database@Google Cloud documentation is also available in the Google documentation at Oracle Database@Google Cloud Overview.

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 enable 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 AI 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 delivery

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 (i.e., Interconnect for Azure) and Google Cloud (i.e., Interconnect for Google Cloud).

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.

Fleet Application Management

Fleet Application Management provides centralized operations across the customer's entire cloud footprint—enabling IT automation, resource management, and patch compliance at scale for any technology deployed on OCI.

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 Data Intelligence

Fusion Data Intelligence provides analytics for Oracle Applications Cloud, powered by Autonomous AI Lakehouse and Oracle Analytics. The service extracts and loads data from Oracle Fusion Cloud Applications into an instance of Oracle Autonomous AI Lakehouse. 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.

Generative AI Agents

Generative AI Agents is a fully managed service that combines the power of large language models (LLMs) with AI technologies to create intelligent virtual agents that can provide personalized, context-aware, and highly engaging customer experiences.

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.

Kubernetes Engine

Kubernetes Engine 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.

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.

Log Analytics

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

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.

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.

Managed Services for Mac (from March 13, 2025)

Managed Services for Mac allows users to run macOS workloads in the Oracle Cloud, extending the flexibility, scalability, and cost benefits of Oracle Cloud Infrastructure to all Apple developers.

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 Data Intelligence 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 Health Intelligence (from May 2, 2025)

Network Health Intelligence is an Oracle internal service that monitors the physical devices of a network, auto-remediates specific failures, and alarms based on specified conditions.

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.

CIDR Notation

A compact method for specifying IP address ranges and network masks.

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

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

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 AI Database on Exadata Cloud@Customer, and Autonomous Exadata VM Cluster (client virtual machines deployed on Oracle Autonomous AI 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 AI Data Platform (from March 25, 2025)

Oracle AI Data Platform is an intelligent data platform with Gen AI tools that provides a single pane of glass for data management for data professionals in an organization using different data platform analytics workloads.

Oracle Clinical Control Plane

Oracle Clinical Control Plane is an Oracle internal service that supports end-to-end lifecycle management of the clinical environments provided to customers by Oracle Health.

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 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 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 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.

Query Service (from June 5, 2025)

Query Service enables customers to run interactive SQL queries over large datasets stored in Object Storage or Autonomous AI Lakehouse.

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.

Raw Metal Cloud (from April 25, 2025)

Raw Metal Cloud is an Oracle internal service that allows Oracle Cloud Infrastructure to manage and track data center related requests from internal and external customers. It enables Oracle Cloud Infrastructure to action on tasks such as hardware ingestion, hardware repairs, inventory management, network health and management, and post-repair workflows.

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.

Resource Scheduler

Resource Scheduler is a service that can reduce the cost of the customer's database and compute OCI cloud resources in a customer's tenancy, organization, realm, or other group of centrally managed tenancies by using a schedule to automatically stop them when they are not needed and restart them when they are needed again.

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.

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 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.

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 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.

Streaming with Apache Kafka

Streaming with Apache Kafka allows users to create and run Kafka clusters in an Oracle Cloud Infrastructure tenancy with all the functionalities of Apache Kafka.

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.

WebLogic Management Service (from June 17, 2025)

WebLogic Management provides a unified view to manage WebLogic Server instances deployed on OCI. Customers can perform lifecycle management operations, such as patching, starting, stopping, or restarting WebLogic domains running on compute instances.

Zero Trust Packet Routing

Zero Trust Packet Routing prevents unauthorized access to data by managing network security policies separately from the underlying network architecture. Using an easily understood and intent-based policy language, security administrators can define specific access pathways for data. Traffic that is not explicitly allowed by policy cannot travel the network, which improves security while simplifying the work of security, network, and audit teams.

Internal Services

The scope of this report includes controls that apply to Oracle internal services used by Oracle Cloud Infrastructure to support the System. These internal services are subject to the same applicable policies, procedures and controls described in this report which include Oracle Cloud Infrastructure common processes for access management and change management. Critical internal services include, but are not limited to, tools that support change management, access management, asset management, incident management, and metering and subscription services.

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 or 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 or Oracle's employees, facilities, business enterprise, and assets.
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.
Corporate Security Architecture	The Oracle corporate security architecture team 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 architecture team 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 website 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 Global Compliance training annually which includes information on corporate policies, information security, the process to report and respond to potential incidents, and other topics important to conducting business. The Oracle Global 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.

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 and policies including the Corporate Security Practices, Cloud Hosting and Delivery Policies, and Global Customer Support 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.

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@AWS and Oracle Database@Azure services use subservice organizations 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 to resolution. In the event that a site does not have an attestation report, or internationally recognized certification, Oracle Cloud Infrastructure performs an annual assessment of the site's control environment, including physical security controls and environmental safeguards.

Additionally, the Generative AI and Generative AI Agents services use subservice organizations to provide additional language models that a customer can opt to use. Oracle Cloud Infrastructure reviews subservice organization attestation reports or internationally recognized certifications at least annually, in accordance with the OCI Supplier Risk Management Standard. Identified issues are evaluated and tracked to resolution.

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.

Control Objectives and Related Control Activities

Control Objective 1: Administrative and Personnel Procedures

Controls provide reasonable assurance that Oracle Cloud Infrastructure hires and retains employees that are properly skilled and vetted.

Personnel Procedures

Human Resources (HR) is a corporate function at Oracle. The controls in this section apply to the global employee population, including Oracle Cloud Infrastructure employees. HR uses several corporate HR management systems for their operations, and HR procedures vary according to local laws, regulations, and Oracle policies. HR representatives are assigned to business areas within Oracle.

Hiring of new employees—traditional new hire or through a merger or acquisition—occurs using formal procedures that follow corporate directives and in-country regulations and processes. A manager, who needs a new employee, accesses a HR self-service application, creates the job requisition, and forwards it to the Recruitment team for review and approval in accordance with the local process.

Oracle advertises job postings for a minimum of two weeks, in accordance with local policy. Submitted résumés or curricula vitae (CVs) are assessed and qualified candidates are selected for interviews. The hiring manager and a recruiter, if requested by the manager, initially interview potential candidates. Then multiple interviewers, selected based on their experience, role, and subject matter expertise, speak with the candidate regarding qualifications.

After a candidate has been identified, Oracle initiates the offer process using a formal Global Approval Matrix (GAM) that indicates the level of approval required for offers and transfers based on the terms of the transaction (e.g., position, salary). The HR recruitment team maintains this GAM. Oracle HR systems are configured to automatically route requests based on the terms specified in the GAM.

After a candidate is selected for the job opening, the candidate's offer request is automatically routed using the GAM. On occasion, hiring approvals may also be obtained via e-mail in accordance with the GAM.

Oracle, or a third-party acting on behalf of Oracle, performs background checks on candidates selected for hire in accordance with local laws, regulations, and Oracle policies. Oracle's supplier agreements require the suppliers of contract personnel to perform background screening of non-direct Oracle workers (sub-contractors) to the extent permitted by local laws, regulations, and Oracle policies before assigning them to Oracle. In the event a non-direct worker is hired as a direct Oracle employee, Oracle will re-perform the same location-based background checks on the individual. A candidate's offer may be released contingent upon satisfactory completion of Oracle's pre-employment background check process.

After a candidate accepts the offer, local HR reviews the appropriate documents to ascertain an applicant's right to work, in accordance with local laws and regulations and policy. HR requires each new employee to complete and sign a core set of new hire forms for their location, such as an employment agreement or equivalent and Propriety Information Agreement, prior to or on the day of hire (or as otherwise required under applicable law), in accordance with local laws, regulations, and Oracle policies. Employees are assigned a job description upon hire that defines their role and the necessary qualifications for their position.

Oracle has developed an employee performance evaluation framework for use by its lines of business. Global Human Resources supports the performance management process by providing guidance and tools to help facilitate individual and team success. The performance management process largely covers goal setting, continuous feedback and conversations with management, and performance evaluations. This process seeks to define what Oracle employees are expected to do, how work goals can be accomplished and how these contribute to the strategic objectives of the organization.

Oracle uses a formal process for terminations. For voluntary terminations, the manager is responsible for ensuring the voluntary termination action is initiated after an employee initiated his or her resignation. HR manages involuntary terminations. HR systems process involuntary terminations and issue automated notifications based on the effective date of termination. The recipient list for the alert includes all necessary parties, such as the employee's manager and HR representative.

When an employee is terminated, Oracle HR updates the employee's status in the HR database and that data is then synchronized with the Oracle Identity Manager (OIM) and Oracle Cloud Infrastructure Permissions system using Oracle Corporate LDAP. OIM and Permissions use data attained from HR to revoke Oracle Cloud Infrastructure access for terminated personnel. When necessary, a person's access may be revoked in the OIM or Permissions system prior to HR processing their termination.

HR termination transactions are monitored quarterly to identify transactions where the termination date entered in the HR system is more than 14 days after the actual termination date. The risks associated with possible extended access are evaluated and risk mitigation performed, as needed. Documentation of review procedures and results are maintained in a secure Oracle repository.

Training

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 Global Compliance training annually which includes information on corporate policies, information security, the process to report and respond to potential incidents, and other topics important to conducting business. The Oracle Global 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.

Additionally, employees with access to source code are required to complete secure code training prior to obtaining access or on an annual basis. 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.

Control Objective 2: Logical Access (Supporting Infrastructure)

Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users.

The Logical Access Controls Policy and Cloud Compliance Standard for Access Control describe logical access control requirements for all Oracle systems, including authentication, authorization, access approval, provisioning and revocation for employees and any other Oracle-defined users with access to Oracle systems which are not internet-facing, publicly accessible systems. Specifically, access to the infrastructure and services supporting the System requires multi-factor authentication, a VPN connection, and an SSH connection with a user account and password/private key.

Oracle Cloud Network Access

The Oracle Cloud Network architecture consists of a multi-tiered demilitarized zone (DMZ) environment inside a dedicated extranet. It is isolated from Oracle's internal corporate network and inaccessible via VPNs for non-cloud services. The Oracle Cloud Network comprises a gateway subnet, tools subnet, and network subnet located in Oracle's DMZ, and it is protected by firewalls.

The first step in the authentication path is the Oracle Cloud Network Access (OCNA) VPN. OCNA functions as a secure access gateway between the user and the target device. OCNA has redundant gateways in various geographies worldwide.

- Authentication – Only approved users with a valid OCNA account in OIM can access OCNA, and they must use two-factor authentication.
- Authorization – User attributes describe the specific entitlements the user has to access resources. These attributes are defined at the time of user account creation or modified later (e.g., added by an appropriate entitlement approver, removed upon termination). The user's access is restricted according to these attributes.
- Posture Check – OCNA performs a security posture check to determine whether the user's endpoint is running up-to-date software including anti-malware software and compliance monitoring tools validating endpoint encryption, has a local firewall enabled, and is in line with Oracle policies regarding software updates before permitting the endpoint to authenticate to the VPN. The VPN is configured to time out after 24 hours of connectivity.

Bastion Server Authentication

The second step in the authentication path is authenticating to the relevant bastion server. Operator access is permitted from bastion servers only, and the bastion servers are permitted to accept connections from OCNA subnets. Access to bastion severs is controlled in two ways, and users must meet both prerequisites to authenticate to a bastion server.

- Entitlement – Only approved engineers with the required entitlement can access the bastion servers. Entitlements are provisioned using the Permissions access management system, are approved by the entitlement owner prior to access being granted, and access is reviewed on a quarterly basis.
- SSH Key – Authorized users provide their public/private SSH key in conjunction with their Linux usernames and authenticate via Lightweight Directory Access Protocol (LDAP). The user's private key is stored on a virtual slot on the user's token, which requires two-factor authentication to access. The user's corresponding public key is configured on the appropriate bastion servers during the access provisioning process.

Access to Individual Devices

Once a user has authenticated to the relevant bastion server, they can connect to an individual device if they have the corresponding Permissions or OIM entitlement for the device. The Permissions and OIM access management systems manage access to the entitlements and groups, including the code integration tools. Access to entitlements and groups must be approved prior to access being granted and an expiration date is required for temporary access requests. User access is reviewed on a quarterly basis and inappropriate access identified during the review is investigated and revoked. In addition to having the group entitlement for network devices, operators must also enter a one-time password (OTP) that expires after 24 hours. Devices supporting Windows and Mac operating systems (OS) are configured to lock automatically after 15 minutes of inactivity.

Access to hosts is provisioned using a SSH public/private key pairing. Oracle Cloud Infrastructure keys and secrets are managed securely via the Vault service.

Access Governed by Permissions

Access to the infrastructure supporting the System, where access is managed by Permissions, is broken up into different layers by Resources, Roles and Groups. A Resource is a representation that defines the downstream entity being controlled by Permissions, such as host class. Each Resource belongs to a specific Service and has predefined access levels, such as read or write. A Role is a collection of Resources with the associated access level for each Resource. A Group is a collection of users that can be granted access to a Role, allowing those users to inherit access to the Resources via the assigned Role.

Permissions is configured to enforce Service Owners and Group Owners to perform quarterly user access reviews to validate that the access to the Services, Groups, and Resources is appropriate based on each user's job role and least privilege principle. If a Service, Resource, or Group is not reviewed by the quarterly deadline, the access is automatically disabled until a review is completed. Issues identified during the review are investigated and remediated. If access is marked for removal, Permissions automatically revokes the access when the review is submitted.

Access Governed by OIM

Access to the infrastructure supporting the System, where access is managed by OIM, is defined by Accounts and Entitlements. An Account is a specific application or asset, and each Account has a subset of Entitlements. An Entitlement is a collection of permissions which allows a user to perform a certain function within an application or asset. Users can be assigned to Entitlements.

On a quarterly basis, Management reviews the users assigned to Entitlements that provide access to the infrastructure supporting the System to validate that access is appropriate based on the user's job role and least privilege principle. If access is marked for removal, OIM automatically revokes the access when the review is submitted.

Oracle Operator Access Control

Customers that have regulatory requirements to audit and control all aspects of their system management, including infrastructure components, may choose to use the Oracle Operator Access Control. This is especially true of Oracle's enterprise customers that are highly regulated and run their most critical systems, their most security-sensitive applications on Oracle. As described previously in Service Descriptions, Oracle Operator Access Control enables customers to grant, audit, and revoke the access Oracle has to their Exadata Infrastructure. Customers utilizing Oracle Operator Access Control are in control of when and how much access Oracle operators have to the Exadata infrastructure. Unless an explicit customer approval is

received, Oracle operators do not have remote shell access to the Exadata infrastructure. Commands and keystrokes executed by Oracle operators are logged. Approved access is automatically revoked when the access duration expires or can be revoked at the customer's discretion. For further details, refer to the Oracle Operator Access Control Configuration and Administration Guide. Refer to Section IV for the control testing that is not in scope for the Exadata Infrastructure with Oracle Operator Access Control service.

System Logs and Intrusion Detection

Authentication logs for assets supporting the System are forwarded to a Security Information and Event Monitoring (SIEM) tool where logs are retained for at least 90 days. Access to the log repository is restricted to approved personnel.

In addition to authentication logs, Oracle Cloud Infrastructure deploys a host intrusion detection system (HIDS) that monitors and detects security events, a network intrusion detection system (NIDS) on the edge to monitor production traffic and detect security events, anti-virus (AV) to detect malware, and file integrity monitoring (FIM) to monitor unauthorized modification of critical system files, configuration files, or content files. Logs from this suite of security controls are sent to the log aggregation tool.

The SIEM tool creates a ticket if suspicious activity is detected. The ticket is updated throughout the investigation and escalated for additional investigation as required.

Control Objective 3: Logical Security (Customer Tenancies)

Controls provide reasonable assurance that logical access to customer tenancies is restricted to users authorized and specified by the customer.

Customer Access to the System

Customers can manage Oracle Cloud Infrastructure resources using the Console (a browser-based interface), the REST API, or through various Java and Ruby Software Development Kits (SDKs). Each of these interfaces, and each of the services offered through them, integrates with the IAM service for authentication and authorization. The IAM service references groups, compartments, and policies defined by the customer's administrator to control which users at their organization can access which services, which resources, and the type of access.

Console

To access the Console, including the customer administration console, the Oracle Alloy operator console, and the Multi-tenant DRCC operator console, the user must use a supported browser and connect using HTTPS and TLS 1.2 or above. If a user attempts to make a connection over a non-secure connection (e.g., HTTP or SSL), the request is denied. During the signup process, the customer receives a customized URL to access the console for their organization. If a user connects using the base URL, they are prompted to specify the relevant tenant (e.g., Company ABC) on the sign-in page in addition to their username and password.

API

Oracle Cloud Infrastructure APIs are typical REST-based and use HTTPS requests and responses. Oracle Cloud Infrastructure API requests require support for HTTPS and TLS 1.2 or above.

Audit Service

Oracle Cloud Infrastructure Audit service automatically records calls to all supported Oracle Cloud Infrastructure public API endpoints as log events. Currently, all services support logging by Audit. Object Storage service support logging for bucket-related events, but not for object-related events. Log events recorded by the Audit service include API calls made by the Oracle Cloud Infrastructure Console, Command Line Interface (CLI), SDK, the customer's custom clients, or other Oracle Cloud Infrastructure services. Information in the logs shows what time API activity occurred, the source of the activity, the target of the activity, what the action was, and what the response was. By default, logs are retained for at least 90 days and cannot be deleted by customers. Customers may request an export of their logs by contacting Oracle.

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API). An administrator in the customer's organization needs to set up groups, compartments

and policies that control which users can access which services, which resources they can access, and the type of access they have. For example, the policies control who can create new users, create, and manage the cloud network, launch instances, create buckets, download objects, etc.

Creating a New Instance

To create a new instance, the customer chooses a bare metal or VM instance from an Oracle-provided image or a custom image. Refer to the Initial Access Restrictions section below for additional details.

Key Pairs

Instances launched using Oracle Cloud Infrastructure-provided Linux images use an SSH key pair instead of a password to authenticate a remote user. A key pair consists of a private key and public key. The customer retains the private key on its computer and provide the public key every time it launches an instance. The customer can have as many key pairs as needed or use one key pair for all or several instances.

Initial Access Restrictions

Each Oracle Cloud Infrastructure-provided Linux image is configured with a default user account. If a user attempts to authenticate with the root account, they receive a message informing them to re-authenticate using the default username. The image only accepts key-based authentication requests via SSH on port 22. Password-based SSH is disabled.

Each Oracle Cloud Infrastructure-provided Windows image is configured without a default administrator account. A user initially authenticates using a password generated during the provisioning process and provided to the user through the console. The system forces the user to change the password the first time they authenticate to the instance. Oracle-provided Windows images initially accept connections using the remote desktop protocol (RDP) only. Administrators can configure their VCN to accept connections over RDP to enable users to connect to the compute instance from outside the VCN.

Oracle-provided images contain default IP tables that restrict access to the instance. However, except for Fusion customers, the customer is responsible for all aspects of the server's management and security. The Fusion Applications Environment Management service manages all aspects of the server's management and security for Fusion customers.

Customer Security Lists

A security list provides a virtual firewall for an instance, with ingress and egress rules that specify the types of traffic allowed in and out. Each security list is enforced at the instance level. However, customers can configure security lists at the subnet level, which results in all instances in each subnet being subject to the same set of rules. The security lists apply to a given instance whether it is communicating with another instance in the VCN or a host outside the VCN.

Each subnet can have multiple security lists associated with it. A particular packet is allowed if any rule in the security lists allows the traffic (or if the traffic is part of an existing connection being tracked).

Access to a VCN is controlled via a combination of security lists and routing tables. When a customer creates a VCN, they have the option to use a default routing table and security list or to configure the security list and routing tables to meet their specific requirements. A customer may also provision a VCN with the default ruleset and subsequently configure the ruleset in line with their requirements.

Access to customer Fusion environments is controlled by network access control lists on the Fusion environment which are configured by the customer. Customer load balancers are configured by the Oracle Cloud Infrastructure Fusion Applications Environment Management team based on customer-provided network access control lists, also referred to as network security lists. Fusion Applications Environment Management maintains the infrastructure security lists and changes to the infrastructure security list rules follow the standard Oracle Cloud Infrastructure change management process.

Fusion Applications Environment Management Break Glass

Fusion customers who elect for additional Oracle support can employ the Fusion Applications Environment Management break glass functionality. For Fusion customers utilizing the break glass functionality, credentials to access the Fusion Applications Environment Management generic administrator accounts are distributed through the Oracle Managed Access

service based on the approval settings configured by customers. The credentials will expire and will be automatically changed at the end of the approved duration or upon customer-initiated revocation.

Control Objective 4: Change Management

Controls provide reasonable assurance that changes are implemented to services supporting the System after they are documented and reviewed in line with the Change Management requirements and provide reasonable assurance that changes are tested prior to implementation.

Documentation

Oracle Cloud Compliance Standard for Change Management is documented and shared with relevant internal stakeholders. Additionally, Oracle Cloud Infrastructure maintains a documented change management process that outlines the types of changes and actions required based on the change type. Oracle Cloud Infrastructure has four different change types:

- Normal change: change with minimal customer impact, negligible blast radius, and minimal security risk.
- Routine change: change that is done regularly, with little to no difference between deployments and do not have significant risks or blast radius.
- Emergency change: change that must be executed immediately, during a period where work is restricted or has sufficient impact that it requires additional review and visibility.
- Mitigating change: change that is for resolving an active or recent incident.

Changes to infrastructure configurations and services supporting the System are documented in an electronic, access-controlled ticketing system. A workflow and mandatory fields are implemented in the ticketing system to help ensure compliance with the change management requirements. The mandatory fields require a description of:

- The nature of the proposed change
- The impacted systems (direct and indirect)
- The impact of the change
- Required updates to system documentation after the change
- The test plan(s)
- The internal and external notification plan (if necessary)
- The rollback plan
- The post-implementation verification process

The workflow prevents the ticket from being moved into the scheduled or implementation phase without the required review and approval of child tickets being in the closed state.

Source Code Management

The source code management tool for services supporting the System is configured to store current and prior versions of source code to support rollback to prior versions. Write access to the source code management tool is restricted to approved personnel.

In addition, access to the source code repositories is approved prior to access provisioning. Users with access to the source code repositories and the code deployment tool are reviewed quarterly. Issues identified during the review are investigated and remediated.

Change Management Review and Approvals

The documented change management process includes review and approval requirements for different types of changes.

Changes to infrastructure configurations and services supporting the System must be reviewed and approved prior to implementation to production. A member of the same team with knowledge of the impacted service, who can technically review the change for accuracy and potential issues, typically acts as the reviewer. The ticketing system is configured to prevent the reviewer from being the same person as the ticket author. Additionally, the code repositories that are configured to require peer reviews, enforce that an appropriate person other than the developer to peer review and approve each individual commit prior to the change being implemented to the production branch.

Further, emergency and mitigating changes to infrastructure configurations and services supporting the System require approvals from a Senior Manager or above. Additional approvals can be required based on the change's risk assessment. Once the underlying commits and change ticket have obtained the required approvals, the change can be deployed to production.

Segregation of Duties

Oracle Cloud Infrastructure achieves segregation of duties by ensuring that the development of the change and at least one approval is performed by separate and appropriate personnel. Additionally, a systematic process conducts change implementation.

Changes to infrastructure configurations and services supporting the System that are developed and promoted through a source code management tool are peer reviewed prior to implementation to production. The peer reviewer is different from the author of the change.

Additionally, Oracle Cloud Infrastructure performs an annual review of the source code management tools to validate that the tools are configured to require an approval from someone other than the person that developed the change before a change can be merged to a production related source code repository. Issues identified during the review are investigated and tracked to resolution.

Change Management Testing

Changes to infrastructure configurations and services supporting the System must be tested prior to implementation. The type of test is dependent on the nature of the change but may include unit, regression, manual, and/or integration tests. The development and testing environment are separated from the production environment to reduce the risks of unauthorized access or changes to the operational environment.

Change Implementation Process

Code changes are implemented through Continuous Integration/Continuous Deployment (CICD) tools. Except where dependencies exist across multiple availability domains (e.g., updates to domain name services), changes are implemented separately in each region and availability domain.

Server Configuration

Each Oracle Cloud Infrastructure service team is responsible for building and managing the fleet of servers used to deliver each service. Except for hypervisors, servers supporting services are built from a standard image that includes the configuration management tool client. Detailed build procedures and server hardening guidelines are made available to relevant personnel. The configuration management tools configure the servers in line with the service's applicable configurations, which are stored in an access-controlled code repository and changes are subject to the change management process. The configuration management tools verify, at regular intervals, that the server's configuration is consistent with the service's applicable configurations. If a discrepancy is identified, the server configuration management tools are configured to automatically revert unauthorized changes back to the master configuration. Write and admin access to the server configurations code repository is restricted to approved personnel.

Hypervisors are built from a standard image which does not include a configuration management tool client. Oracle Cloud Infrastructure monitors changes to the configuration and creates a ticket for investigation and correction when a hypervisor is not configured with the standard configuration.

For Exadata Database on Cloud@Customer, the Database as a Service (DBaaS) team is responsible for building and managing the fleet of servers hosted at the customer's data center used to deliver the service. These servers are built from a base image which does not include a configuration management tool client. Detailed build procedures and server hardening guidelines are made available to relevant personnel. Server configurations are stored in an access-controlled code repository and changes are subject to the change management process. Oracle Cloud Infrastructure maintains prior versions of the server configurations in the code repository to enable rollback.

File Integrity

File integrity monitoring (FIM) tools alert personnel to unauthorized modification of critical system files, configuration files, or content files on the infrastructure supporting the System. Logs are sent to the log aggregation tool which will create a ticket

if suspicious activity is detected. The ticket is updated throughout the investigation and escalated for additional investigation as required.

Control Objective 5: Incident Management

Controls provide reasonable assurance that incidents impacting the security and integrity of the infrastructure supporting the System are recorded, investigated, and tracked to closure.

Incident Recording

Incidents, including incidents reported directly to a customer's account manager, are recorded via an internal access-controlled electronic ticketing system. Oracle Cloud Infrastructure routes, communicates, and escalates incidents depending on factors including urgency and impact to customers. The procedures for external users to report an incident to Oracle is outlined on the Oracle website. To engage Oracle regarding a security incident, external users can log a Service Request (SR) with Oracle Customer Support.

Incidents reported via MOS or through the external user incident reporting process are routed to Oracle Cloud Infrastructure personnel and tracked in the electronic ticketing system in the same manner as an internally identified incident.

Severity Definitions

Incident severity levels help define the appropriate response, escalation requirements, customer messaging requirements, and internal communication of the severity. Oracle Cloud Infrastructure has four internal severity levels and four customer severity levels.

The table below outlines the four internal severity levels.

SEVERITY	IMPACT	DEFINITION
SEV1	Any Tier 0/1 Service down at an AD or greater level	Production down or major malfunction that results in a product-inoperative condition. Customers/Services are unable to perform their normal functions. The specific functionality is mission-critical to the business.
SEV2	Service down or degraded	Loss of functionality or performance resulting in services/customers being unable to perform their normal functions. Major feature/service failure; inconvenient workaround or no workaround exists. The service is usable but severely limited.
SEV3	Actionable event where there is no direct impact	An issue that is blocking another team/customer or needs to be addressed quickly to prevent a more serious problem, such that it should be the highest team priority after SEV 1 or SEV 2 incidents and should be actively worked during business hours until resolved.
SEV4	Informational or operational tasks	These items are operational tasks, or they can also be tasks that after they've been triaged become backlog items that should be closed once the item is tracked in the backlog as a task or work item.

The table below outlines the four customer severity levels, in accordance with the Oracle Cloud Hosting and Delivery Policies.

SEVERITY	IMPACT	DEFINITION
Severity 1	Critical Outage	Complete loss of service.
Severity 2	Significant Impairment	Severe loss of service. Important features are unavailable with no acceptable workaround.
Severity 3	Technical Issue	Minor loss of service. The impact is an inconvenience, which may require a workaround to restore functionality.
Severity 4	General Guidance	No loss of service. Request for information, enhancement, or documentation clarification, but there is no impact on the operation of the service.

Incident Resolution

Once incidents are assigned a severity rating, they are tracked to resolution. Incident resolution service level agreements are defined according to the Oracle Cloud Hosting and Delivery Policies located on the Oracle website.

Security Incidents

Security incidents are assigned a severity rating and tracked to resolution by the Oracle Cloud Infrastructure Security Operations team. Oracle Cloud Infrastructure reports confirmed security incidents with customer impact to Oracle GIS and Oracle Legal, who are responsible for any notices or disclosures to the public, customers, affected individuals, or law enforcement authorities. The Security Incident Management Policy and OCI Security Incident Response Standard specify the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including, as applicable, notification of affected customers. This policy and standard also outline the responsibilities of each team during the process.

Escalations

Technical Operations Support Incident Management (TOS:IM) and the Security Operations team have documented procedures that outline the process for handling each category of incident, including escalation to senior personnel who may be required to resolve and manage the incident. Oracle Cloud Infrastructure operates a paging system to contact appropriate staff in the event an incident requires their support.

Corrective Action/Preventative Action Process

Oracle Cloud Infrastructure has a comprehensive incident follow-up and reporting procedure for SEV 1 incidents that meet the Corrective Action/Preventative Action (CAPA) review requirements. The CAPA process involves the identification of the root cause of the incident and the documentation of follow-up actions and “lessons learned” to prevent recurrence. CAPAs are documented in an electronic ticketing system and mandatory fields include incident start and resolution time, root cause of the incident, steps taken to mitigate and/or resolve the incident, expected impact, and preventive actions.

Performance and Capacity Monitoring

Oracle Cloud Infrastructure uses an in-house telemetry and monitoring system to collect, process, and report metrics, logs, and notifications for the services. This system operates on servers and network devices supporting the System to provide visibility into the health, utilization, and performance of the services system.

The telemetry and monitoring system can monitor a wide variety of metrics, including file system capacity, CPU utilization, network latency, average memory usage, and network traffic. Each service team is responsible for designing a monitoring regime appropriate for the service. Raw metrics can be captured every few seconds or milliseconds. The telemetry and monitoring system ingests the raw data and aggregates it into per-minute digests, which contain a minute of data points in a compact representation. Metrics can be queried at defined time roll-ups called granularities (e.g., 60, 300, or 3600 seconds).

In addition to specifying which metrics are monitored, each service team is responsible for deciding the appropriate thresholds at which the monitoring system will alert. The monitoring system can compute the aggregations for values between 60 seconds and one day and set alerts based on statistical functions, such as average, sum, minimum, maximum, standard deviation, percentile, and sample count.

Alerting is configured at the service level. A triggered alert is sent to the appropriate service team queue, and either TOS:IM or the on-call engineer for that service team will be the initial respondent for the relevant service. In addition, the monitoring system automatically generates a ticket when thresholds are exceeded for monitored events that could significantly impact system availability. Oracle Cloud Infrastructure escalates these tickets according to the incident management process.

Control Objective 6: Availability, Physical Security and Environmental Safeguards

Controls provide reasonable assurance that infrastructure supporting the System and customer tenancies is available, protected against physical and environmental threats, and physical access is restricted to authorized individuals.

Data Backup

For autonomous AI database services, database backups are configured by Oracle by default and performed automatically. Depending on the database service model, data is retained in-line with the schedule configured either by Oracle by default or by the customer. For all other database services, database backups are performed and retained in-line with the schedule configured by customers.

Fusion Applications Environment Management databases are configured to be backed up weekly by the Oracle Infrastructure Cloud Fusion Applications Environment Management team. Data backups are retained for 60 days by default. Backup failures are monitored and resolved timely. Fusion Applications Environment Management backup data restoration testing is performed monthly to ascertain that the data can be retrieved when necessary.

Physical Security and Environmental Safeguards

Oracle Cloud Infrastructure contracts with third-party data center co-location vendors to provide dedicated data halls and suites for the use of the Oracle Cloud Infrastructure. The data halls within each data center are for the exclusive use of Oracle Cloud Infrastructure, and the sole purpose of each data center is that of a co-location vendor. The term data hall refers to any physically segregated and secured computer room housing Oracle Cloud Infrastructure equipment, including equipment used to host customer data. Segregation refers to physical barriers, such as solid walls or metal security caged areas. The term data center throughout this section refers to both data centers housing availability domains and points of presence (PoP) sites.

Dedicated Region Cloud@Customer and Oracle Alloy is Oracle Cloud Infrastructure deployed in a customer's own data center. Physical and environmental safeguards are a shared responsibility between the customer and Oracle Cloud Infrastructure. The customer can either contract with a data center provider directly or use a data center provider contracted by Oracle Cloud Infrastructure. If the customer contracts with a data center provider directly, the physical security and environmental safeguards are the customer's responsibility. Please see further information in section Complementary User Entity Controls.

Data Center Assessment Program

The Oracle Cloud Infrastructure Data Center Services (DCS) Program Management, Audit, Security, and Safety (PASS) team performs an assessment of data center and PoP site control environments, including physical security controls, environmental safeguards, and media destruction, prior to the data center hosting production traffic (go-live) and then thereafter in accordance with the schedule defined in the Data Center Assessment Program. Identified issues are evaluated and tracked through resolution.

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

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

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

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

Controls assessed as part of the Data Center Assessment Program are outlined in the sections below.

Preventive Maintenance

Each data center operates a preventive maintenance program to reduce the risk of a failure of environmental safeguards. The program includes the servicing of air handling units, fire suppression and detection equipment, uninterruptable power supply

(UPS), battery arrays, and generators on a predefined basis by competent professionals who are qualified to complete the maintenance. In addition to routine servicing, generators are turned on and run for a defined period at regular intervals to meet local environmental regulations.

Redundant Power Supplies

Critical mechanical and electrical components supporting Oracle data halls and suites at each facility are designed with N+1, N+2, and occasionally 2N redundancy. Each data center is served by multiple connections to the power grid and are connected to redundant power feeds. In addition, infrastructure within Oracle data halls is connected to an UPS and generator. Generators have a minimum of 24-hour supply of fuel and can carry the entire data center load.

Emergency backup power is used in Oracle Cloud Infrastructure data halls in the event of power loss. Backup power provides time for an orderly shutdown of systems or transition to alternate power source. Emergency power shut off capabilities are available for Oracle Cloud Infrastructure data halls. The devices are protected against accidental or unauthorized access but easily accessible for authorized personnel. Emergency lighting automatically activates in Oracle Cloud Infrastructure data halls if power is disrupted.

Fire Detection and Suppression

The data center building must be a permanent construction type, including concrete, brick, and/or steel as the fundamental structure. Each data center has an advanced fire suppression and smoke detection system in operation throughout the facility and within the Oracle data halls, that automatically trigger alarms upon event. The fire suppression system has both an extinguishing system and an automatic water sprinkler system. Suppression and detection devices are supported by an independent energy source. Fire extinguishers are located throughout the data center.

Fire doors throughout each facility are alarmed and can only be opened from the inside. The fire doors are fitted with push bars to open from the inside. When a fire door is opened, either an audible alarm sounds, or an alert is generated in the operations center.

Heating, Ventilation, and Air Conditioning

Data center mechanical systems are in line with American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) requirements. Airflow is monitored for temperature and humidity tolerances at all data centers. Oracle data halls maintain a consistent temperature during normal conditions and during incidents where there is a loss of utility power or loss of a single computer room air conditioner (CRAC). During outages, the infrastructure can carry the heat load until the emergency system comes online and the cooling system is restarted. CRAC systems are connected to generators.

Building Management System

A building management system (BMS) is in place at each data center for mechanical, electrical, and plumbing management and monitoring. The BMS monitors the temperature across the data hall and on each individual CRAC unit, where applicable. The BMS also monitors the humidity level and water detectors. If the humidity or temperature is above or below the predefined levels, or water is detected, an alarm/notification is triggered. The BMS is also connected to generators for activation in the event of a power outage.

Physical and Environmental Protection

Vehicle barriers and gates protect the entrances to each facility. Formal access procedures exist to allow vehicular and pedestrian access to the facilities. The security staff who work at each facility are instructed not to reveal that Oracle Cloud Infrastructure is housed at the site. Each facility has a security operation center manned on a 24x7 basis by physical security staff. The lobby of each facility is staffed by a security guard and access to the facility requires each person to pass through a mantrap or similar physical access control mechanism.

CCTV cameras are in operation both inside and outside each facility. The positioning of the cameras is designed to cover strategic areas, including the perimeter, the doors to the building, delivery/loading bays, and the entry point to each computer room from public circulation spaces. Monitors for the CCTV cameras are in the control room(s). The CCTV records are stored for a period of up to 90 days.

All facilities operate in line with applicable local and national regulatory requirements for environment, health, and safety, including written emergency response plans, emergency contact notification, personal protective equipment (PPE), chemical spill kits, and hazard communication/warning signage. Food and drink are prohibited in the data center raised floor areas.

Cables, equipment, and infrastructure in the data centers is secured in overhead cable trays, under a raised floor, or in a secured cage to prevent accidental or deliberate tampering.

Access Procedures and Reviews

Oracle Cloud Infrastructure restricts facility access to approved personnel based on job function. Requests for permanent access to a data center or PoP are approved prior to access being provisioned. When a user with permanent data center or PoP access is terminated, their access to the data center or PoP is revoked within 14 days of termination. Users with permanent access to data halls at each facility are reviewed at least quarterly. Issues identified during the review are investigated and remediated.

All Oracle Cloud Infrastructure guests to a facility must have a pre-approved access request. Requests are documented in the electronic ticketing system and must include the region, availability domain, name of the visitor/guest as it appears on a government ID, company the individual works for, contact information, duration of access, and business justification for access. All requests are approved by the relevant Oracle Cloud Infrastructure prior to access being granted. Visitors are required to show government-issued ID and be always escorted by an Oracle Cloud Infrastructure employee with permanent access to the facility. Visitors are provided with a visitor badge, which does not enable them to access any non-public areas of the facility.

Access to Oracle Cloud Infrastructure data halls requires two-factor authentication. Each user must present a valid access card along with a biometric fingerprint, hand scan, or retina scan. An alert in the operations center is triggered if the door to an Oracle data hall is left open for a predefined period. The access control systems are contained in the control room(s).

Complementary Subservice Organization Controls (CSOCs)

Oracle Cloud Infrastructure uses multiple subservice organizations to perform various services as described below.

Oracle Database@AWS uses a subservice organization, AWS, to support the physical and environmental components of the service. All infrastructure for Oracle Database@AWS is co-located in AWS's physical data centers and uses Amazon Virtual Private Cloud for networking, and Amazon Simple Storage Service (S3) for backups, managed within the AWS environment. Identity and access management for Oracle Database@AWS is provided by AWS Identity and Access Management. Amazon Virtual Private Cloud, AWS Identity and Access Management and Amazon Simple Storage Service (S3) are not within the scope of the System.

Oracle Database@Azure 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.

Generative AI and Generative AI Agents use subservice organizations, Google, OpenAI and xAI, to provide language model services. By leveraging Generative AI and Generative AI Agents, customers can choose to utilize Google, OpenAI and xAI owned models. Generative AI is responsible for connecting to the Google, OpenAI and xAI endpoints. The Google, OpenAI and xAI endpoints and models are not within the scope of the System.

The Oracle Cloud Infrastructure System covers only a portion of the overall internal control environment. It is not feasible for the control objectives related to the System to be achieved solely by Oracle Cloud Infrastructure. To achieve certain control objectives, the applicable controls specified below must be operating effectively at the subservice organizations, AWS, Google, Microsoft Azure, OpenAI, and xAI.

CSOC NUMBER	CONTROL ACTIVITY EXPECTED TO BE IMPLEMENTED BY SUBSERVICE ORGANIZATIONS	CONTROL OBJECTIVE	APPLICABLE SERVICE
CSOC-001	Google, OpenAI and xAI are responsible for restricting logical access to their own endpoints and systems to authorized personnel including secure authentication mechanisms, access authorization and revocation policies, and periodic user access reviews.	Control Objective 2	Generative AI; Generative AI Agents
CSOC-002	AWS and Microsoft Azure are responsible for restricting physical access to the data center to authorized employees, vendors, contractors, and visitors.	Control Objective 6	Oracle Database@AWS; Oracle Database@Azure
CSOC-003	AWS and Microsoft Azure are responsible for implementing security verification and check-in for personnel requiring temporary access to the interior of the data center facility, including tour groups or visitors.	Control Objective 6	Oracle Database@AWS; Oracle Database@Azure
CSOC-004	AWS and Microsoft Azure are responsible for reviewing and verifying physical access to the data center quarterly.	Control Objective 6	Oracle Database@AWS; Oracle Database@Azure
CSOC-005	AWS and Microsoft Azure are responsible for implementing physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) to restrict access to authorized individuals.	Control Objective 6	Oracle Database@AWS; Oracle Database@Azure
CSOC-006	AWS and Microsoft Azure are responsible for monitoring the data center facility 24x7 by security personnel.	Control Objective 6	Oracle Database@AWS; Oracle Database@Azure
CSOC-007	Google, OpenAI and xAI are responsible for maintaining robust security of their own endpoints and systems to prevent and detect unauthorized access including encryption, antimalware, denial of service, and vulnerability management mechanisms.	Control Objective 3	Generative AI; Generative AI Agents
CSOC-008	Google, OpenAI and xAI are responsible for maintaining the capacity and availability of the endpoints and systems supporting the models, and are responsible for reporting availability incidents to Oracle, including downtimes impacting the System.	Control Objective 6	Generative AI; Generative AI Agents
CSOC-009	AWS and Microsoft Azure are responsible for maintaining and testing data center-managed environmental equipment within the facility.	Control Objective 6	Oracle Database@AWS; Oracle Database@Azure
CSOC-010	AWS and Microsoft Azure are responsible for implementing environmental controls to protect systems inside data center facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.	Control Objective 6	Oracle Database@AWS; Oracle Database@Azure

CSOC NUMBER	CONTROL ACTIVITY EXPECTED TO BE IMPLEMENTED BY SUBSERVICE ORGANIZATIONS	CONTROL OBJECTIVE	APPLICABLE SERVICE
CSOC-011	AWS, Google, Microsoft Azure, OpenAI, and xAI are responsible for maintaining incident response procedures and reporting security incidents impacting the System to Oracle. The incident response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.	Control Objective 6	Oracle Database@AWS; Oracle Database@Azure; Generative AI; Generative AI Agents
CSOC-012	Google, OpenAI and xAI are responsible for configuring zero data retention on all systems processing or transmitting data so that data cannot be stored after processing is complete.	Control Objective 3	Generative AI; Generative AI Agents

Complementary User Entity Controls (CUECs)

Cloud security is a shared responsibility between a cloud service provider and its customers. Oracle Cloud Infrastructure controls were designed with the assumption that certain controls would be implemented by user entities (or "customers"). This section describes additional controls that customers must have in operation to complement the controls of Oracle Cloud Infrastructure to achieve certain control objectives. The list of customer control considerations presented below and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by customers. Customers may be required to implement additional administrative or technical controls to meet their business and legal needs.

CUEC NUMBER	CUEC DESCRIPTION	CONTROL OBJECTIVE	APPLICABLE SERVICES
CUEC-001	Customers are responsible for securely configuring firewall rules and ACLs relevant to their own environment.	Control Objective 2 Control Objective 3	All, except Fusion Applications Environment Management
CUEC-002	Customers are responsible for securely configuring network ACLs relevant to their own environment.	Control Objective 2 Control Objective 3	Fusion Applications Environment Management
CUEC-003	Customers are responsible for generating certificates that are shared with Oracle for communications between the customer owned tenancy and OCI owned tenancy.	Control Objective 2 Control Objective 3	Security Assurance System
CUEC-004	Customers are responsible for defining groups, roles, and responsibilities for management of network components in their environment.	Control Objective 2 Control Objective 3 Control Objective 5	All, except Fusion Applications Environment Management

CUEC NUMBER	CUEC DESCRIPTION	CONTROL OBJECTIVE	APPLICABLE SERVICES
CUEC-005	Customers are responsible for appropriately safeguarding crypto keys that they own, manage, and maintain, including securing the repository where cryptographic keys are stored or archived. If customers opt to export keys from the hardware security module, they are responsible for securing the keys and discarding the keys from local memory to protect the key contents.	Control Objective 3	All, except Fusion Applications Environment Management
CUEC-006	If customers choose to Bring Your Own Keys (BYOK) to Oracle Cloud Infrastructure, they are responsible for key ownership, configuration, encryption, and rotation.	Control Objective 3	All
CUEC-007	Customers are responsible for configuring in-transit encryption for Block Volume, File Storage, Object Storage and Boot Volume traffic for VM instances.	Control Objective 3	All, except Fusion Applications Environment Management
CUEC-008	Customers are responsible for configuring in-transit encryption for their own on-premises environment.	Control Objective 3	Exadata Database on Cloud@Customer (ExaDB-C@C); Compute Cloud@Customer
CUEC-009	Customers are responsible for configuring their respective systems and networks to log events according to their own requirements and implementing measures to review and monitor activities.	Control Objective 3	All, except Fusion Applications Environment Management
CUEC-010	Customers are responsible for configuring, managing, patching and maintenance of operating systems, databases, applications, and other components within their environment in line with their requirements and policies.	Control Objective 3	All, except Fusion Applications Environment Management, Autonomous AI Database services, and Serverless services as described in Section III
CUEC-011	Customers are responsible for defining, implementing, and enforcing identity and access management policies and procedures (including provisioning, reviewing, and revoking user access) with respect to their Console, API, SDK, VCN, applications and workloads, if applicable. Systems should be restricted to their own authorized users.	Control Objective 3	All
CUEC-012	Customers are responsible for designing, implementing, and maintaining interconnectivity between their resources on Oracle Cloud Infrastructure and resources elsewhere, if applicable.	Control Objective 3	All
CUEC-013	Customers are responsible for designing, implementing, operating, and maintaining their VCN in accordance with their policies and procedures for firewall rules, network segmentation, ACLs, load balancing, routing, and encryption of data in transit relevant to their own environment.	Control Objective 3	All, except Fusion Applications Environment Management
CUEC-014	Customers are responsible for enforcing multifactor authentication with respect to their environment.	Control Objective 3	Exadata Database on Cloud@Customer (ExaDB-C@C)

CUEC NUMBER	CUEC DESCRIPTION	CONTROL OBJECTIVE	APPLICABLE SERVICES
CUEC-015	Customers are responsible for ensuring their security credentials such as passwords, SSH keys, and secrets, if applicable, are kept confidential.	Control Objective 3	All
CUEC-016	Customers are responsible for installing, configuring, and maintaining firewall software on laptop and desktop computers within their own environment.	Control Objective 3	Exadata Database on Cloud@Customer (ExaDB-C@C)
CUEC-017	Customers are responsible for not removing "root" rules from Oracle provided images since all Oracle provided images include rules that allow only "root" on Linux instances to make outgoing connections to the iSCSI network endpoints (169.254.0.2:3260, 169.254.2.0/ 24:3260) that serve the instance's boot and block volumes. If the rules are removed, non-root users will have access to the instance's boot disk volume. Customers are responsible for ensuring that these rules are not deleted and are included in all customer images. It is the customer's responsibility to consider and mitigate against the potential security implications of modifying these rules.	Control Objective 3	All, except Fusion Applications Environment Management
CUEC-018	Customers are responsible for properly implementing and using Oracle Cloud Infrastructure Vault to encrypt data in accordance with their own policies and industry and applicable regulatory compliance requirements.	Control Objective 3	All, except Fusion Applications Environment Management
CUEC-019	Customers are responsible for reviewing audit logs of interactions with the API performed by their users.	Control Objective 3	All
CUEC-020	Customers are responsible for securely configuring Exadata instances as well as other systems running in their own environment.	Control Objective 3	Exadata Database on Cloud@Customer (ExaDB-C@C)
CUEC-021	Customers are responsible for selecting their desired MySQL configuration, VCN, and subnet to place their MySQL endpoint. To enable access from their client hosts, customers are responsible for setting the security rules to allow only from the trusted sources.	Control Objective 3	MySQL Heatwave
CUEC-022	Customers utilizing the break glass functionality are responsible for setting up approval templates for their resources in line with their company policies.	Control Objective 3	Fusion Applications Environment Management
CUEC-023	Customers utilizing the Operator Access Control service are responsible for managing Oracle access to the Exadata infrastructure and approving remote shell access if required.	Control Objective 3	Operator Access Control
CUEC-024	The Oracle Alloy partner is responsible for provisioning Windows images and the removal of the default Administrator account, restricting authentication to Remote Desktop Protocol (RDP) and the enforcement of password management policies and procedures.	Control Objective 3	Oracle Alloy
CUEC-025	Customers are responsible for managing the database including data schema and encryption keys.	Control Objective 3 Control Objective 6	Exadata Database on Cloud@Customer (ExaDB-C@C)
CUEC-026	Customers are responsible for developing configuration standards for Exadata instances as well as other system components running in their own environment.	Control Objective 4	Exadata Database on Cloud@Customer (ExaDB-C@C)

CUEC NUMBER	CUEC DESCRIPTION	CONTROL OBJECTIVE	APPLICABLE SERVICES
CUEC-027	Customers are responsible for securely connecting Compute Cloud@Customer racks in their data centers to their network.	Control Objective 4	Compute Cloud@Customer
CUEC-028	Customers are responsible for reviewing Oracle Cloud Infrastructure release notes and other notices of changes; evaluating changes; and, if necessary, taking steps to mitigate the effects of any changes.	Control Objective 4	All
CUEC-029	While Oracle is responsible for the base OS and hardware, customers are responsible for the Guest VM OS, Grid Infrastructure, and the database software maintenance.	Control Objective 4	Exadata Database on Cloud@Customer (ExaDB-C@C)
CUEC-030	Customers are responsible for informing Oracle of potential incidents in their environment.	Control Objective 5	All
CUEC-031	Customers are responsible for notifying Oracle of any unauthorized use of, and other known or suspected breach of security related to their applications and workloads.	Control Objective 5	All
CUEC-032	Customers are responsible for reviewing incident response details and security alerts provided by Oracle and initiating inquiry or follow-up as appropriate.	Control Objective 5	All
CUEC-033	Customers are responsible for authorizing, designing, developing or acquiring, implementing, maintaining, and monitoring environmental protections.	Control Objective 6	Exadata Database on Cloud@Customer (ExaDB-C@C); Compute Cloud@Customer; Security Assurance System DTC; Dedicated Regions (except NJA and UKB); Oracle Alloy regions
CUEC-034	Customers are responsible for designing and implementing a backup and/or replication process in line with their requirements and policies, including scheduling and configuring database backups manually and performing snapshots as needed.	Control Objective 6	All, except Fusion Applications Environment Management, NoSQL Database, Autonomous AI Database services, and Serverless services as described in Section III
CUEC-035	Customers are responsible for designing, developing, and implementing procedures for recovering their applications in accordance with their own recovery plans and periodically testing such plans to help meet availability commitments and requirements of their customers.	Control Objective 6	All, except Fusion Applications Environment Management
CUEC-036	Customers are responsible for implementing denial of service (DoS) mitigation and other network filtering processes to protect their systems appropriately.	Control Objective 6	All, except Fusion Applications Environment Management

CUEC NUMBER	CUEC DESCRIPTION	CONTROL OBJECTIVE	APPLICABLE SERVICES
CUEC-037	Customers are responsible for managing data within their environment according to the customers' company policies and procedures, including data handling, backup frequency, retention, and discovery of sensitive data and personal data within the customers' tenancies.	Control Objective 6	All
CUEC-038	Customers are responsible for monitoring their systems' availability and performance.	Control Objective 6	All, except Fusion Applications Environment Management
CUEC-039	Customers are responsible for performing data restoration testing to ascertain data retrievability.	Control Objective 6	All, except Fusion Applications Environment Management
CUEC-040	Customers are responsible for the following: • Restrict physical access to facilities (including sensitive areas and data centers) and protected information assets to authorized personnel. • Discontinue physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet their business needs. • Restrict the physical transmission, movement, and removal of information to authorized internal and external users and processes, and protect it during transmission, movement, or removal.	Control Objective 6	Exadata Database on Cloud@Customer (ExaDB-C@C); Compute Cloud@Customer; Security Assurance System DTC; Dedicated Regions (except NJA and UKB); Oracle Alloy regions (except TYO)
CUEC-041	Customers are responsible for ensuring that their data is exported from Oracle Cloud Infrastructure before expiry of contractual relationship with Oracle or within a reasonable amount of time after contract termination.	Control Objective 6	All

SECTION IV – ORACLE CLOUD INFRASTRUCTURE CONTROLS, TEST PROCEDURES, AND RESULTS OF TESTING

Description of Objectives, Controls, Tests, and Results of Testing

On the pages that follow, the control objectives and the controls designed to achieve the objectives have been specified by and are the responsibility of Oracle. The Testing Performed and Results of Testing are the responsibility of the service auditor. Unless specifically documented by the caption “Results of Testing” in the column titled “Results of Testing”, no deviations resulted from testing.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity

For tests of controls requiring the use of information provided by the entity (IPE) (e.g., controls requiring system-generated populations for sample-based testing), we perform a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management’s use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspect management’s procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Oracle Operator Access Control - Impacted Controls

Due to agreements between Oracle Cloud Infrastructure and their Exadata Cloud@Customer customers utilizing the Oracle Operator Access Control service, Oracle Cloud Infrastructure does not have access to the customer's Exadata Infrastructure without the customer’s approval, which may put limitations on the service auditor’s ability to perform certain test procedures. As such, Exadata Cloud@Customer Infrastructure with Oracle Operator Access Control is out of scope for the impacted controls and associated test attributes denoted with * below.

Refer to the "Oracle Operator Access Control" within Section III for further details.

Control Objective 1 – Administrative and Personnel Procedures

Controls provide reasonable assurance that Oracle Cloud Infrastructure hires and retains employees that are properly skilled and vetted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-01.01: Oracle performs background checks on candidates for hire in accordance with local laws and regulations as well as local Oracle policy.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the background check documentation for a sample of new hires selected from the HR system and ascertained the background checks were completed in accordance with local laws and regulations as well as local Oracle policy.	No deviations noted.
OCI-01.02: Employees are required to complete the Ethics and Business Conduct, Information Protection Awareness, and the Anti-Corruption and Foreign Corrupt Practices Act online courses upon hire. New hires who do not complete these courses in the allotted time frames are tracked and followed up by the Oracle Global Training Team.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the course records for a sample of new employees selected from the HR system and ascertained the new employees had completed the Ethics and Business Conduct, Information Protection Awareness, and Anti-Corruption & Foreign Corrupt Practices Act online e-courses or were tracked and followed up by the Oracle Global Training Team.	No deviations noted.
OCI-01.03: Employees are required to complete Global Compliance Training annually, which covers security awareness and how to report incidents. Employees who do not complete training in the allotted time frame are tracked and followed up by the Oracle Global Training Team.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the Information Security Policy and ascertained it specified the requirement for employees and contractors to complete security awareness training.	No deviations noted.
	Inspected the Global Compliance Training material and ascertained it outlined the process and procedures to report incidents.	No deviations noted.
	Inspected the Global Compliance Training completion date in the Oracle learning tool for a sample of employees and contingent workers selected from the HR system and ascertained the employees completed the training in the past year or were tracked and followed up by the Oracle Global Training Team.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-01.04: Employees are assigned a job description upon hire that defines their role and the necessary qualifications for their position.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the job description for a sample of new employees selected from the HR system and ascertained a job description existed which defined their role and the necessary qualifications for their position.	No deviations noted.

Control Objective 2 – Logical Access (Supporting Infrastructure)

Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-02.01: Access to the infrastructure and services supporting the System requires multi-factor authentication, a VPN connection, and an SSH connection with a user account and password/private key.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the Authentication Policy configuration and ascertained access to the infrastructure and services supporting the System were configured to require multi-factor authentication.	No deviations noted.
	Observed a user connect to the OCNA VPN and ascertained they were required to use multi-factor authentication.	No deviations noted.
	Inspected the configuration set on the configuration management tool for servers supporting the services and ascertained servers were configured to use SSH protocol for authentication and access was restricted to users with appropriate resource or group entitlements.	No deviations noted.
	Observed a user with appropriate access to a server attempt to SSH to a sample server without first connecting to a bastion server in the same region and ascertained the connection was unsuccessful. Alternatively, observed a user with appropriate access to a server attempt to SSH to a sample server from a bastion server in the same region and ascertained the connection was successful. Additionally, observed a user without appropriate access to a server attempt to connect to a sample server from a bastion server in the same region and ascertained the connection was unsuccessful.	No deviations noted.
	Inspected the bastion configuration for a sample of bastions selected from the asset tool and ascertained they were configured to only accept traffic from OCNA subnets.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Observed a user with appropriate access to a bastion attempt to SSH to a bastion server while connected to the OCNA VPN and ascertained the connection was successful when the SSH private key of the public/private key pair was provided to the server. Additionally, observed a user with appropriate access to a bastion attempt to SSH to a sample bastion server without connecting to the OCNA VPN and ascertained the connection was unsuccessful.	No deviations noted.
	Inspected the authentication configuration for a sample of network devices selected from the asset tool and ascertained they were configured to use the RADIUS protocol for authentication and access was restricted to users with the appropriate role.	No deviations noted.
	Observed a user attempt to connect to a sample network device without first connecting to the regional bastion server and ascertained the connection was unsuccessful. Additionally, observed a user attempt to connect to a sample network device while first connecting to the regional bastion server and ascertained the connection was successful.	No deviations noted.
OCI-02.02.A: Access to user groups and resources are approved in the access management systems prior to access provisioning. An expiration date is required for temporary access requests.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the permissions tool configuration and ascertained it was configured to require two approvals from either a user's manager, Service owner, or group owner prior to a user being added to a role/group or a group being added to a role.	No deviations noted.
	Observed an approved user authenticate into a group and role and ascertained the user was automatically provisioned access to the respective group and role after receiving approval. Additionally, observed an unapproved user attempt to authenticate into a group and role and ascertained the user was unable to access the respective group or role without appropriate approval.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Inspected the permissions tool configuration and ascertained temporary access to a role was configured to expire based on the approved duration.	No deviations noted.
	Observed a user within a current temporarily approved group successfully authenticate to a resource and inspected a report from the permissions tool and ascertained the temporary access was automatically removed within three days or less. Alternatively, observed a user with temporary access to a resource and inspected a report from the permissions tool and ascertained the temporary access was automatically removed within three days or less.	No deviations noted.
	Inspected the permissions tool configuration and ascertained temporary access to a group was configured to expire on a specific expiration date.	No deviations noted.
	Observed an expired temporarily approved user authenticate into a group and attempt to authenticate into the same group after the assigned expiration date and ascertained temporary access was automatically removed by the expiration date.	No deviations noted.
	Observed a user with the correct role and a user without the correct resource attempt to authenticate to the below asset types and ascertained only the user with the correct resource could authenticate to the below asset type: • Bastion Server • SmartNIC card • Load Balancer • Hypervisor • ILOM • Network Device • Server	No deviations noted.
	Inspected the permissions tool configuration and ascertained Just-in-time access to a role was configured to expire on a specific expiration time/date.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Observed an approved user successfully authenticate to a Just-in-time role and ascertained the Just-in-time access was automatically removed once the time limit was met. Additionally, observed an unapproved user attempt to authenticate into a Just-in-time role and ascertained the user was unable to access the respective role without appropriate approval.	No deviations noted.
	Inspected the permissions tool configuration and ascertained that access to resources was only granted through roles.	No deviations noted.
	Inspected the permissions tool configuration and ascertained that OCI synchronizes with the corporate LDAP, generating an email alert in the event of any changes to the reporting structure.	No deviations noted.
	Inspected the root account configuration on server hosts and ascertained that root access would not bypass the Permissions tool.	No deviations noted.
OCI-02.02.B: Access to the source code repositories is approved prior to access provisioning.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the approval documentation for a sample of users with write access to the source code repository and ascertained their access was approved prior to access being provisioned.	No deviations noted.
	Inspected the approval documentation for a sample of users with write access to the source code repository and ascertained the approver was appropriate based on job function.	No deviations noted.
	Observed users with and without approved access to the source code repository attempt to access the source code repository and ascertained the ability to access the source code repository was restricted to approved users.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-02.03: User access is revoked within 14 days of termination.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the configurations set on the permissions tool and VPN tool and ascertained user access to the permissions tool and user VPN access were automatically revoked within 14 days of termination.	No deviations noted.
	Inspected the access and termination details for a sample user and ascertained their access was revoked within 14 days of termination.	No deviations noted.
OCI-02.04: Users with access to the infrastructure and services supporting the System and source code repositories are reviewed quarterly. Issues identified during the review are investigated and remediated.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the permissions tool configuration and ascertained it was configured to inform group, service, and resource owners of the review requirement every quarter.	No deviations noted.
	Inspected the permissions tool configuration and ascertained it was configured to automatically revoke the access of users who were identified for access revocation during the quarterly review and to automatically revoke the access of users who had not been re-approved during the access review.	No deviations noted.
	Observed an owner of a group and service perform a user access review and mark a user for removal and ascertained the user was automatically notified and removed from the respective group and service.	No deviations noted.
	Inspected a group or service that was not reviewed by the quarterly deadline and ascertained access was automatically disabled to the group or service.	No deviations noted.
	Inspected the permissions tool configuration and ascertained it was configured to prevent a reviewer from completing a review two quarters in a row.	No deviations noted.
	Inspected the permissions tool configuration and ascertained it was configured to populate permissions with the list of users for groups, services, and resources.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Inquired of a sample of owners with access to perform user access reviews and ascertained they had the appropriate authority and were sufficiently competent to perform the review.	No deviations noted.
	Inspected the quarterly access review performed for users with write access to the Exadata Database on Cloud at Customer (ExaDB-C@C) service for a sample of quarters and ascertained the appropriateness of users was verified and approved, with any change or removal actions executed, if applicable.	No deviations noted.
OCI-02.05: Users with access to the code deployment tool supporting the System are reviewed quarterly. Issues identified during the review are investigated and remediated.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Observed the group or service that allows privileged access to the code deployment tool and ascertained the group or service was reviewed within the period and was managed via the permissions tool.	No deviations noted.
	Observed a user with and without appropriate permissions to the code deployment tool attempt to deploy a change and ascertained the ability to deploy a change via the tool was restricted to users with appropriate permissions.	No deviations noted.
OCI-02.06: Authentication logs for servers supporting services, hypervisors, and bastion hosts are forwarded to a Security Information and Event Monitoring (SIEM) tool, which is configured to store logs for at least 90 days. Access to the log repository is restricted to approved personnel. ** Refer to section "Oracle Operator Access Control - Impacted Controls" for additional information.*	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the configuration set on the configuration management tool for servers supporting services and bastion servers and ascertained it was configured to forward logs, including authentication logs, to the SIEM tool.	No deviations noted.
	Inspected the configuration for a sample of hypervisors selected from the asset tool and ascertained it was configured to forward logs, including authentication logs, to the SIEM tool.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Observed an engineer login to the below asset types and inspected the SIEM tool and ascertained the device was sending authentication events to the log repository: • Server • Bastion Server • Hypervisor	No deviations noted.
	Inspected the logging configuration for servers supporting the Exadata Database on Cloud at Customer (ExaDB-C@C) service and ascertained they were configured to forward logs, including authentication logs, to the centralized log repository in the associated availability domain.	No deviations noted.
	Observed an engineer login to a server supporting the Exadata Database on Cloud at Customer (ExaDB-C@C) service and the centralized log repository, inspected the server and centralized log repository and ascertained the server was sending authentication events to the log repository.	No deviations noted.
	Inspected the retention period configuration for the SIEM tool in the code repository and ascertained it was configured to retain data for 90 days.	No deviations noted.
	Inspected the permissions tool and ascertained it was configured to control access to the log repository.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-02.07: Dynamic Access Policies are configured to validate the following on endpoints prior to granting access to the infrastructure supporting the System: 1) devices are running up-to-date software including anti-malware software and compliance monitoring tools validating endpoint encryption, and 2) a local firewall is installed. The VPN is configured to time out after 24 hours of connectivity. Devices supporting Windows and Mac Operating Systems are configured to lock automatically after 15 minutes of inactivity.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the Dynamic Access Policies for OCNA and ascertained it was configured to check if endpoints were running up-to-date software, including anti-malware software, encryption monitoring software, and had a local firewall installed prior to granting access to the infrastructure supporting the System.	No deviations noted.
	Observed an employee attempt to connect to OCNA from a mobile device and ascertained the connection was unsuccessful as the device did not meet the requirements of a configured Dynamic Access Policies.	No deviations noted.
	Inspected the VPN configuration and ascertained the VPN was configured to time out after 24 hours.	No deviations noted.
	Inspected sample endpoints supporting Windows and Mac Operating Systems and ascertained it was configured to lock automatically after 15 minutes of inactivity.	No deviations noted.
OCI-11.19: The Logical Access Controls Policy and Cloud Compliance Standard for Access Control describe logical access control requirements for all Oracle systems, including authentication, authorization, access approval, provisioning and revocation for employees and any other Oracle-defined users with access to Oracle systems which are not internet-facing, publicly accessible systems.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the Logical Access Controls Policy and Cloud Compliance Standard for Access Control and ascertained it described logical access control requirements for Oracle systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle defined users with access to Oracle systems which were not Internet-facing, publicly accessible systems.	No deviations noted.

Control Objective 3 – Logical Security (Customer Tenancies)

Controls provide reasonable assurance that logical access to customer tenancies is restricted to users authorized and specified by the customer.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-03.01: Authentication logs for Oracle's Integrated Lights Out Management (ILOM), SmartNIC and Network Devices are forwarded to a Security Information and Event Monitoring (SIEM) tool, which is configured to store logs for at least 90 days. Access to the log repository is restricted to approved personnel.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the configuration for the automated host provisioning/deprovisioning process and ascertained it was configured to enable authentication logs on ILOMs and SmartNICs and to forward the logs to the SIEM tool during the host provisioning process.	No deviations noted.
	Inspected the logging configuration for Network Devices and ascertained it was configured to enable authentication logs on Network Devices to forward the logs to the SIEM tool.	No deviations noted.
	Inspected the configuration for a sample of the below asset types selected from the asset tool and ascertained the devices were configured to forward logs, including authentication logs, to the SIEM tool: • ILOM • SmartNIC card • Network Device	No deviations noted.
	Observed an engineer login to the below asset types, inspected the SIEM tool and ascertained the devices were sending authentication events to the log repository: • ILOM • SmartNIC card • Network Device	No deviations noted.
	Observed an engineer login to a log forwarding host, inspected the SIEM tool and ascertained the host was sending authentication events to the log repository.	No deviations noted.
	Inspected the retention period configuration for the SIEM tool in the code repository and ascertained it was configured to retain data for 90 days.	No deviations noted.
	Inspected the permissions tool and ascertained it was configured to control access to the log repository.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-03.02: Customer API calls, including actions from the customer administration console, are logged and retained for at least 90 days and cannot be deleted by customers. Customers may request an export of their logs by contacting Oracle.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the audit log retention configuration in the code repository and ascertained the retention period was configured for at least 90 days.	No deviations noted.
	Inspected the audit events log within the administration console in a sample tenancy and ascertained API calls were available from at least 90 days prior to the inspection date and could not be deleted by the user.	No deviations noted.
	Created a compute instance using the console in a sample tenancy and ascertained the event was written to the log.	No deviations noted.
	Inspected the public Oracle website and ascertained it specified a customer could request an export of their logs by submitting a request through MyOracle Support.	No deviations noted.
OCI-03.03: Access to customer virtual cloud networks is controlled by a combination of security lists and routing tables configured by the customer.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Created a new virtual cloud network from the customer console using the default settings and ascertained the virtual cloud network was configured with a default routing table and security list.	No deviations noted.
	Inspected the routing table and security list and ascertained the user could configure the routing table/security list by updating ingress and egress rules.	No deviations noted.
	Updated an ingress rule to allow SSH traffic on port 24 instead of port 22, attempted to connect to a server in the VCN over the SSH protocol on port 22 and ascertained the connection was unsuccessful. Restored the default setting, attempted to connect to the server again and ascertained the connection was successful.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-03.05: When a customer initiates the deletion of a virtual machine in a multi-tenant environment, a termination workflow deletes the virtual machine.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the virtual machine termination configuration and ascertained it was configured to delete the virtual machine and release the capacity to the hypervisor when the deletion request was received. Additionally, ascertained the workflow was configured to create a ticket if the termination workflow failed.	No deviations noted.
	Created a virtual machine using the console in a sample tenancy and subsequently observed the same virtual machine on the virtualization management software host (hypervisor). Terminated the virtual machine in the console and once the termination completed, observed an engineer query for the virtual machine on the hypervisor and ascertained the virtual machine was terminated.	No deviations noted.
	Inspected the ticket and supporting documentation for a sample of availability and operational incidents selected from the ticketing system and ascertained the ticket was investigated and resolved or was being tracked through resolution.	No deviations noted.
	For the Fusion Applications Environment Management service, inspected the virtual machine termination configuration and ascertained it was configured to delete the virtual machine when the deletion request was received and created a ticket if the termination workflow failed.	No deviations noted.
	For the Fusion Applications Environment Management service, observed a production Fusion environment in a sample tenancy and ascertained the same Fusion environment's attributes were in an active and functional state. Terminated the Fusion environment, and once the termination completed, observed an engineer query for the Fusion environment and ascertained its contents were no longer accessible.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	For the Fusion Applications Environment Management service, inspected the ticket and supporting documentation for a sample of availability and operational incidents selected from the ticketing system and ascertained the ticket was investigated and resolved or was being tracked through resolution.	No deviations noted.
OCI-03.09: When a storage instance is terminated by the customer, there is an automated process to render the data inaccessible.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the block storage termination configuration and ascertained it was configured to delete the instance's access key from the controller upon termination of the instance.	No deviations noted.
	Created two block storage volumes in a sample tenancy using the console, terminated one of the block storage volumes, and ascertained the deleted volume was inaccessible while the active volume remained accessible.	No deviations noted.
	Inspected the configuration that renders the data inaccessible when an object storage instance was deleted and ascertained it was configured to delete the instance's encryption key upon termination of the instance.	No deviations noted.
	Created an object storage instance in a sample tenancy using the console, terminated the object storage instance, and ascertained the deleted volume was inaccessible.	No deviations noted.
	Inspected the configuration that renders the data inaccessible when a file storage instance was deleted and ascertained it was configured to disassociate the instance's encryption key upon termination of the instance.	No deviations noted.
	Created a file storage instance in a sample tenancy using the console, terminated the file storage instance, and ascertained the file storage instance was inaccessible.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	For the Fusion Applications Environment Management service, inspected the configuration that renders the data inaccessible when an Automated Storage Management (ASM) storage instance is deleted and ascertained it was configured to delete the existing user domain (DomU) stored within the instance, which rendered the encryption key inaccessible.	No deviations noted.
	For the Fusion Applications Environment Management service, created an ASM storage instance in a sample tenancy using the console, terminated the ASM storage instance, and ascertained the ASM storage instance was inaccessible.	No deviations noted.
OCI-03.12: Oracle-provided Windows images are initially configured without a provisioned default Administrator account, restricting authentication to the Remote Desktop Protocol (RDP). Initial login occurs via a system generated password that must be changed at first logon.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Conducted a port scan of servers provisioned from a sample of Windows images, selected from the customer console, and ascertained the only open port was in accordance with Oracle Cloud Infrastructure documentation.	No deviations noted.
	Authenticated to servers provisioned from a sample of Windows images, selected from the customer console, using the system generated password and ascertained the user was required to change their password on initial logon.	No deviations noted.
	Inspected the initially provisioned user accounts on servers provisioned from a sample of Windows images, selected from the customer console and ascertained the only provisioned account was "opc" and the admin and guest accounts were not provisioned.	No deviations noted.
OCI-03.13: Oracle-provided Linux images are initially configured to disable access to the root account and restrict authentication to the SSH protocol using a public/private key pair.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Conducted a port scan on servers provisioned from a sample of Linux images, selected from the customer console and ascertained the only open port was in accordance with Oracle Cloud Infrastructure documentation.	No deviations noted.
	Attempted to authenticate to servers built from a sample of Linux images, selected from the customer console, using SSH without providing the SSH private key paired to the public key provided during the provisioning process and ascertained the connection was denied. Additionally, attempted to authenticate to servers built from a sample of Linux images, selected from the customer console, using SSH while providing the SSH private key paired to the public key provided during the provisioning process and ascertained the connection was successful.	No deviations noted.
	Inspected the authentication configuration on servers provisioned from a sample of Linux images, selected from the console, and ascertained users with the exception of "opc" and “ubuntu” (for Ubuntu images) were configured to deny login attempts.	No deviations noted.
	Attempted to connect to servers provisioned from a sample of Linux images, selected from the customer console, using the root account and ascertained the user was unable to connect and received a message specifying that the user must authenticate using the "opc" account or “ubuntu” (for Ubuntu images) account.	No deviations noted.
OCI-03.14: For Fusion customers utilizing the break glass functionality, credentials to access the Fusion Applications Environment Management generic administrator accounts are distributed through the Oracle Managed Access service based on the approval settings configured by customers. The credentials will expire and will be automatically changed at the end of the approved duration or upon customer-initiated revocation.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the break glass configuration and ascertained credentials for Fusion Applications Environment Management service generic administrator accounts were managed through the Oracle Managed Access (OMA) service.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Inspected the configuration in Fusion Application Control Plane (FACP) Vault Manager and ascertained Fusion generic administrator accounts were managed through the Oracle Managed Access (OMA) service. Observed an engineer create a sample break glass request and ascertained credentials for Fusion Applications Environment Management service generic administrator accounts were managed through the OMA service.	No deviations noted.
	Inspected the break glass configuration and ascertained customer approvals were required before the generic administrator account credentials could be distributed.	No deviations noted.
	Observed an engineer create a sample break glass request through the console and attempt to access the generic administrator account before and after the customer approved the request and ascertained customer approvals were required before the generic administrator account credentials could be distributed.	No deviations noted.
	Inspected the break glass configuration and ascertained generic administrator account credentials would expire and would be automatically changed at the end of the approved duration or upon customer-initiated revocation.	No deviations noted.
	Observed an engineer attempt to access the generic administrator account through an approved break glass request after the expiration period elapsed and after the customer-initiated revocation and ascertained generic administrator account credentials expired and were changed at the end of the approved duration or upon customer-initiated revocation.	No deviations noted.
	Inspected the break glass configuration and ascertained simultaneous access requests required customer approvals before the generic administrator account credentials could be distributed.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Observed an engineer create a sample break glass request through the console and then create another identical break glass request to the same resource and ascertained customer approvals were required before the generic administrator account credentials could be distributed.	No deviations noted.

Control Objective 4 – Change Management

Controls provide reasonable assurance that changes are implemented to services supporting the System after they are documented and reviewed in line with the Change Management requirements and provide reasonable assurance that changes are tested prior to implementation.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-04.01.A: Changes to infrastructure configurations and services supporting the System follow the Cloud Compliance Standard for Change Management and are documented, tested, and approved prior to implementation to production.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the authentication configuration in the ticketing system and ascertained it was configured to use LDAP to authenticate users.	No deviations noted.
	For a sample of changes selected from the ticketing system inspected the change ticket and supporting documentation and ascertained the changes to infrastructure configurations and services supporting the system were tested prior to implementation to production.	No deviations noted.
	For a sample of changes selected from the ticketing system inspected the change ticket and supporting documentation and ascertained the changes to infrastructure configurations and services supporting the system were approved by an engineer other than the change author prior to implementation to production.	No deviations noted.
	Inspected the Permissions tool and ascertained only authorized personnel could deploy Fusion Applications Environment Management patches into production.	No deviations noted.
	For a sample of changes implemented to the Fusion Applications Environment Management service, selected from the deployment tools, inspected the change ticket and supporting documentation and ascertained the changes to infrastructure configurations and services supporting the system were tested prior to implementation to production.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	For a sample of changes selected from the ticketing system and implemented to the Fusion Applications Environment Management service inspected the change ticket and supporting documentation and ascertained the changes to infrastructure configurations and services supporting the system were approved by an engineer other than the change author prior to implementation to production.	No deviations noted.
	Inspected the ticketing system configuration and ascertained the ticketing system was configured to prevent the approver from being the author of the change ticket.	No deviations noted.
	Observed an engineer create a change ticket, assign themselves as the approver, attempt to approve the ticket and ascertained the ticketing system prevented the approval. Then observed the engineer re-assign the peer reviewer to a different engineer and ascertained the approval was successful.	No deviations noted.
OCI-04.01.B: Changes to infrastructure configurations and services supporting the System that are developed and promoted through a source code management tool are peer reviewed prior to implementation to production. The peer reviewer is different from the author of the change.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the Cloud Compliance Standard for Change Management policy and ascertained that a peer review was required for all changes.	No deviations noted.
	Inspected the source code management tool and change tickets for a sample of commits related to a sample of change tickets selected from the ticketing system and ascertained a peer review was performed by someone other than the author of the change prior to implementation to production.	No deviations noted.
	Observed a developer attempt to promote a code change to a production branch within the code repositories when the approval configurations were set to require at least 1 peer approval and ascertained the commit was promoted to the production branch after the commit was approved.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Observed a developer attempt to promote a code change to a production branch within the code repositories when the approval configurations were set to require at least 1 peer approval and ascertained the commit was unable to be promoted to the production branch without peer approval.	No deviations noted.
OCI-04.02: Changes to hypervisor configurations are investigated and tracked to resolution.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the hypervisor documentation and ascertained hypervisors were configured with a base image and the monitoring tool was configured to detect hosts with a configuration that deviated from the base image.	No deviations noted.
	Inspected the configuration for a sample of hypervisors selected from the asset tool and ascertained they were configured to; • run anti-virus • send monitoring metrics to the monitoring tool • run the File Integrity Monitoring system • run the Host Intrusion Detection system/ Workload Protection (WLP) • obtain time via Network Time Protocol (NTP) from the NTP server • forward logs to the Security Information and Event Monitoring (SIEM) tool.	No deviations noted.
	Inspected the monitoring tool configuration and ascertained it was configured to monitor the configuration of hypervisors and to generate an operational incident ticket if the configuration deviated from the base image.	No deviations noted.
	Inspected the ticket and supporting documentation for a sample of availability and operational incidents selected from the ticketing system and ascertained the ticket was investigated and resolved or was being tracked through resolution.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-04.03: Emergency and mitigating changes to infrastructure configurations and services supporting the System require approval of a Senior Manager or above.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected a sample of emergency and mitigating change tickets and supporting documentation selected from the ticketing system and ascertained the emergency changes to infrastructure configurations and services supporting the system were approved by a Senior Manager or above prior to implementation to production.	No deviations noted.
OCI-04.04: The server configuration management tools for services supporting the System are configured to automatically revert unauthorized changes back to the master configuration. Write and admin access to the server configurations code repository is restricted to approved personnel.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Observed an engineer update a configuration on a sample server supporting a service and a sample bastion server and inspected the configuration after the next execution of the configuration management tool and ascertained the configuration was reverted to the prior state.	No deviations noted.
	Inspected the schedule for a sample server supporting services in the system and a sample bastion server selected from the asset tool and ascertained the configuration management tool was configured to execute at least hourly.	No deviations noted.
	Inspected the access configuration for the code repository tool and ascertained write and admin access to the source code repository tool was controlled by the Permissions tool.	No deviations noted.
	Inspected a sample update to the master configuration and ascertained the change to the configuration followed the standard OCI change management process.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-04.05: The source code management tools for services supporting the System are configured to store current and prior versions of source code to support rollback to prior versions. Write access to the source code management tools are restricted to approved personnel.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the source code management tools for a sample of services and supporting services and ascertained the current and prior versions of the source code were available to support rollback to prior versions.	No deviations noted.
	Inspected the access configuration for the code repository tools and ascertained write and admin access to the source code repository tool was controlled using resources managed by the permissions tools.	No deviations noted.
OCI-04.08: Development/testing and production environments are logically separated.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the network plan configuration for a sample of realms and ascertained the testing and development environments were logically separated from the production environments.	No deviations noted.
OCI-04.12: Source code management tools are reviewed annually to validate that the tools are configured to require at least one independent approval before a change can be merged to a production related source code repository. Issues identified are investigated and tracked to resolution.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the source code tools review documentation and ascertained that the review was completed within the past year to validate that source code management tools were configured to require at least one independent approval before a change could be merged to a production related source code repository and any issues identified were investigated and tracked to resolution.	No deviations noted.
OCI-07.06: File integrity monitoring (FIM) tools alert personnel to unauthorized modification of critical system files, configuration files, or content files on the infrastructure supporting the System. * Refer to section "Oracle Operator Access Control - Impacted Controls" for additional information.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Inspected the configuration management tool configuration for the below asset types and ascertained it was configured with file integrity monitoring to detect the unauthorized modification of critical system files, configuration files, or content files: • Servers • Hypervisors • Bastions	No deviations noted.
	For the Exadata Database on Cloud at Customer (ExaDB-C@C) service, inspected the configuration for a sample of servers and ascertained it was configured with file integrity monitoring to detect the unauthorized modification of critical system files, configuration files, or content files.	No deviations noted.
	Inspected an alert raised by the file integrity monitoring tool and ascertained an associated ticket was investigated and resolved.	No deviations noted.

Control Objective 5 – Incident Management

Controls provide reasonable assurance that incidents impacting the security and integrity of the infrastructure supporting the System are recorded, investigated and tracked to closure.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-05.01: Security incidents are assigned a severity rating and tracked to resolution by the Oracle Cloud Infrastructure Security Operations team. Oracle Cloud Infrastructure reports confirmed security incidents with customer impact to Oracle Global Information Security (GIS) and Oracle Legal, who are responsible for notices or disclosures to the public, customers, affected individuals, and law enforcement authorities.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Queried the ticketing systems in each realm for security incidents created during the period and ascertained there were no incidents without an assigned severity.	No deviations noted.
	Inspected a sample of security incident tickets and supporting documentation selected from the ticketing systems and ascertained the incidents followed the handling process and were tracked through resolution.	No deviations noted.
	Inspected the Information Security Incident Reporting and Response Policy and ascertained it specified that confirmed breaches were escalated to GIS for investigation and customer notification in line with the requirements of the policy.	No deviations noted.
	Inspected the documentation of the escalation to GIS and formal customer notification for a sample of confirmed customer security breaches selected from the ticketing system and ascertained Oracle Cloud Infrastructure reported the security incident to Oracle Global Information Security (GIS) and Oracle Legal or that there was no customer impact.	No deviations noted.
OCI-05.02: The Security Incident Management Policy and OCI Security Incident Response Standard specify the process for classification, prioritization and escalation of security incidents including reporting, managing and responding to security incidents including, as applicable, notification of affected customers. This policy and standard also outline the responsibilities of each team during the process.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the Security Incident Management Policy and OCI Security Incident Response Standard and ascertained it specified the process for classification, prioritization and escalation of security incidents including reporting, managing, and responding to security incidents including, as applicable, notification of affected customers as well as the responsibilities of each team during the process.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-05.03: Monitoring tools are used to collect metrics relating to the status and load of assets supporting the services System. The monitoring tools are configured to trigger alerts upon reaching or exceeding specified thresholds that impact availability and operational system metrics. Alerts are tracked to resolution.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the configuration for a sample of the below asset types selected from the asset tool and ascertained they were configured to forward metrics related to the status and load of the devices to the monitoring tool. • Servers • Bastions • Hypervisors • Network devices • SmartNIC cards • ILOMs	No deviations noted.
	Inspected the monitoring tool for a sample of services and supporting services, and ascertained the services were monitored for availability based on defined metrics and thresholds.	No deviations noted.
	Inspected the monitoring tool configuration and ascertained it was configured to generate a ticket when the pre-defined monitoring thresholds were exceeded.	No deviations noted.
	Inspected the ticket and supporting documentation for a sample of availability and operational incidents selected from the ticketing system and ascertained the ticket was investigated and resolved or was being tracked through resolution.	No deviations noted.
	Inspected the monitoring configuration for servers supporting the Exadata Database on Cloud at Customer (ExaDB-C@C) service and ascertained it was configured to forward metrics related to the status and load of the device to the monitoring tool.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-05.04: Operational and availability incidents are assigned a severity, follow the incident handling process and are tracked through resolution.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Queried the ticketing systems for the in-scope commercial and government regions for operational and availability incidents created during the period and ascertained there were no incidents without an assigned severity.	No deviations noted.
	Inspected a sample of operational and availability incident tickets and supporting documentation selected from the ticketing systems and ascertained the incidents followed the incident handling process and were tracked through resolution.	No deviations noted.
OCI-05.05: A Corrective Action/Preventive Action (CAPA) review is completed after the resolution of an Incident Command Center SEV1 incident that met the CAPA review requirements.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the Corrective Action / Preventative Action documentation for a sample of severity 1 incidents which met the CAPA review requirements selected from the ticketing systems and ascertained the CAPA review was completed.	No deviations noted.

Control Objective 6 – Availability, Physical Security and Environmental Safeguards

Controls provide reasonable assurance that infrastructure supporting the system and customer tenancies is available, protected against physical and environmental threats and physical access is restricted to authorized individuals.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-06.01: Oracle Cloud Infrastructure evaluates the data center and PoP site's control environment, including physical security controls and environmental safeguards, prior to the site receiving production traffic (go-live). Identified issues are evaluated and tracked through resolution.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the assessment reports for a sample of new in-scope data center and PoP sites and ascertained Oracle Cloud Infrastructure performed an evaluation of the control environments, including physical security controls and environmental safeguards prior to go-live and that identified issues were tracked through resolution.	No deviations noted.
OCI-06.02: In accordance with the schedule defined in the Data Center Assessment Program, Oracle Cloud Infrastructure periodically performs an assessment of in-scope data center and PoP site's control environments, including physical security controls, environmental safeguards, and media destruction. Identified issues are evaluated and tracked through resolution.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the most recent Oracle Cloud Infrastructure assessment report for a sample of in-scope data center and PoP sites and ascertained Oracle Cloud Infrastructure performed an evaluation of the data center within the defined schedule, including physical security controls, environmental safeguards, and media destruction in line with the requirements of the data center classification level and identified issues were evaluated and tracked to resolution.	No deviations noted.
OCI-06.03: 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 to resolution. In the event that a site does not have an attestation report, or internationally recognized certification, Oracle Cloud Infrastructure performs an assessment annually of the site's control environment, including physical security controls and environmental safeguards.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Inspected the Oracle Cloud Infrastructure review documentation for a sample of in-scope data centers and PoP sites and ascertained a review of the provider's attestation reports or internationally recognized certification or a controls assessment by Oracle Cloud Infrastructure was completed within the past year.	No deviations noted.
	Inspected ticket evidence of the identified issues for a sample of in-scope data centers and PoP sites provider attestation reports or internationally recognized certification or a controls assessment by Oracle Cloud Infrastructure and ascertained they were evaluated and tracked to resolution.	No deviations noted.
	Inspected the Oracle Cloud Infrastructure review documentation for the subservice organizations and ascertained a review of the provider's attestation reports or internationally recognized certification or a controls assessment by Oracle Cloud Infrastructure was completed within the past year.	No deviations noted.
OCI-06.04: Physical access to data halls in the Availability Domains and PoPs is approved prior to access being granted.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the access approval documentation for a sample of users granted physical access to data halls in the in-scope availability domains and PoP sites selected from the Oracle physical access management tool and ascertained the user's access was approved by an appropriate approver prior to being granted.	No deviations noted.
OCI-06.05: Permanent physical access to data halls in the Availability Domains and PoPs is revoked within 14 days of termination.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the physical access records for a sample of terminated employees and contractors selected from the HR tool and ascertained permanent physical access to data halls in the Availability Domains and PoPs was revoked within 14 days of termination.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
OCI-06.06: Users with permanent physical access to data halls in the Availability Domains and PoPs are reviewed at least quarterly. Issues identified during the review are investigated and remediated.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the review documentation for a sample of quarters for access to in-scope data centers and PoP sites and ascertained the reviews were performed timely by an appropriate individual for both quarters in the examination period and inappropriate access, if any, was investigated and remediated.	No deviations noted.
OCI-09.05: Database backups are performed and retained in-line with the configured schedule.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the database backup configurations and ascertained it was configured to perform backups in-line with the schedule configured by the customer or the automated default schedule for an autonomous AI database.	No deviations noted.
	Created a database and configured the database to backup for a specified period of time and ascertained the backup was performed in accordance with the specified schedule. Alternatively created an autonomous AI database and ascertained the backup was performed in accordance with the automated default schedule.	No deviations noted.
OCI-09.06: Fusion Applications Environment Management databases are backed up weekly and data backups are retained for 60 days by default. Backup failures are monitored and resolved timely.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	Inspected the database configuration and ascertained Fusion Applications Environment Management databases were configured to be backed up weekly, backups were automatically monitored for failures and were retained for 60 days by default.	No deviations noted.
	Selected a sample database, inspected the backup logs, and ascertained the database was performing backups on a weekly basis and the expiration of those backups was set to 60 days.	No deviations noted.

CONTROL DESCRIPTION	TESTING PERFORMED	RESULTS OF TESTING
	Inspected ticket documentation for a sample of backup failure notifications selected from the ticketing system and ascertained backup failures were investigated and resolved timely.	No deviations noted.
	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
OCI-09.07: Fusion Applications Environment Management backup data restoration testing is performed monthly.	Inquired of the control owner and ascertained the control was designed and operated as described.	No deviations noted.
	For a sample of months, inspected a Fusion Applications Environment Management backup data restoration test and ascertained Fusion Applications Environment Management backup data restoration testing was performed monthly.	No deviations noted.

SECTION V – ADDITIONAL INFORMATION PROVIDED BY ORACLE CLOUD INFRASTRUCTURE

Documentation

Oracle Cloud Infrastructure documentation provides technical descriptions and guidance for configuring and managing each service including information on security features and best practices. For more information, please review the following documentation:

- Oracle Cloud Basics
- Oracle Cloud Infrastructure Security Guide
- Security Services and Features
- Security Best Practices

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. They include a suite of internal information security policies and customer-facing security practices that apply to different services. Oracle Corporate Security Practices describe how Oracle protects the confidentiality, integrity, and availability of customer data and systems that are hosted in the Oracle Cloud and/or accessed when providing cloud services.

General Data Protection Regulation

Privacy compliance is a shared responsibility between Oracle Cloud Infrastructure and the customer. Oracle Cloud Infrastructure and the GDPR explains how the features and functionality of Oracle Cloud Infrastructure can help customers meet General Data Protection Regulation (GDPR) requirements.

Contracts and Policies

Oracle has standard contracts and policies that govern the terms, service descriptions and delivery of cloud services. For more information, please review the following documentation:

- Data Processing Agreement for Oracle Services
- Oracle Cloud Services Contracts
- Oracle Cloud Hosting and Delivery Policies
- Oracle Artificial Intelligence Terms