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, 2019, to March 31, 2020

Prepared in Accordance with AICPA Standard SSAE No.18

Copyright © 2020, Oracle and/or its affiliates
Table of Contents

Section I – Report of Independent Accountants 2

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 5

Attachment A – Description of Oracle Cloud Infrastructure’s System 7
  Oracle Corporation Overview 7
  Oracle Cloud Infrastructure Overview 7
  Relevant Aspects of the Control Environment 16
  Information and Communication 18
  Risk Assessment 19
  Monitoring 19
  Complementary User Entity Controls (CUECS) 20

Attachment B – Principal Service Commitments and System Requirements 21
  Overview 21
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’s Cloud Infrastructure System Based on the Trust Services Criteria for Security, Availability, and Confidentiality” (Assertion), that Oracle Cloud Infrastructure’s controls over the Oracle Cloud Infrastructure System were effective throughout the period October 1, 2019 to March 31, 2020, 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:

- Archive Storage
- Audit
- Block Volume
- Compute
- Container Engine for Kubernetes
- Data Transfer
- Database - Bare Metal
- Database - Exadata
- Database - Virtual Machine
- Distributed Denial of Service (DDoS) Protection
- Digital Assistant
- Email Delivery
- Events
- FastConnect
- File Storage
- Functions
- Health Checks
- Identity and Access Management (IAM)
- Key Management
- Load Balancing
- Monitoring
- Networking: Virtual Cloud Network (VCN)
- Notifications
- Object Storage
- Registry
- Resource Manager
- Streaming
- Web Application Firewall (WAF) (from February 1, 2020)

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

Commercial Regions
- Australia East, Sydney, Australia
- Australia Southeast, Melbourne, Australia (from February 1, 2020)
- Brazil East, Sao Paulo, Brazil
- Canada Southeast, Toronto, Canada
- Germany Central, Frankfurt am Main, Federal Republic of Germany
- India West, Mumbai, India
- Japan Central, Osaka, Japan (from January 24, 2020)
- Japan East, Tokyo, Japan
- Netherlands Northwest, Amsterdam, Netherlands (from February 1, 2020)
- Saudi Arabia West, Jeddah, Saudi Arabia (from February 1, 2020)
- South Korea Central, Seoul, Republic of Korea
- Switzerland North, Zurich, Switzerland
- United Kingdom South, London, United Kingdom
- United States East, Ashburn, Virginia, United States
- United States West, Phoenix, Arizona, United States

**Government regions**

- United Kingdom Government South, London, United Kingdom (from November 30, 2019)
- 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

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

- Bangalore, India
- Dublin, Ireland
- Hyderabad, India
- Kaunas, Lithuania
- Nashua, New Hampshire, United States
- Seattle, Washington, United States

(collectively, the “System”).

The Assertion also indicates that Oracle Cloud Infrastructure’s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Oracle Cloud Infrastructure’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

**Management’s Responsibilities**

Oracle Cloud Infrastructure’s management is responsible for its assertion, selecting the trust services categories and associated criteria on which the 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 our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our 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. 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.

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 management assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria, if the user entity controls assumed in the design of Oracle Cloud Infrastructure's controls operated effectively throughout the period October 1, 2019 to March 31, 2020.

Ernst & Young LLP

May 15, 2020
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:

- Archive Storage
- Audit
- Block Volume
- Compute
- Container Engine for Kubernetes
- Data Transfer
- Database – Bare Metal
- Database – Exadata
- Database – Virtual Machine
- Distributed Denial of Service (DDoS) Protection
- Digital Assistant
- Email Delivery
- Events
- FastConnect
- File Storage
- Functions
- Health Checks
- Identity and Access Management (IAM)
- Key Management
- Load Balancing
- Monitoring
- Networking: Virtual Cloud Network (VCN)
- Notifications
- Object Storage
- Registry
- Resource Manager
- Streaming
- Web Application Firewall (WAF) (from February 1, 2020)

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

Commercial regions:

- Australia East, Sydney, Australia
- Australia Southeast, Melbourne, Australia (from February 1, 2020)
- Brazil East, Sao Paulo, Brazil
- Canada Southeast, Toronto, Canada
- Germany Central, Frankfurt am Main, Federal Republic of Germany
- India West, Mumbai, India
- Japan Central, Osaka, Japan (from January 24, 2020)
- Japan East, Tokyo, Japan
• Netherlands Northwest, Amsterdam, Netherlands (from February 1, 2020)
• Saudi Arabia West, Jeddah, Saudi Arabia (from February 1, 2020)
• South Korea Central, Seoul, Republic of Korea
• Switzerland North, Zurich, Switzerland
• United Kingdom South, London, United Kingdom
• United States East, Ashburn, Virginia, United States
• United States West, Phoenix, Arizona, United States

Government regions:
• United Kingdom Government South, London, United Kingdom (from November 30, 2019)
• 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

and office facilities and security/network operating centers in the following locations:
• Bangalore India
• Dublin, Ireland
• Hyderabad, India
• Kaunas, Lithuania
• Nashua, New Hampshire, United States
• Seattle, Washington, United States

(collectively, the “System”).

In designing the controls over the System we determined that certain trust services criteria can be met only if complementary user entity controls are suitably designed and operating effectively for the period October 1, 2019 through March 31, 2020.

We assert that the controls over the system were effective throughout the period October 1, 2019 to March 31, 2020, 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, if user entities applied the complementary user entity controls assumed in the design of Oracle Cloud Infrastructure’s controls throughout the period October 1, 2019 to March 31, 2020.
ATTACHMENT A – DESCRIPTION OF ORACLE CLOUD INFRASTRUCTURE’S SYSTEM

Oracle Corporation Overview
Oracle Corporation provides products and services that address all aspects of corporate information technology (IT) environments—applications, platform, and infrastructure. Our applications, platform, and infrastructure offerings are delivered to customers worldwide through a variety of flexible and interoperable IT deployment models—cloud-based, on-premise, or hybrid—that enable customer choice and flexibility. Oracle markets and sells its offerings globally to businesses of many sizes, government agencies, educational institutions, and resellers with a worldwide sales force positioned to offer the combinations that best meet customer needs.

Oracle's cloud offerings provide a comprehensive and fully integrated stack of applications, platform, compute, storage, and networking services in all three primary layers of the cloud: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Oracle's Cloud SaaS, PaaS, and IaaS offerings (collectively, “Oracle Cloud Services”) integrate software, hardware, and services on the customers’ behalf within IT environments that are deployed, supported, and managed for the customer. Oracle's integrated Oracle Cloud Services are designed to be rapidly deployable to accelerate customers toward innovation; simplify maintenance to reduce integration and testing work; deployment model agnostic to enable interchangeability and extendibility between IT environments; compatible with other environments to allow movement of workloads to and from the Oracle Cloud; scalable to lower upfront customer investment; secure; standards-based; and reliable. As a leader in the core technologies of cloud IT environments—database and middleware software, enterprise applications, virtualization, clustering, large-scale systems management, and related infrastructure—Oracle's products and services are the building blocks of its Oracle Cloud Services, its partners’ cloud services, and its customers’ cloud IT environments.

Oracle's cloud license and on-premise license deployment models include Oracle Applications, Oracle Database, and Oracle Fusion Middleware software offerings, among others. Customers deploy these offerings using IT infrastructure from the Oracle Cloud or from their own cloud-based or on-premise IT environments. Most customers choose to purchase license support contracts when they purchase a license. Our hardware products include Oracle Engineered Systems, servers, storage, and industry-specific products, and customers generally opt to purchase hardware support contracts when they make a hardware purchase.

Providing choice and flexibility to its customers as to when and how they deploy Oracle applications, platform and infrastructure technologies is an important element of Oracle's corporate strategy. We believe that offering customers broad, comprehensive, flexible, and interoperable deployment models for applications, platform, and infrastructure technologies is important to our growth strategy and better addresses customer needs relative to our competitors, many of whom provide fewer offerings and more restrictive deployment models.

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 offers high-performance compute capabilities (as physical hardware instances) and storage capacity in a flexible overlay virtual network that is securely accessible from customer on-premise networks.

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

Key Concepts and Terminology

Regions and Availability Domains
The Oracle Cloud Infrastructure System is hosted physically in regions and availability domains. A region is a geographic area, composed of one or more availability domains, which are the data centers within a region. Oracle Cloud Infrastructure resources are either region-specific, such as a Virtual Cloud Network (VCN), or availability domain-specific, such as a compute instance.

Availability domains are logically and physically isolated from each other, fault tolerant, and designed not to be impacted by the failure of another availability domain. Availability domains within the same region are interconnected by a low-latency, high-bandwidth network, which makes it possible for the customer to build replicated systems in multiple availability domains for both high-availability and disaster recovery.
Realm

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 Oracle Cloud Infrastructure currently offers a realm for commercial regions, United States Government Cloud regions, United States Department of Defense (DoD) Cloud regions, and United Kingdom Government Cloud region.

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>OCI</td>
<td>1</td>
</tr>
<tr>
<td>Australia Southeast (Melbourne)</td>
<td>ap-melbourne-1</td>
<td>Melbourne, Australia</td>
<td>MEL</td>
<td>OCI</td>
<td>1 – from February 1, 2020</td>
</tr>
<tr>
<td>Brazil East (Sao Paulo)</td>
<td>sa-saopaulo-1</td>
<td>Sao Paulo, Brazil</td>
<td>GRU</td>
<td>OCI</td>
<td>1</td>
</tr>
<tr>
<td>Canada Southeast (Toronto)</td>
<td>ca-toronto-1</td>
<td>Toronto, Canada</td>
<td>YYZ</td>
<td>OCI</td>
<td>1</td>
</tr>
<tr>
<td>Germany Central (Frankfurt)</td>
<td>eu-frankfurt-1</td>
<td>Frankfurt, Germany</td>
<td>FRA</td>
<td>OCI</td>
<td>3</td>
</tr>
<tr>
<td>India West (Mumbai)</td>
<td>ap-mumbai-1</td>
<td>Mumbai, India</td>
<td>BOM</td>
<td>OCI</td>
<td>1</td>
</tr>
<tr>
<td>Japan Central (Osaka)</td>
<td>ap-osaka-1</td>
<td>Osaka, Japan</td>
<td>KIX</td>
<td>OCI</td>
<td>1 – from January 24, 2020</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>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>Netherlands Northwest</td>
<td>eu-amsterdam-1</td>
<td>Amsterdam, Netherlands</td>
<td>AMS</td>
<td>OC1</td>
<td>1 – from February 1, 2020</td>
</tr>
<tr>
<td>(Amsterdam)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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 – from February 1, 2020</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>Switzerland North (Zurich)</td>
<td>eu-zurich-1</td>
<td>Zurich, Switzerland</td>
<td>ZHR</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>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>US West (Phoenix)</td>
<td>us-phoenix-1</td>
<td>Phoenix, Arizona, US</td>
<td>PHX</td>
<td>OC1</td>
<td>3</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 region 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, United Kingdom</td>
<td>LTN</td>
<td>OC4</td>
<td>1 – from November 30, 2019</td>
</tr>
</tbody>
</table>

**Console**

Customers can access Oracle Cloud Infrastructure using the Console (a browser-based interface), the representational state transfer application programming interface (REST API), or through various Java and Ruby Software Development Kits (SDKs). The Console is a simple and intuitive web-based user interface that customers use to access and manage Oracle Cloud Infrastructure.

**Tenancy**

For each customer, Oracle creates a tenancy, which is a secure and isolated partition within Oracle Cloud Infrastructure where the customer can create, organize, and administer their cloud resources.

**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 is accessible only by groups that have been given permission by an administrator. A compartment is a logical group and not a physical container.

**Virtual Cloud Network**

A VCN is a virtual version of a traditional network—including subnets, route tables, and gateways—on which Oracle Cloud Infrastructure instances run. A cloud network resides within a single region but can cross multiple availability domains. A VCN may contain multiple subnets, and each subnet must belong to a single availability domain. The customer may configure a cloud network with an Internet gateway to handle public traffic and with an optional IPsec VPN connection to securely extend the customer’s on-premises network.

**Instances**

Oracle Cloud Infrastructure offers both bare metal and virtual machine (VM) instances.

Oracle Cloud Infrastructure Bare Metal Hosts provide customers with control of the physical host (i.e., bare metal) machine. Bare metal compute instances run directly on bare metal servers without a hypervisor. When a customer provisions a bare metal compute instance, they maintain control of the physical central processing unit (CPU), memory, and network interface card (NIC). The customer can configure and use the full capabilities of each physical machine as if it were hardware running in their own data center. Customers do not share the physical machine with any other tenants.

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.

**Image**

The image is a template on a virtual hard drive that defines the operating system and other software for an instance. Oracle provides a set of images that the customer can use when launching a new instance. The customer 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.

**Shape**

For Oracle Cloud Infrastructure Compute, the shape specifies the number of CPUs (virtual or physical) and amount of memory allocated to the instance.
For Oracle Cloud Infrastructure Load Balancing, the shape determines the load balancer's total pre-provisioned maximum capacity (i.e., bandwidth) for ingress and egress.

**Key Pair**
The instance secure shell (SSH) SSH Key pair is used to establish SSH connection to an instance. When a customer provisions an instance, they provide the public key, which is saved to the instance's authorized key file. To log on to the instance, the customer provides their private key, which is verified with the public key.

**Bucket**
A bucket is a logical container used by Object Storage for storing data and files. A bucket can contain an unlimited number of objects.

**Oracle Cloud Identifier**
Every Oracle Cloud Infrastructure resource is assigned a unique Oracle Cloud Identifier (OCID). The OCID is part of the resource's information in both the Console and API.

**Replication**
Oracle Cloud Infrastructure does not offer backup, replication, or recovery as a service. Customers are responsible for implementing a backup and/or replication process in line with their requirements and policies.

Customers are advised to design their architecture in a manner that replicates or backs up their data to multiple availability domains and/or regions as appropriate for their needs and for compliance with applicable internal policies, laws and regulations.

Oracle uses industry-standard, enterprise-grade protection for block volumes, files, and objects. Oracle Cloud Infrastructure Storage keeps multiple copies of objects on different nodes within a region and periodically checks them to help ensure data integrity. Oracle provides application-level capabilities to protect against outages through technologies such as Oracle Data Guard, which replicates databases in real time to different locations and Oracle Real Application Clusters (RACs).

**Service Descriptions**
The scope of this report includes the controls placed in operation specifically for the following Oracle Cloud Infrastructure services to meet the Trust Services Criteria related to security, availability, and confidentiality. These criteria are set forth in TSP section 100, 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 both the contractual agreement with and the services provisioned by each individual customer.

**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 Key Management service.

**Audit**
Audit provides the customer with comprehensive visibility into their Cloud Infrastructure. Audit automatically records calls to all supported Oracle Cloud Infrastructure API endpoints as log events. Currently, all services support logging by Audit. Customer API calls, including actions from the customer Console, are logged and retained for 90 days.

**Block Volume**
Block Volume allows the customer to dynamically provision and manage block storage volumes. The customer can create, attach, connect, and move volumes as needed to meet storage 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 Key Management service.
Compute
Compute allows customers to provision and manage computer 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.

Container Engine for Kubernetes
Container Engine for Kubernetes allows customers to deploy containerized applications to the cloud. The services 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 for each management and discovery.

Data Transfer
Data Transfer allows the customer to migrate data to Oracle Cloud Infrastructure. Customers can transfer data into a bucket in either the Object Storage service or Archive Storage service. Data files can be sent as files on an encrypted commodity disk or on Oracle-supplied storage appliances to an Oracle transfer site. By default, Data Transfer encrypts data at rest using AES 256-bit encryption.

Database
Database as a Service (DBaaS) consists of databases, compute nodes, and storage services. They can include bare metal, virtual machine, and Exadata database (DB) systems that customers can customize resources and settings. DBaaS systems enable customers to elastically request, provision, instantiate, connect, and manage databases in the cloud.

Database systems are hardware systems provisioned as either dedicated hardware or virtual hardware with embedded software, as though the customer had an on-premises system. Database maintenance, security and the embedded software development practices of the database systems are not in the scope of the Oracle Cloud Infrastructure System. The security controls and services within a database system are described in detail and are made available to the public on the Oracle website.

Bare Metal DB Systems
Oracle Cloud Infrastructure offers 1-node database (DB) systems on bare metal machines. Bare metal DB systems consist of a single bare metal server running Oracle Linux 6.8, with locally attached NVMe storage.

Virtual Machine DB Systems
Oracle Cloud Infrastructure offers 1-node virtual machine DB system consisting of one virtual machine and a 2-node virtual machine RAC DB system consisting of two virtual machines.

Exadata DB Systems
An Exadata DB system consists of a base system, quarter rack, half rack, or full rack of compute nodes and storage servers. Exadata DB systems enable customers to elastically request, provision, instantiate, connect, and manage Exadata machines in the cloud.

The Exadata DB 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. The security controls and services within an Exadata Machine are described in detail and are made available to the public on the Oracle website.
Digital Assistant
Digital Assistant allows the customer 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.

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 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 design DDoS protection mechanisms to meet their requirements.

Email Delivery
Email Delivery is an email sending service that provides a fast and reliable managed solution for sending high-volume emails that need to reach customer recipients’ inboxes. 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 the customer to create automation based on the state changes of resources throughout their tenancy. Customers can use Events to allow their development teams to automatically respond when a resource changes its state.

FastConnect
FastConnect allows the customer to create a dedicated, private connection between their office and/or data center and Oracle Cloud Infrastructure. With FastConnect, customers can choose to use private peering, public peering, or both.

File Storage
File Storage allows the customer to access an unlimited pool of file systems to manage growth of structured and unstructured data. The customer can connect to a File Storage service file system from any bare metal, VM, or container instance in the VCN. The customer can also access a file system from outside the VCN using Oracle Cloud Infrastructure FastConnect and Internet Protocol security (IPSec) virtual private network (VPN). Data stored on File Storage service is encrypted 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 Key Management service.

Functions
Functions is a fully managed, multi-tenant, highly scalable, on-demand, Functions-as-a-Service platform. It is powered by the Fn Project open source engine. Fn Project is an open source, container native, serverless platform that can be run anywhere, 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.

Health Checks
Health Checks allows customers to determine the availability and performance of any publicly facing service, including hosted websites, API endpoints, or externally facing load balances through high frequency external monitoring. 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) allows the customer to control access to their cloud resources, including who has access, what resources they can access, and what type of access they have to the resources. Additionally, the customer can manage complex organizations and rules using logical user groups, logical resource groups, and defined policies.
Key Management

Key Management allows the customer to centrally manage the encryption of their data. The customer can create master encryption keys and data encryption keys, rotate keys to generate new cryptographic material, enable or disable keys for use in cryptographic operations, assign keys to resources, and use keys for encryption and decryption.

Key Management integrates with Object Storage, Block Volume, and File Storage to support encryption at rest of data in buckets, block or boot volumes, and file systems. Integration with IAM allows customers to control who and what services can access which keys and what they can do with those keys. Integration with Audit allows customers to monitor key usage.

Keys are stored on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standard (FIPS) 140-2 Security Level 3 security certification. Key Management uses the AES as its encryption algorithm, and its keys are AES symmetric.

Load Balancing

Load Balancing allows the customer to create a public or private load balancer within their VCN. It provides automated traffic distribution from one entry point to multiple servers within the customer’s VCN based on demand.

Monitoring

Monitoring allows customers to actively and passively monitor their cloud resource using the Metrics and Alarms features. Monitoring uses metrics to monitor resources and alarms to notify customers when those metrics meet alarm-specified triggers. Metrics are emitted to the Monitoring service by resources as raw data points, or timestamp-value pairs, along with dimensions and metadata. Alarms publishes alarm messages to configured destinations managed by the Notifications service.

Networking

The Networking service uses virtual versions of transitional network components.

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 a single, continuous IPv4 CIDR block of the customer 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.

Private and Public IP

Each VNIC has a primary private IPv4 address, and the customer can add a remove 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.

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.

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.

Internet Gateway

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

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 resource to incoming internet connections.
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.

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.

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.

Dynamic Host Configuration Protocol Options

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

Notifications

Notifications broadcasts messages to distributed components through a publish-subscribe pattern, delivering secure, highly reliable, low latency and durable messages for applications hosted on Oracle Cloud Infrastructure and externally. Customers can use Notifications to get notified when alarms are breached.

Object Storage

Object Storage allows the customer to store an unlimited amount of unstructured data regardless of content type. 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 Key Management service.

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 users Terraform to codify the customer’s infrastructure in declarative configuration files, which allows the customer to review and edit, version, persist, reuse, and share them across teams. Customers can then use Resource Manager to provision Oracle Cloud Infrastructure resources using their Terraform configurations.

Streaming

Streaming provides a fully managed, scalable, and durable storage solution for ingesting continuous, high-volume streams of data that the customer can consume and process in real time. It can be used for messaging, ingesting high-volume data such as application logs, operational telemetry, web click-stream data, or other use cases in which data is produced and processed continually and sequentially in a publish-subscribe messaging model.
Web Application Firewall (from February 1, 2020)

Web Application Firewall (WAF) protects applications from malicious and unwanted internet traffic. WAF can protect any internet facing endpoint, providing consistent rule enforcement across the customer’s applications.

WAF protects the customer 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 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.

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

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

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

Oversight Responsibility of the Board of Directors

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

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

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

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

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

<table>
<thead>
<tr>
<th>SECURITY GROUP</th>
<th>ROLES AND RESPONSIBILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Corporate Architect</td>
<td>Reports directly to the Executive Chairman and Chief Technology Officer (CTO), manages the functional departments directly.</td>
</tr>
<tr>
<td>Oracle Security Oversight Committee (OSOC)</td>
<td>Oversees the implementation of Oracle-wide security programs, including security policies and data privacy standards. The committee includes senior management from lines of business and security organizations.</td>
</tr>
<tr>
<td>Oracle Global Information Security (GIS)</td>
<td>Responsible for security oversight, compliance, enforcement, assessment, policy and strategy development, and training and awareness at the corporate level. GIS security policies are available to employees on the GIS Policy Portal. GIS also serves as the primary contact for security incident response, providing overall direction for incident prevention, identification, investigation, and resolution.</td>
</tr>
<tr>
<td>Risk Management for Oracle Cloud Infrastructure</td>
<td>Responsible for incorporating risk management into governance and operations; communicating current, strategic, and emerging risks to operational and leadership teams; identifying and managing risk; advising on best practices; evaluating and advising on risk to relevant teams; designing security strategy; performing architectural review of systems and solutions; conducting threat intelligence; and performing technical assessments of component groups and technologies.</td>
</tr>
<tr>
<td>Legal Security and Privacy</td>
<td>The Oracle Chief Privacy Officer and Oracle Legal Department, working in conjunction with Oracle Security organizations, develop and manage the implementation of and compliance with the Oracle Data Privacy Policies.</td>
</tr>
<tr>
<td>Corporate Security Architecture Review Board (CSARB)</td>
<td>Evaluates proposed corporate strategic projects and initiatives to ensure alignment with Oracle Corporate Security Architecture strategy, direction, and intent as well as Oracle Corporate Security privacy and legal policies, procedures, and standards.</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 Engagement, Onboarding, and Monitoring (EOM) 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 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 are to provide advice with respect to the Corporation’s financial matters; oversee the accounting and financial reporting processes of the Corporation and the audits of the financial statements of the Corporation; assist the Board of Directors in fulfilling its oversight responsibilities regarding finance, accounting, tax, and legal compliance; and evaluate 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 and are available to all personnel.

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

**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


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 product offerings are available to customers, the data gathered by the application 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 their thoughts on company risk.

The Oracle Cloud Infrastructure Engagement, Onboarding, and Monitoring team is responsible for identifying, analyzing, measuring, mitigating/responding to, and monitoring risk specific to the Oracle Cloud Infrastructure organization. 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.

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

Impact of Covid-19 (Corona Virus)

In response to the global Covid-19 pandemic and at the direction of local, state and federal / governmental authorities in the jurisdictions in which we operate, Oracle implemented a work from home policy as of March 2020 for all non-essential
employees and vendors. The architecture of the Oracle Cloud Infrastructure System has been designed in a manner which enables Oracle to continue business as usual operations irrespective of the physical location of employees.

Oracle Cloud Infrastructure data center teams continue to perform and sustain standard operating procedures, as they relate to the controls tested in this audit. Due to the novel coronavirus, where required by local mandates, precautionary measures and limitations have been placed on the number of visitor staff and duration of visits at the data centers. In the event of a procedural impact or modification for the purposes of conforming to the constraints presented by COVID-19, Oracle Cloud Infrastructure data center teams have initiated and executed any required approvals for such exceptions. Critical functions continue to operate.

**Complementary User Entity Controls (CUECS)**

Cloud security is a shared responsibility between a cloud service provider and its customers. Oracle Cloud Infrastructure controls were designed with the assumption that certain controls would be implemented by user entities (or “customers”). Certain requirements can be met only if complementary user entity controls assumed in the design of Oracle Cloud Infrastructure’s controls are suitably designed and operating effectively, along with related controls at Oracle Cloud Infrastructure.
ATTACHMENT B – PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Overview

Oracle designs its processes and procedures to meet its objectives for its 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 state 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.

As an Infrastructure as a Service (IaaS) System, the Oracle Cloud Infrastructure System is designed based on a shared responsibility model where both Oracle and the user entities 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.