System and Organization Controls (SOC 3) Report

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

For the Period October 1, 2022 to March 31, 2023

Prepared in Accordance with AICPA Attestation Standards

Copyright © 2023, Oracle and/or its affiliates
### Table of Contents

**Section I – Report of Independent Accountants**  
3

**Section II – Management’s Report of Its Assertions on the Effectiveness of Its Controls Over the Oracle Cloud Infrastructure System Based on the Trust Services Criteria for Security, Availability, and Confidentiality**  
8

**Attachment A – Description of the Oracle Cloud Infrastructure System**  
12

- Oracle Overview  
12
- Oracle Cloud Infrastructure Overview  
12
- Relevant Aspects of the Control Environment  
34
- Information and Communication  
37
- Risk Assessment  
38
- Monitoring  
38

**Attachment B – Principal Service Commitments and System Requirements**  
39

- Overview  
39
SECTION I – REPORT OF INDEPENDENT ACCOUNTANTS

To the Management of Oracle Cloud Infrastructure:

Scope
We have examined management’s assertion, contained within the accompanying “Management’s Report of Its Assertions on the Effectiveness of Its Controls Over the Oracle Cloud Infrastructure System Based on the Trust Services Criteria for Security, Availability, and Confidentiality” (Assertion), that Oracle’s controls over the Oracle Cloud Infrastructure System were effective throughout the period October 1, 2022 to March 31, 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA’s TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

The System consists of the following services:

- Access Governance
- Account Tracking and Automation Tool
- Accounts Management
- Analytics Cloud
- Anomaly Detection
- API Gateway
- Application Dependency Management
- Application Performance Monitoring
- Archive Storage
- Artifact Registry
- Audit
- Autonomous Database on Cloud at Customer
- Autonomous Database on Dedicated Exadata Infrastructure (ADB-D on ExaCS)
- Autonomous Database on Shared Exadata Infrastructure (ADB-S on ExaCS)
- Bare Metal and Virtual Machine Database Systems
- Bastion
- Big Data
- Bling
- Block Volume
- Blockchain Platform
- Budgets
- Certificates
- Classic Migration
- Client Logging
- Full Stack Disaster Recovery from 10/25/2022
- Functions
- Fusion Analytics Warehouse
- Fusion Apps as a Service (FAaaS)
- GoldenGate
- Health Checks
- Identity and Access Management
- Integration
- Java Management
- Language
- License Manager
- Load Balancer (formerly known as Load Balancing)
- Logging
- Logging Analytics
- Managed Access
- Management Agent
- Marketplace - Consumer
- Monitoring
- MySQL Database
- NetSuite Health Check
- Network Firewall
- Network Load Balancer
- Network Path Analyzer
- Networking
- NoSQL Database
- Cloud Advisor
- Cloud Guard
- Cloud Incident Service
- Cloud Shell
- Compute
- Console Announcements
- Container Engine for Kubernetes
- Container Instances from 10/25/2022
- Content Management (formerly known as Content and Experience)
- Customer Feedback Service
- Data Catalog
- Data Flow
- Data Integration
- Data Labeling
- Data Safe
- Data Science
- Data Transfer
- Database Management
- Database Migration
- Database Tools
- DDoS Protection
- DevOps - Build Service
- DevOps - Deployment Pipelines
- DevOps - Project Service
- DevOps - Source Code Management
- Digital Assistant
- Digital Media
- Domain Name System (DNS)
- Email Delivery
- Events
- Exadata Cloud at Customer
- Exadata Cloud Service
- FastConnect
- File Storage
- Notifications
- Object Storage
- Operations Insights
- Operator Access Control
- Oracle Database Service for Azure
- Oracle Ksplice
- Oracle Open Data
- Oracle Search Cloud
- OS Management
- Process Automation
- Recovery Database Service
- Registry
- Resource Manager
- Roving Edge Infrastructure
- Search
- Search with OpenSearch
- Security Zones
- Service Connector Hub
- Service Manager Proxy
- Service Mesh
- Site-to-Site VPN (formerly known as VPN Connect)
- Speech
- Stack Monitoring
- Status
- Streaming
- Tagging
- Threat Intelligence
- Vault
- Vision
- Visual Builder Cloud
- Visual Builder Studio
- VMWare Solution
- Vulnerability Scanning
- Web Application Acceleration
- Web Application Firewall
supported by availability domains and points of presence in the following regions:

**Commercial Regions**
- Australia East, Sydney, Australia
- 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
- 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
- Israel Central, Jerusalem, Israel
- Italy Northwest, Milan, Italy
- Japan Central, Osaka, Japan
- Japan East, Tokyo, Japan
- Mexico Central, Queretaro, Mexico
- Netherlands Northwest, Amsterdam, Netherlands
- Saudi Arabia West, Jeddah, Saudi Arabia
- Singapore, Singapore
- South Africa Central, Johannesburg, South Africa
- South Korea Central, Seoul, Republic of Korea
- South Korea North, Chuncheon, Republic of 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 from 12/15/2022
- United States West, Phoenix, Arizona, United States
- United States West, San Jose, California, United States

**Government Regions**
- 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

**Dedicated Regions**
- Canberra, Australia
- Chiyoda, Japan
- Osaka, Japan
- Muscat, Oman
- Milan, Italy

and office facilities and security/network operating centers in the following locations:
- Bangalore, India
- Dublin, Ireland
- Guadalajara, Mexico
- Noida, India
- Seattle, Washington, United States

(collectively, the “System”).

**Management’s Responsibilities**
Oracle Cloud Infrastructure’s management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the system
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

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

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

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

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

Opinion
In our opinion, Oracle Cloud Infrastructure’s controls over the system were effective throughout the period October 1, 2022 to March 31, 2023 to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

May 15, 2023
SECTION II – MANAGEMENT’S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER THE ORACLE CLOUD INFRASTRUCTURE SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY, AND CONFIDENTIALITY

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

- Identifying the Oracle Cloud Infrastructure System and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the Oracle Cloud Infrastructure System to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the Trust Services categories that are the basis of our assertion

The System consists of the following services:

- Access Governance
- Account Tracking and Automation Tool
- Accounts Management
- Analytics Cloud
- Anomaly Detection
- API Gateway
- Application Dependency Management
- Application Performance Monitoring
- Archive Storage
- Artifact Registry
- Audit
- Autonomous Database on Cloud at Customer
- Autonomous Database on Dedicated Exadata Infrastructure (ADB-D on ExaCS)
- Autonomous Database on Shared Exadata Infrastructure (ADB-S on ExaCS)
- Bare Metal and Virtual Machine Database Systems
- Bastion
- Big Data
- Bling
- Block Volume
- Blockchain Platform
- Budgets
- Certificates
- Classic Migration
- Client Logging
- Cloud Advisor
- Functions
- Fusion Analytics Warehouse
- Fusion Apps as a Service (FAaaS)
- GoldenGate
- Health Checks
- Identity and Access Management
- Integration
- Java Management
- Language
- License Manager
- Load Balancer (formerly known as Load Balancing)
- Logging
- Logging Analytics
- Managed Access
- Management Agent
- Marketplace - Consumer
- Monitoring
- MySQL Database
- NetSuite Health Check
- Network Firewall
- Network Load Balancer
- Network Path Analyzer
- Networking
- NoSQL Database
- Notifications
- Object Storage
- Operations Insights
• Cloud Guard
• Cloud Incident Service
• Cloud Shell
• Compute
• Console Announcements
• Container Engine for Kubernetes
• Container Instances from 10/25/2022
• Content Management (formerly known as Content and Experience)
• Customer Feedback Service
• Data Catalog
• Data Flow
• Data Integration
• Data Labeling
• Data Safe
• Data Science
• Data Transfer
• Database Management
• Database Migration
• Database Tools
• DDoS Protection
• DevOps - Build Service
• DevOps - Deployment Pipelines
• DevOps - Project Service
• DevOps - Source Code Management
• Digital Assistant
• Digital Media
• Domain Name System (DNS)
• Email Delivery
• Events
• Exadata Cloud at Customer
• Exadata Cloud Service
• FastConnect
• File Storage
• Full Stack Disaster Recovery from 10/25/2022
• Operator Access Control
• Oracle Database Service for Azure
• Oracle Ksplice
• Oracle Open Data
• Oracle Search Cloud
• OS Management
• Process Automation
• Recovery Database Service
• Registry
• Resource Manager
• Roving Edge Infrastructure
• Search
• Search with OpenSearch
• Security Zones
• Service Connector Hub
• Service Manager Proxy
• Service Mesh
• Site-to-Site VPN (formerly known as VPN Connect)
• Speech
• Stack Monitoring
• Status
• Streaming
• Tagging
• Threat Intelligence
• Vault
• Vision
• Visual Builder Cloud
• Visual Builder Studio
• VMWare Solution
• Vulnerability Scanning
• Web Application Acceleration
• Web Application Firewall

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

Commercial Regions
• Australia East, Sydney, Australia
• 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
• 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
• Israel Central, Jerusalem, Israel
• Italy Northwest, Milan, Italy
• Japan Central, Osaka, Japan
• Japan East, Tokyo, Japan
• Mexico Central, Queretaro, Mexico
• Netherlands Northwest, Amsterdam, Netherlands
• Saudi Arabia West, Jeddah, Saudi Arabia
• Singapore, Singapore
• South Africa Central, Johannesburg, South Africa
• South Korea Central, Seoul, Republic of Korea
• South Korea North, Chuncheon, Republic of 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 from 12/15/2022
• United States West, Phoenix, Arizona, United States
• United States West, San Jose, California, United States

Government Regions

• 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

Dedicated Regions

• Canberra, Australia
• Chiyoda, Japan
• Milan, Italy
• Muscat, Oman
• Osaka, Japan

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

• Bangalore, India
• Dublin, Ireland
• Guadalajara, Mexico
• Noida, India
• Seattle, Washington, United States

(collectively, the “System”).

We assert that the controls over the system were effective throughout the period October 1, 2022 to March 31, 2023, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to Security, Availability and Confidentiality set forth in the AICPA’s TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Very truly yours,

ORACLE
ATTACHMENT A – DESCRIPTION OF THE ORACLE CLOUD INFRASTRUCTURE SYSTEM

Oracle Overview

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

Oracle Cloud Services offerings, which include Oracle Software-as-a-Service (SaaS) and Oracle Cloud Infrastructure (OCI), provide comprehensive and integrated applications and infrastructure services delivered via cloud-based deployment models. Oracle Cloud Services integrate IT components, including software, hardware and services, on a customer’s behalf in a cloud-based IT environment that Oracle deploys, manages, supports and upgrades for the customer and may be accessed by the customer 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 different deployment models to enable interchangeability and extendibility between IT environments; compatible to easily move workloads between the Oracle Cloud and other IT environments; cost-effective by requiring lower upfront customer investment; and secure; standards-based and reliable.

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

Oracle hardware product offerings 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 services to assist our customers and partners to maximize the performance of their Oracle purchases.

Providing choice and flexibility to Oracle customers as to when and how they deploy Oracle applications and infrastructure technologies is an important element to our corporate strategy. We believe that offering customers broad, comprehensive, flexible, and interoperable deployment models for Oracle applications and infrastructure technologies is important to our growth strategy.

Oracle Cloud Infrastructure Overview

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

Dedicated Region is a cloud region built with Oracle-designed high-performance infrastructure to help customers bring all second-generation cloud primitives and services closer to existing data and applications. It is a fully featured public cloud with all services on premises.
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. Dedicated regions are public regions assigned to a single organization.

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

**Fault Domains**

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

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

**Realms**

Regions are grouped into 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 the customer can have resources in the regions within that realm. Customers cannot access regions that are not in their realm.

The following table lists the regions in the Oracle Cloud Infrastructure commercial realm included in the scope of the System:

<table>
<thead>
<tr>
<th>REGION NAME</th>
<th>REGION IDENTIFIER</th>
<th>REGION LOCATION</th>
<th>REGION KEY</th>
<th>REALM KEY</th>
<th>AVAILABILITY DOMAINS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia East (Sydney)</td>
<td>ap-sydney-1</td>
<td>Sydney, Australia</td>
<td>SYD</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Australia Southeast (Melbourne)</td>
<td>ap-melbourne-1</td>
<td>Melbourne, Australia</td>
<td>MEL</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Brazil East (Sao Paulo)</td>
<td>sa-saopaulo-1</td>
<td>Sao Paulo, Brazil</td>
<td>GRU</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Brazil Southeast (Vinhedo)</td>
<td>sa-vinhedo-1</td>
<td>Vinhedo, Brazil</td>
<td>VCP</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>REGION NAME</td>
<td>REGION IDENTIFIER</td>
<td>REGION LOCATION</td>
<td>REGION KEY</td>
<td>REALM KEY</td>
<td>AVAILABILITY DOMAINS</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>------------</td>
<td>-----------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Canada Southeast (Montreal)</td>
<td>ca-montreal-1</td>
<td>Montreal, Canada</td>
<td>YUL</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Canada Southeast (Toronto)</td>
<td>ca-toronto-1</td>
<td>Toronto, Canada</td>
<td>YZ</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Chile (Santiago)</td>
<td>sa-santiago-1</td>
<td>Santiago, Chile</td>
<td>SCL</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>France Central (Paris)</td>
<td>eu-paris-1</td>
<td>Paris, France</td>
<td>CDG</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>France South (Marseille)</td>
<td>eu-marseille-1</td>
<td>Marseille, France</td>
<td>MRS</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Germany Central (Frankfurt)</td>
<td>eu-frankfurt-1</td>
<td>Frankfurt, Germany</td>
<td>FRA</td>
<td>OC1</td>
<td>3</td>
</tr>
<tr>
<td>India South (Hyderabad)</td>
<td>ap-hyderabad-1</td>
<td>Hyderabad, India</td>
<td>HYD</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>India West (Mumbai)</td>
<td>ap-mumbai-1</td>
<td>Mumbai, India</td>
<td>BOM</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Israel Central (Jerusalem)</td>
<td>il- jerusalem-1</td>
<td>Jerusalem, Israel</td>
<td>MTZ</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Italy Northwest (Milan)</td>
<td>eu-milan-1</td>
<td>Milan, Italy</td>
<td>LIN</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Japan Central (Osaka)</td>
<td>ap-osaka-1</td>
<td>Osaka, Japan</td>
<td>KIX</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Japan East (Tokyo)</td>
<td>ap-tokyo-1</td>
<td>Tokyo, Japan</td>
<td>NRT</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Mexico Central (Queretaro)</td>
<td>mx-queretaro-1</td>
<td>Queretaro, Mexico</td>
<td>QRO</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Netherlands Northwest (Amsterdam)</td>
<td>eu-amsterdam-1</td>
<td>Amsterdam, Netherlands</td>
<td>AMS</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Saudi Arabia West (Jeddah)</td>
<td>me-jeddah-1</td>
<td>Jeddah, Saudi Arabia</td>
<td>JED</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Singapore (Singapore)</td>
<td>ap-singapore-1</td>
<td>Singapore, Singapore</td>
<td>SIN</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>South Africa Central (Johannesburg)</td>
<td>af-johannesburg-1</td>
<td>Johannesburg, South Africa</td>
<td>JNB</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>South Korea Central (Seoul)</td>
<td>ap-seoul-1</td>
<td>Seoul, South Korea</td>
<td>ICN</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>South Korea North (Chuncheon)</td>
<td>ap-chuncheon-1</td>
<td>Chuncheon, South Korea</td>
<td>YNY</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Spain Central (Madrid)</td>
<td>eu-Madrid-1</td>
<td>Madrid, Spain</td>
<td>MAD</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Sweden Central (Stockholm)</td>
<td>eu-stockholm-1</td>
<td>Stockholm, Sweden</td>
<td>ARN</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Switzerland North (Zurich)</td>
<td>eu-zurich-1</td>
<td>Zurich, Switzerland</td>
<td>ZRH</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>UAE Central (Abu Dhabi)</td>
<td>me-abudhabi-1</td>
<td>Abu Dhabi, UAE</td>
<td>AUH</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>UAE East (Dubai)</td>
<td>me-dubai-1</td>
<td>Dubai, UAE</td>
<td>DXB</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>UK South (London)</td>
<td>uk-london-1</td>
<td>London, UK</td>
<td>LHR</td>
<td>OC1</td>
<td>3</td>
</tr>
<tr>
<td>UK West (Newport)</td>
<td>uk-cardiff-1</td>
<td>Newport, UK</td>
<td>CWL</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>US East (Ashburn)</td>
<td>us-ashburn-1</td>
<td>Ashburn, Virginia, US</td>
<td>IAD</td>
<td>OC1</td>
<td>3</td>
</tr>
<tr>
<td>REGION NAME</td>
<td>REGION IDENTIFIER</td>
<td>REGION LOCATION</td>
<td>REGION KEY</td>
<td>REALM KEY</td>
<td>AVAILABILITY DOMAINS</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------</td>
<td>--------------------------</td>
<td>------------</td>
<td>-----------</td>
<td>----------------------</td>
</tr>
<tr>
<td>US Midwest (Chicago)</td>
<td>us-chicago-1</td>
<td>Chicago, IL</td>
<td>ORD</td>
<td>OC1</td>
<td>3 – From December 15, 2022</td>
</tr>
<tr>
<td>US West (Phoenix)</td>
<td>us-phoenix-1</td>
<td>Phoenix, Arizona, US</td>
<td>PHX</td>
<td>OC1</td>
<td>3</td>
</tr>
<tr>
<td>US West (San Jose)</td>
<td>us-sanjose-1</td>
<td>San Jose, California, US</td>
<td>SJC</td>
<td>OC1</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>REGION NAME</th>
<th>REGION IDENTIFIER</th>
<th>REGION LOCATION</th>
<th>REGION KEY</th>
<th>REALM KEY</th>
<th>AVAILABILITY DOMAINS</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Gov East (Ashburn)</td>
<td>us-langley-1</td>
<td>Ashburn, Virginia, US</td>
<td>LFI</td>
<td>OC2</td>
<td>1</td>
</tr>
<tr>
<td>US Gov West (Phoenix)</td>
<td>us-luke-1</td>
<td>Phoenix, Arizona, US</td>
<td>LUF</td>
<td>OC2</td>
<td>1</td>
</tr>
</tbody>
</table>

The following table lists the regions in the Oracle Cloud Infrastructure United States DoD Cloud realm included in the scope of the System:

<table>
<thead>
<tr>
<th>REGION NAME</th>
<th>REGION IDENTIFIER</th>
<th>REGION LOCATION</th>
<th>REGION KEY</th>
<th>REALM KEY</th>
<th>AVAILABILITY DOMAINS</th>
</tr>
</thead>
<tbody>
<tr>
<td>US DoD East (Ashburn)</td>
<td>us-gov-ahsburn-1</td>
<td>Ashburn, Virginia, US</td>
<td>RIC</td>
<td>OC3</td>
<td>1</td>
</tr>
<tr>
<td>US DoD North (Chicago)</td>
<td>us-gov-chicago-1</td>
<td>Chicago, Illinois, US</td>
<td>PIA</td>
<td>OC3</td>
<td>1</td>
</tr>
<tr>
<td>US DoD West (Phoenix)</td>
<td>us-gov-phoenix-1</td>
<td>Phoenix, Arizona, US</td>
<td>TUS</td>
<td>OC3</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>REGION NAME</th>
<th>REGION IDENTIFIER</th>
<th>REGION LOCATION</th>
<th>REGION KEY</th>
<th>REALM KEY</th>
<th>AVAILABILITY DOMAINS</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK Gov South (London)</td>
<td>uk-gov-london-1</td>
<td>London, UK</td>
<td>LTN</td>
<td>OC4</td>
<td>1</td>
</tr>
<tr>
<td>UK Gov West (Newport)</td>
<td>uk-gov-cardiff-1</td>
<td>Newport, UK</td>
<td>BRS</td>
<td>OC4</td>
<td>1</td>
</tr>
</tbody>
</table>

The following table lists the Dedicated Region Cloud at Customer regions included in the scope of the System:

<table>
<thead>
<tr>
<th>REGION NAME</th>
<th>REGION IDENTIFIER</th>
<th>REGION LOCATION</th>
<th>REGION KEY</th>
<th>REALM KEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>NJA Dedicated Region</td>
<td>ap-chiyoda-1</td>
<td>Chiyoda, Japan</td>
<td>NJA</td>
<td>OC8</td>
</tr>
<tr>
<td>UKB Dedicated Region</td>
<td>ap-ibaraki-1</td>
<td>Osaka, Japan</td>
<td>UKB</td>
<td>OC8</td>
</tr>
<tr>
<td>MCT Dedicated Region</td>
<td>me-dcc-muscat-1</td>
<td>Muscat, Oman</td>
<td>MCT</td>
<td>OC9</td>
</tr>
<tr>
<td>WGA Dedicated Region</td>
<td>ap-dcc-canberra-1</td>
<td>Canberra, Australia</td>
<td>WGA</td>
<td>OC10</td>
</tr>
<tr>
<td>BGY Dedicated Region</td>
<td>eu-dcc-milan-1</td>
<td>Milan, Italy</td>
<td>BGY</td>
<td>OC14</td>
</tr>
</tbody>
</table>
Account and Access Concepts

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.

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

Core Service Concepts
Virtual Cloud Network
A VCN is a virtual version of a traditional network—including subnets, route tables, and gateways—on which the customer 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 ensure access to 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 (OCI) services to meet the Trust Services Criteria related to security, availability, and confidentiality. These criteria are set forth in TSP section 100, of the 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

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

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

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

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

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

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

API Gateway
API Gateway allows customers to publish APIs with private endpoints that are accessible from within their network, and which they can expose with public IP addresses to enable them to accept traffic from the internet. The endpoints support API validation, request and response transformation, cross-origin resource sharing (CORS), authentication and authorization, and request limiting. Using the API Gateway service, the customer can create one or more API gateways in a regional subnet to process traffic from front-end clients and route it to back-end services. A single API gateway can be used to link multiple back-end services (such as load balancers, compute instances, and OCI Functions) into a single consolidated API endpoint.

Application Dependency Management
Application Dependency Management (ADM) detects security vulnerabilities in application dependencies. It relies on scores provided by the Common Vulnerability Scoring System: an open framework for communicating the characteristics and severity of software vulnerabilities. ADM is configured in the "Managed Build" stage of a DevOps pipeline.
Application Performance Monitoring

Application Performance Monitoring provides customers with 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 best for preserving cold data for compliance and audit mandates, retroactively analyzing log data, historical or infrequently accessed content repository data, and application generated data that requires archival for future analysis or legal purposes. 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, and to help ensure compliance with standards or regulations. Log events recorded by Audit include API calls made by the Oracle Cloud Infrastructure Console, Command Line Interface (CLI), Software Development Kits (SDK), custom clients, or other OCI 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 any software or protocol support by Secure Shell (SSH) sessions. When connected, users can interact with the target resource by using any software or protocol supported by SSH. For example, customers can use the Remote Desktop Protocol (RDP) to connect to a Windows host, or use Oracle Net Services to connect to a database.

Big Data

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

Bling

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

Block Volume

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

Blockchain Platform

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

**Budgets**

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

**Certificates**

Certificates provides customers with certificate issuance, storage, and management capabilities, including revocation and automatic renewal. The Certificates service can be used to exercise lifecycle management features for certificate authorities (CAs), certificates, and certificate authority (CA) bundles, helping customers to control these resources and access to them.

**Classic Migration**

Classic Migration simplifies the migration of applications from Oracle Cloud Infrastructure Classic and Oracle Cloud at Customer to Oracle Cloud Infrastructure. An application is a combination of deployable artifacts and the applied configurations, which can be exported from a service instance running in a source environment and imported into a compatible service instance running on Oracle Cloud Infrastructure.

**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 maximize cost savings and 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 risk 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 shapes that are designed to meet a range of compute and application requirements.

**Console Announcements**

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

**Container Engine for Kubernetes**

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

**Container Instances (from October 25, 2022)**

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

**Content Management**

Content Management (formerly known as Content and Experience) 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 fully managed, self-service, data discovery and governance solution for enterprise data. With Data Catalog, customers get a single collaborative environment to manage technical, business, and operational metadata.

**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 a simple user interface with API support for integration with applications and workflows.

**Data Integration**

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

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

Data Transfer
Data Transfer allows customers to migrate data to Oracle Cloud Infrastructure. Customers can export data currently residing in Oracle Cloud Infrastructure to the data center offline. Customers can transfer data as files on encrypted USB 2.0/3/0 disk to an Oracle transfer site; as files on secure, high-capacity, Oracle-supplied storage appliances to an Oracle transfer site or customers can export their data from Object Storage bucket to their data center using an Oracle-provided appliance. Data Transfer uses the following encryption methods: data at rest is encrypted with AES-256 encryption, node-to-node communication is encrypted with GCM-AES-128, console and API are using TLS and will default to AES-256.

Database
The Database service offers autonomous, bare metal, virtual machine, and Exadata Database cloud solutions. Autonomous databases are preconfigured environments that are suitable for either transaction processing or for data warehouse workloads. Bare metal, virtual machine, and Exadata database systems can be customized by the customer with the resources and settings that meet their needs. Customers can quickly provision any database system. Customers have full access to the features and operations available with the database, but Oracle owns and manages the infrastructure.

Customers can also extend database services into their data center by using Exadata Cloud at Customer, which applies the combined power of Exadata and Oracle Cloud Infrastructure while enabling customers to meet their data-residency requirements.

Bare Metal and Virtual Machine Database Systems
Oracle Cloud Infrastructure offers single-node database systems on either bare metal or virtual machines, and 2-node RAC database systems on virtual machines. If the customer needs to provision a database system for development or testing purposes, a special fast-provisioning single-node virtual machine system is available. Bare metal database systems consist of a single bare metal service running Oracle Linux, with locally attached NVMe storage.

There are two types of database systems on virtual machines including a 1-node virtual machine database system consisting of one virtual machine and a 2-node virtual machine database system consisting of two virtual machines.

Bare Metal and Virtual Machine database backups are performed and retained in-line with the schedule configured by customers.

Exadata Cloud Service
An Exadata database system consists of a base system, quarter rack, half rack, or full rack of compute nodes and storage servers. Exadata Cloud Service (ExaCS) enables customers to elastically request, provision, instantiate, connect, and manage Exadata machines in the cloud. Exadata database backups are performed and retained in-line with the schedule configured by customers.
The Exadata database systems as described above are considered in the scope of the Oracle Cloud Infrastructure System and conforms to the controls outlined in this service description.

Exadata racks are “engineered systems” provisioned as dedicated hardware with embedded software, as though the customer had an on-premises rack. Exadata rack maintenance, security, and the embedded software development practices of the Exadata rack engineering systems are not in the scope of the Oracle Cloud Infrastructure System.

**Exadata Cloud at Customer**

Exadata Cloud at Customer (ExaC@C) combines cloud simplicity, agility, and elasticity inside the customer’s data center to provide full-feature Oracle Database instances hosted on an Oracle Exadata Database Machine. The System enables customers to elastically request, provision, instantiate, connect, and manage Exadata machines in an on-premises cloud.

An Exadata Database Machine consists of a base system, quarter rack, half rack, or full rack of compute nodes and storage servers. The ExaC@C service is deployed ExaC@C rack (data plane) in a data center (control plane) of the customer’s choice. The ExaC@C rack contains all the components of a standard Exadata Database Machine, 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 ExaC@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, ExaC@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.

**Autonomous Databases**

The Database service offers Oracle’s Autonomous Database with transaction processing and data warehouse workload types. It is a preconfigured database environment with four workload types available, Autonomous Transaction Processing, Autonomous Data Warehouse, Oracle APEX Application Development and Autonomous JSON Database. Customers do not need to configure or manage any hardware or install any software. Autonomous Database has several infrastructure options. Autonomous database backups are performed and retained in-line with the schedule configured by customers.

- **Autonomous Database on Dedicated Exadata Infrastructure** (ADB-D on ExaCS), customers have exclusive use of the Exadata hardware. Dedicated Exadata Infrastructure offers multitenant database architecture, allowing customers to create and manage multiple Autonomous Databases within a single database system. Both workload types (transaction processing and warehouse) can be provisioned on Dedicated Exadata infrastructure.
- **Autonomous Database on Cloud at Customer** (ADB-D on ExaC@C) combines the benefits of a self-driving, self-securing, and self-repairing database management system and the security and control offered by having it deployed securely on premise behind the customer’s firewall.
- **Autonomous Database on Shared Exadata Infrastructure** (ADB-S on ExaCS), customers provision and manage only the Autonomous Database, while Oracle deploys and manages the Exadata infrastructure. Both workload types (transaction processing and warehouse) can be provisioned with shared Exadata infrastructure.

**Database Management**

Database Management provides customers with comprehensive database performance diagnostics and management capabilities to monitor and manage Oracle Databases. In addition, Database Management can be used to discover and monitor Oracle Database System components, such as Clusters and ASM, located outside of Oracle Cloud Infrastructure.

**Database Migration**

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

DevOps is an end-to-end, continuous integration and continuous delivery (CI/CD) platform for developers that allows customers to 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 - Project Service

A project logically groups the DevOps resources needed to implement a CI/CD workflow. DevOps resources can be artifacts, build pipelines, deployment pipelines, external connections, triggers, and environments. To successfully build and deploy applications by using the DevOps service, customers need to create a DevOps project first.

DevOps - Source Code Management

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 - Build Service

A build pipeline contains the stages that define the build process for successfully compiling, testing, and running software applications before deployment. A stage is an action in the build pipeline. The DevOps service includes the following pre-defined stages that customers can use in a build pipeline: managed build, deliver artifacts, trigger deployment, and wait.

DevOps - Deployment Pipelines

A deployment pipeline holds the requirements that must be satisfied to deliver a set of artifacts to the target environment. A stage is an action in the deployment pipeline. Deployment pipelines contain different stages for automated deployment. Customers can run the deployment pipeline based on their release strategies. DevOps service includes the following pre-defined stages that could be readily used in a deployment pipeline: deploy to a Kubernetes cluster, deploy to an instance group, deploy based on Blue-Green strategy, deploy based on Canary strategy, deploy to functions, deploy to Helm Chart, control (approval, traffic shift, and wait), and integrations (invoke and shell).

Digital Assistant

Digital Assistant allows customers to create and deploy digital assistants, which are virtual devices that help users accomplish tasks through natural language conversations, without having to seek out and wade through various applications and websites. Each digital assistant contains a collection of specialized skills. When a user engages with the digital assistant, the digital assistant evaluates the user input and routes the conversation to and from the appropriate skills.

Digital Media

Digital Media service consists of the Media Flow and Media Streams services, which can be used independently or together and operate on the content stored in the Oracle Cloud Infrastructure Object Store. It is a fully managed service for processing media (video) source content. It provides scalable distribution and origination for just-in-time packaged Adaptive Bitrate (ABR) video content.

- Media Flow enables customers to configure content processing workflows that can be used to process video source content. The processing includes transcoding, transcribing, thumbnail generation, ABR packaging, and integration with Oracle Cloud Infrastructure AI Services such as Speech (for automatic transcription), Language (for Natural Language Processing (NLP) based analysis of the transcript), and Vision (for object detection and text extraction).
- Media Streams provides the capability to deliver digital video packaged in a format such as HTTP Live Streaming (HLS) to viewers. Customers can ingest pre-packaged HLS packages, or they can use Media Flow to transcode and package a source video into a format suitable for streaming. Media Streams can be configured to act as the origin service for video distribution through a Content Delivery Network (CDN).

Distributed Denial of Service Protection

Distributed Denial of Service (DDoS) protection is an always-on detection and mitigation platform for common DDoS volumetric attacks. The service protects against common layer 3 and 4 attacks like SYN floods, UDP floods, ICMP floods, and NTP Amplification attacks. DDoS Protection of system traffic passing through gateway routers is included with all Oracle Cloud Infrastructure accounts and no configuration or monitoring is required; however, customers are responsible for designing DDoS protection mechanisms to meet their requirements.
Domain Name System (DNS)
The Oracle Cloud Infrastructure Domain Name System (DNS) service lets 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.

Email Delivery
Email Delivery is an email sending service that provides a fast and reliable managed solution for sending secured, high-volume marketing and transactional emails. Email Delivery provides the tools necessary to send application-generated email for mission-critical communications such as receipts, fraud detection alerts, multi-factor identity verification, and password resets.

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.

FastConnect
FastConnect allows customers to create a dedicated, private connection between their resources and Oracle Cloud Infrastructure. FastConnect provides customers with higher-bandwidth options, and a more reliable and consistent networking experience. With FastConnect, customers can choose to use private peering, public peering, or both.

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

Full Stack Disaster Recovery (from October 25, 2022)
Full Stack Disaster Recovery (FSDR) is an Oracle Cloud Infrastructure 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 fully-managed, multi-tenant, highly scalable, on-demand, Functions-as-a-Service platform. It runs on a serverless and elastic architecture, which means there’s no infrastructure administration or software administration for customers to perform. It is based on the Fn Project. Fn Project is an open source, container native, serverless platform that can be run anywhere – any cloud or on-premises. Functions allows customers to write code in Java, Python, Node, Go, and Ruby. Customers can deploy their code, call it directly or trigger it in response to events, and get billed only for the resource consumed during the execution.

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

Fusion Applications as a Service
Fusion Applications as a Service (FAaaS) provides self-service management of the environments where customers provision, run, and maintain their Fusion Applications. FAaaS databases are managed by Oracle and utilize the Exadata Cloud Service.

When a customer subscribes to Fusion Applications, for features that are available in FAaaS, they are allotted one production environment and one test environment, and 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 is a logical
grouping of environments set up to facilitate management of the related environments. 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. When a customer creates an environment, they can configure some options specifically for each environment in the family, including some maintenance schedule options, language packs, and network access control rules. After the customer creates an environment, they can manage the lifecycle of the environment, including:

- View metrics and availability,
- Get detailed information about upcoming scheduled maintenance,
- Monitor maintenance in progress,
- Manage other services that are integrated with the customer’s Fusion Applications environment,
- Refresh test and development environments, and
- Edit options such as language packs, network access control rules, and some maintenance schedule settings.

**GoldenGate**

GoldenGate helps customers move data in real-time, at scale, from one or more data management systems to Oracle Cloud databases. GoldenGate enables customers to 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 customers 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. By using Health Checks, customers can be made aware immediately of any availability issue affecting their customers. Key components used in creating a health check include monitors, on-demand probes, vantage points, and protocols.

**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. IAM allows customers to control access to their cloud resources. Customers can control what type of access a group of users have and to which specific resources. IAM can be used with identity domains or without.

**Integration**

Integration allows customers to integrate their cloud and on-premises applications, gain insight into their business processes, and use a Secure File Transfer Protocol (SFTP) compliance file server to store and retrieve files.

**Java Management**

Java Management Service (JMS) is a reporting and management infrastructure integrated with Oracle Cloud Infrastructure Platform services. It allows customers to observe and manage their use of Java SE (on-premise or in the Cloud). Customers can use insights from JMS to optimize workloads across their enterprise (desktop, server, cloud); and protect their Java SE investments by identifying outdated Java installations, unauthorized applications, and Java runtime and application mismatches.

**Language**

Language allows customers to perform sophisticated text analysis at scale. Using the pretrained and custom models, customers 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. Customers 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 is a free, opt-in service that allows customers to bring their own licenses (BYOL) into Oracle Cloud Infrastructure. It can be used to:

- Automate the license portability rules, such as creating BYOL Oracle Database resources (e.g., Autonomous Database), to eliminate overhead for Software Asset Managers (SAMs) and for developers in an enterprise.
• Centrally track license usage for Oracle Database products or third-party products by Compute resources.
• Monitor BYOL resources that have licensing needs, by managing a list of email addresses to be notified about the expiration or over-subscription of licenses.

Load Balancer
Load Balancer (formerly known as Load Balancing) service 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 customer’s choice of a public or private IP address, and provisioned bandwidth.

Logging
Logging service provides a highly scalable and fully managed single interface for all the logs in the tenancy. Customers can use Logging to access logs from all Oracle Cloud Infrastructure resources, as well as enable, manage, and search them.

Logging Analytics
Logging Analytics allows customers to index, enrich, aggregate, explore, search, analyze, correlate, visualize and monitor all log data from customers’ applications and system infrastructure on cloud or on-premises.

Managed Access
Oracle Managed Access enables customers to 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 Access:

• Provides the operator temporary user credentials for a specific duration,
• Specifies the access level for the representative, and
• Creates logs of all actions, providing an audit trail.

Management Agent
Management Agent provides low latency interactive communication and data collection between Oracle Cloud Infrastructure and any other targets.

Marketplace – Consumer
Marketplace is an online store that offers solutions specifically for customers of Oracle Cloud Infrastructure. In the Oracle Cloud Infrastructure Marketplace catalog, the customer can find listings for two types of solutions from Oracle and trusted partners: images and stacks. These listing types include different categories of applications. Also, some listings are free, and others require payment.

Images are templates of virtual hard drives that determine the operating system and software to run on an instance. The customer can deploy image listings on an Oracle Cloud Infrastructure Compute instance.

Stacks represent definitions of groups of Oracle Cloud Infrastructure resources that customers can act on as a group. Each stack has a configuration consisting of one or more declarative configuration files. With an image or a stack, the customer has a customized, more streamlined way of getting started with a publisher’s software. Solutions offered on the Marketplace are not included in the scope of this report.

Monitoring
Monitoring allows customers to monitor their cloud resource using the Metrics and Alarms features actively and passively. Monitoring uses metrics to monitor resources and alarms to notify customers when those metrics meet alarm-specified triggers. The Metrics feature relays metric data about the health, capacity, and performance of customers’ cloud resources. The Alarms feature publishes alarm messages to configured destinations such as topics in the Notifications service and streams in Streaming service.
MySQL Database
MySQL Database enables customers to:
- Instantly provision MySQL instances and connect to a production ready, pre-configured MySQL database.
- Automate database specific tasks such as configuration, security patching, backup, and monitoring.
- Choose from multiple compute shapes depending on their application and capacity requirements.
- Provision fast, reliable, and secure cloud storage for all enterprise workloads from high performance local SSD to extremely durable and cost-effective archive.
- Enable fast, predictable networking with end-to-end network security including a Virtual Cloud Network.
- Monitor the health of resources, optimize performance of applications, and respond to anomalies in real time.
- MySQL database backups are performed and retained in-line with the schedule configured by customers.

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 managed network firewall and intrusion detection and prevention service for customers' Oracle Cloud Infrastructure virtual cloud network (VCN), powered by Palo Alto Networks®. The Network Firewall service offers simple setup and deployment and gives customers visibility into traffic entering the cloud environment as well traffic between subnets.

Network Load Balancer
Network Load Balancers provide automated traffic distribution from one entry point to multiple servers in a backend set. Network Load Balancers help customers ensure that services remain available by directing traffic only to healthy servers.

Network Path Analyzer
Network Path Analyzer (NPA) provides a unified and intuitive capability customers 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:

Dynamic Host Configuration Protocol Options
Configuration information that is automatically provided to the instances when they boot up.

Dynamic Routing Gateway
Dynamic Routing Gateway (DRG) is an optional virtual router that a customer can add to their VCN. Provides a path for private network traffic between the customer VCN and on-premises network.

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

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

Network Address Translation Gateway
Network Address Translation (NAT) Gateway is an optional virtual router that a customer 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.
Private and Public IP
Each VCN has a primary private IPv4 address, and the customer can add secondary private IPs. The customer can optionally assign a public IP to their instances or other resource that have a private IP. Oracle supports dual-stack IPv4/IPv6 addressing for VCNs. Every VCN always supports IPv4, and customers can optionally enable IPv6 during VCN creation.

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

Remote Peering Gateway
Remote Peering Gateway (RPG) lets customers peer one VCN to another VCN in a different region.

Route Tables
Virtual route tables for the customer’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 the customer’s VCN that specify the types of traffic (protocol and port) allowed in and out of the instances. The customer can designate whether a given rule is stateful or stateless. To implement security rules, the customer can use network security groups or security lists.

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

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 Cloud Network
A virtual cloud network (VCN) is a virtual, private network that the customer sets up in Oracle data centers. A VCN resides in a single Oracle Cloud Infrastructure region and covers one or more CIDR blocks (IPv4 and IPv6, if enabled), of the customer’s choice.

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.

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 customers know when something happens with their resources in Oracle Cloud Infrastructure. Using alarms, event rules, and service connectors, customers can get human-readable messages through supported endpoints, including email and text messages (SMS). Customers can also automate tasks through custom HTTPS endpoints and Oracle Cloud Infrastructure Functions.
**Object Storage**
Object Storage allows customers to store an unlimited amount of unstructured data regardless of 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.

**Operations Insights**
Operations Insights provides 360-degree insight into the resource utilization and capacity of databases and hosts. Customers can easily analyze CPU and storage resources, forecast capacity issues, and proactively identify SQL performance issues across their database fleet.

**Operator Access Control**
Operator Access Control enables customers to grant, audit, and revoke the access Oracle has to their infrastructure administered by Oracle, and to obtain audit reports of all actions taken by a human operator, in a near real-time manner. Operator Access Control enables customers to maintain close management and audit trails of all actions that an Oracle operator performs on the infrastructure.

**Oracle Database Service for Azure**
Oracle Database Service for Azure (ODSA) is an Oracle managed service delivering Oracle Database services in OCI directly to Microsoft Azure customers through the OCI Azure Interconnect, a capability available between the two cloud environments in regions located around the world. Though ODSA databases reside in OCI, Azure administrators and developers work mainly in Azure, connecting their applications to Oracle databases using Microsoft’s Azure ExpressRoute, Azure’s standard way of exposing Azure resources to applications. On the other hand, OCI resources are connected to Azure using the OCI FastConnect service. Together, ExpressRoute and FastConnect are referred to as OCI Azure Interconnect.

**Oracle Ksplice**
Oracle Ksplice allows Oracle Linux customers 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. As there are other errata updates and bug fixes, customers should continue to apply updates to their entire system at regular intervals based on their organization’s best practices.

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

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

**OS Management**
OS Management allows customers to manage and monitor updates and patches for the operating system environment on their Oracle Cloud Infrastructure instances, as well as allowing customers to provide options for discovering and monitoring resources on their instances.

**Process Automation**
Process Automation is used to rapidly design, automate, and manage business processes in a collaborative manner using a Low Code web-based declarative environment. Key capabilities include structured and dynamic process modeling, decision modeling, connectivity to outside apps and integrations, web forms, and use task management and tracking. Process Automation is an internal Oracle service.
Recovery Database Service
Recovery Database Service simplifies database backup management and provides enhanced data protection to Oracle Cloud Databases. It provides customers with options to preserve backups before terminating a database, as well as supports data recovery from accidental or malicious damages.

Registry
Registry allows customers to store, share, and manage development artifacts like Docker images. Registry can be used by customers as a private Docker registry for internal use, pushing and pulling Docker images to and from the Registry using the Docker V2 API and the standard Docker command line interface (CLI). Customers can also use Registry as a public Docker registry, enabling any user with internet access and knowledge of the appropriate URL to pull images from public repositories in Registry.

Resource Manager
Resource Manager allows customers to automate the process of provisioning their Oracle Cloud Infrastructure resources. It helps customers install, configure, and manage resources using the “infrastructure-as-code” model. Resource Manager uses Terraform to codify the customer’s infrastructure in declarative configuration files.

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.

Roving Edge Infrastructure is the extension of your Oracle Cloud Infrastructure tenancy. Customers can request to have virtual machines and objects from their tenancy loaded onto Oracle Cloud Infrastructure devices and device clusters by creating and configuring device nodes and cluster resources in Oracle Cloud Infrastructure. These nodes and clusters function as requests for the corresponding devices and indicate what Oracle Cloud Infrastructure-based content is to be pre-loaded or provisioned on them. Customers can synchronize their object storage datasets with their Oracle Cloud Infrastructure tenancy after establishing an internet connection between the Roving Edge Device (RED) and the customer’s Oracle Cloud Infrastructure region.

Search
Search allows customers to find resources within a tenancy, pages of the Console within services, and documentation within the Oracle Cloud Infrastructure Getting Started Guide and Oracle Cloud Infrastructure User Guide. Results are sorted by resource, service, or documentation, helping customers avoid navigating through menus, the latency associated with loading a long list of results onto a single page, or the inconvenience of viewing a long list that spans multiple pages. Customers can also filter results by criteria specific to the search category after results are found and sorted by category.

Search with OpenSearch
Search with OpenSearch is a managed service that allows customers 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. This allows customers to focus resources on building features for their OpenSearch solutions.

Security Zones
Security Zones give customers the confidence that their resources in Oracle Cloud Infrastructure, including Compute, Networking, Object Storage, and Database resources, comply with their security principles.

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

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

**Service Mesh**

Service Mesh allows customers 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. With a service mesh, customer can automatically add features to their cloud native microservice application, which will enable the customer to manage security, control traffic, and add observability features without changing their application's source code.

**Site-to-Site VPN**

Site-to-Site VPN (formerly known as VPN Connect) provides customers with a site-to-site IPSec connection between their 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. Site-to-Site VPN was previously referred to as VPN Connect and IPSec VPN.

**Speech**

Speech is an Automatic Speech Recognition (ASR) system with pre-trained acoustic and language models. Speech can transcribe customer service calls, automate subtitling, and generate metadata for media assets to create a fully searchable archive. Customers can use the Speech service to convert media files to readable text that is stored in JSON and SRT format.

**Stack Monitoring**

Stack Monitoring allows customers 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. These status and performance metrics are stored and provided to customers to troubleshoot performance issues or errors at the application layer and the underlying components of the stack.

**Status**

Status provides dashboards to customers to view the status of Oracle Cloud Infrastructure services in a region, which allow customers to query service status programmatically. There is a dashboard for commercial regions and a dashboard for government regions.

**Streaming**

Streaming provides scalable and durable storage solution for ingesting and consuming high-volume streams in real time. It can be used for messaging, metrics and log ingestion, web or mobile activity data ingestion, infrastructure and app event processing, or other use cases in which data is produced and processed continually and sequentially in a publish-subscribe messaging model.

**Tagging**

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

**Threat Intelligence**

Threat Intelligence aggregates threat intelligence data across many different sources and manages this data to provide actionable guidance for threat detection and prevention in Oracle Cloud Guard and other Oracle Cloud Infrastructure services. This service provides insights from Oracle security researchers, our own unique telemetry, open-source feeds such as abuse.ch and Tor exit relays, and third-party partners. It can help customers detect potentially malicious activities, prioritize alerts, and assess their security posture.
Vault
Vault allows customers to centrally manage the encryption keys that protect their data and the secret credentials that they use 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.

Vision
Vision is a serverless, multi-tenant service, accessible using the Console, REST APIs, SDK, or CLI. Customers can upload images to detect and classify objects in them. If a customer has lots of images, the customer can process them in batch using asynchronous API endpoints. Vision's features are thematically split between Document AI for document-centric images, and Image Analysis for object and scene-based images. Pretrained models and custom models are supported.

Visual Builder Cloud
Visual Builder Cloud service is a visual and declarative cloud environment for developing and hosting engaging mobile and web applications. Oracle Visual Builder Cloud Service provides easy access to data from any REST-based service and enables the creation of custom reusable business objects for storing and managing data. Using the cloud-based visual development tools, customers can create and test responsive web applications and native mobile apps without the need to install any additional software.

Visual Builder Studio
Visual Builder Studio is an application development platform service that helps customers plan and manage work through all stages of the application development lifecycle: design, build, test, and deploy. Visual Builder Studio enables developers to easily deploy their applications to their preferred target.

VMware Solution
VMware Solution allows customers to create and manage VMware enabled software-defined data centers (SDDCs) in Oracle Cloud Infrastructure. VMware Solution gives customers full access to the features of a VMware SDDC, along with the following benefits: high availability, scalability, lift and shift, full integration, manageability, and layer 2 networking.

Vulnerability Scanning
Vulnerability Scanning helps customers improve their security posture in Oracle Cloud by routinely checking hosts for potential vulnerabilities. The service generates reports with metrics and details about these vulnerabilities.

Web Application Acceleration
Web Application Acceleration can be 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. WAF protects customers with the ability to create and manage rules for internet threats including Cross-Site Scripting (XSS), SQL Injection and other Open Web Application Security Project (OWASP)-defined vulnerabilities. Unwanted bots can be mitigated while tactically allowed desirable bots to enter. Access rules can limit based on geography or the signature of the request.

Relevant Aspects of the Control Environment

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

Commitment to Integrity and Ethical Values

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

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

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

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

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

Oversight Responsibility of the Board of Directors

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

Oracle Legal reviews the profiles of Board members to ensure the board and committee members meet current regulatory and internal requirements, including independence and expertise.
Oracle maintains, and distributes externally via its website, its Corporate Governance Guidelines as well as charters for its Finance and Audit Committee, Independent Committee, Compensation Committee, and Nomination and Governance Committee.

**Assignment of Authority and Responsibility**

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

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

<table>
<thead>
<tr>
<th>SECURITY GROUP</th>
<th>ROLES AND RESPONSIBILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Information Security</td>
<td>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.</td>
</tr>
<tr>
<td>Global Product Security</td>
<td>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.</td>
</tr>
<tr>
<td>Global Physical Security</td>
<td>Responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle’s employees, facilities, business enterprise, and assets.</td>
</tr>
<tr>
<td>Global Trade Compliance</td>
<td>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.</td>
</tr>
<tr>
<td>Business Assessment and Audit</td>
<td>Oracle’s Business Assessment &amp; Audit (BA&amp;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&amp;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.</td>
</tr>
</tbody>
</table>

**Commitment to Competence**

Oracle Cloud Infrastructure’s commitment to employee competence begins with formal hiring practices designed to help ensure that new employees are qualified for their job responsibilities. The hiring process also includes a robust background check, performed on candidates selected for hire, in accordance with local laws and regulations, and local Oracle policy.
New employees are supported by a new hire web site and orientation courses. Ongoing training is available to all employees through a variety of courses delivered through web learning and external courses. Training for each employee is tailored to support his or her job role.

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

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

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

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

**Accountability**

Oracle Cloud Infrastructure’s commitment to an effective system of internal control begins with the Oracle Board of Directors and Finance and Audit Committee. The primary functions of the Finance and Audit Committee (the “Committee”) are to assist the Board of Directors (the “Board”) of Oracle Corporation with the Board’s oversight of: management’s conduct of the Corporation’s financial accounting and reporting processes; the integrity of the Corporation’s financial statements; the Corporation’s compliance with legal and regulatory requirements; its independent registered public accounting firm’s qualifications, performance and independence; the performance of the Corporation’s internal audit function; and the evaluation of merger and acquisition transactions and investment transactions proposed by the Corporation’s management. The Finance and Audit Committee holds regular meetings as necessary, but not less than quarterly, and special meetings as may be called by the Chairman of the Committee.

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

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

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

MyOracle Support

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

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

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

External Communication


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. 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. 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.

Security Practices

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

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

Data Classification

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

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

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

The Oracle Cloud Infrastructure Global Enterprise Risk team is responsible for identifying, analyzing, measuring, mitigating/responding to, and monitoring risk specific to the Oracle Cloud Infrastructure organization. In accordance with the Cloud Compliance Standard for Risk Management, risk assessments are performed annually across Oracle Cloud Infrastructure to identify threats and risks that could impact the security, confidentiality, or availability of the system. The risk assessment is modeled after National Institute of Standards and Technology (NIST) Special Publication 800-30 Rev. 1 guidelines and incorporates risk assessment requirements from the ISO/IEC 27001:2013 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 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 27001:2013.
ATTACHMENT B – PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Overview

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

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

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

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

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

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