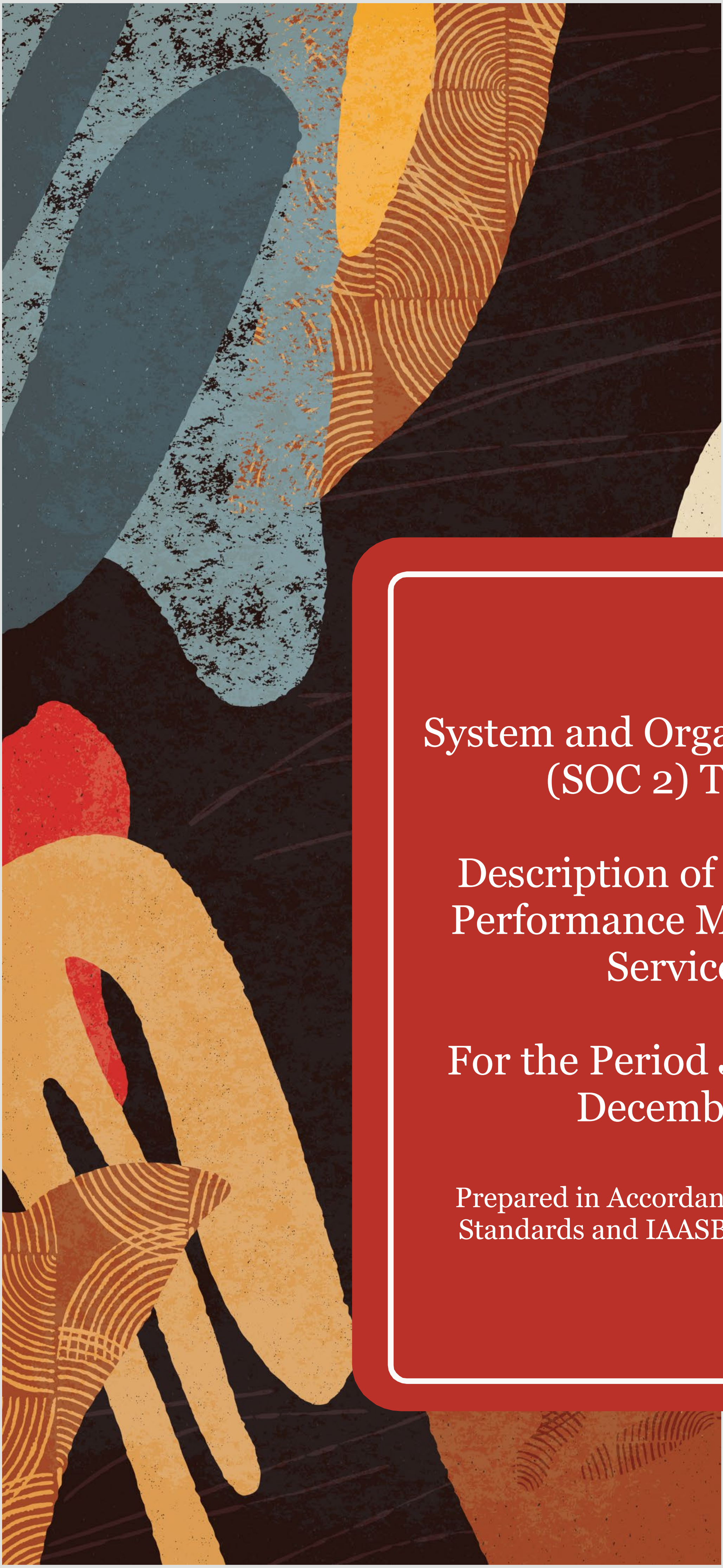

ORACLE

System and Organization Controls 2 (SOC 2) Type 2 Report

Description of Oracle Enterprise Performance Management Cloud Services System

For the Period January 1, 2022 to December 31, 2022

Prepared in Accordance with AICPA Attestation Standards and IAASB Standard ISAE No. 3000

TABLE OF CONTENTS

SECTION I – ORACLE ENTERPRISE PERFORMANCE MANAGEMENT CLOUD SERVICES MANAGEMENT ASSERTION

We have prepared the accompanying "Description of Oracle Enterprise Performance Management Cloud Services System" (Description) of Oracle America, Inc. ("Oracle" or "Service Organization") in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the Oracle Enterprise Performance Management Cloud Services System (System) that may be useful when assessing the risks arising from interactions with the System throughout the period January 1, 2022 to December 31, 2022, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, availability and confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria).

Carved-out component subservice organization: The Oracle Enterprise Performance Management Cloud Services System uses data center hosting services provided by Oracle Cloud Services Data Centers (component subservice organization), a component of Oracle. The Description includes only controls of the System and excludes the controls of the component subservice organization. Certain controls specified by the Oracle Enterprise Performance Management Cloud Services System can be achieved only if complementary subservice organization controls are suitably designed and operating effectively. The Description identifies the types of complementary controls of the component subservice organization that are necessary to achieve certain Oracle's service commitments and system requirements based on the applicable trust services criteria. The scope of this description did not include the complementary controls of the component subservice organization.

Management of the component subservice organization has prepared a separate description of the services used by the System, which includes the aforementioned complementary component subservice organization controls. This Description should be read in conjunction with the separate component subservice organization SOC 2 report.

Carved-out unaffiliated subservice organizations: Oracle also uses Cyxtera, Digital Realty, Etisalat, Equinix, and QTS (unaffiliated subservice organizations) to provide third-party data center hosting services. The Description includes only the controls of Oracle and excludes controls of the unaffiliated subservice organizations. The Description also indicates that certain trust services criteria specified therein can be met only if unaffiliated subservice organizations' controls assumed in the design of Oracle's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of unaffiliated subservice organization.

Complementary user entity controls: The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Oracle's controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to controls of user entities.

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

a. The Description presents the System that was designed and implemented throughout the period January 1, 2022 to December 31, 2022 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of Oracle’s controls throughout the period January 1, 2022 to December 31, 2022.

c. The Oracle controls stated in the Description operated effectively throughout the period January 1, 2022 to December 31, 2022 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of Oracle’s controls throughout the period January 1, 2022 to December 31, 2022.

Building a better
working world

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

Tel: +1 415 894 8000
Fax: +1 415 894 8099
ey.com

SECTION II – INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

To the Management of Oracle America, Inc.

Scope

We have examined Oracle America, Inc.'s ("Oracle" or "Service Organization") accompanying "Description of Oracle Enterprise Performance Management Cloud Services System" (Description) for processing user entities' transactions throughout the period January 1, 2022 to December 31, 2022 in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout January 1, 2022 to December 31, 2022 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for security, availability and confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria).

Carved-out component subservice organization: The Oracle Enterprise Performance Management Cloud Services System uses data center hosting services provided by Oracle Cloud Services Data Centers (component subservice organization), a component of Oracle. The Description includes only controls of the Oracle Enterprise Performance Management Cloud Services System and excludes the controls of component subservice organization. Certain controls specified by Oracle Enterprise Performance Management Cloud Services System can be achieved only if complementary subservice organization controls are suitably designed and operating effectively. The Description identifies the types of complementary controls of the component subservice organization that are necessary to achieve certain Oracle's service commitments and system requirements. The scope of this examination did not include the complementary controls of the component subservice organization.

Management of the component subservice organization has prepared a separate description of the services used by the System, which includes the aforementioned complementary component subservice organization controls. This report should be read in conjunction with the separate component subservice organization SOC 2 report.

Carved-out unaffiliated subservice organizations: Oracle also uses Cyxtera, Digital Realty, Etisalat, Equinix, and QTS (unaffiliated subservice organizations) to provide third-party data center hosting services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Oracle, to achieve Oracle's service commitments and system requirements based on the applicable trust services criteria. The Description presents Oracle's system; its controls; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at unaffiliated subservice organization. Our examination did not extend to the services provided by unaffiliated subservice organizations, and we have not evaluated whether the controls management assumes have been implemented at the unaffiliated subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2022 to December 31, 2022.

Complementary user entity controls: The Description also indicates that Oracle'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'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.

Oracle's responsibilities

Oracle is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved. Oracle has provided the accompanying assertion titled, "Oracle Enterprise Performance Management Cloud Services Management Assertion" (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Oracle is responsible for (1) selecting the trust services criteria applicable to the Description, (2) preparing the Description and Assertion; (3) the completeness, accuracy, and method of presentation of the Description and Assertion; (4) providing the services covered by the Description; (5) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the Service Organization's service commitments and system requirements based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). Our examination was also performed in accordance with the International Standard on Assurance Engagements (ISAE) 3000, Assurance Engagement Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. 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 we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- performing procedures to obtain evidence about whether the controls stated in the Description are presented in accordance with the Description Criteria.
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively based on the applicable trust services criteria.

- testing the operating effectiveness of those controls based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls based on the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested and the nature, timing, and results of those tests are listed in the accompanying "Section IV – Oracle Enterprise Performance Management Cloud Services System Controls, Test Procedures and Results of Testing" (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

a. the Description presents the Oracle Enterprise Performance Management Cloud Services System that was designed and implemented throughout the period January 1, 2022 to December 31, 2022 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively and if subservice organizations and user entities applied the controls assumed in the design of Oracle's controls throughout the period January 1, 2022 to December 31, 2022.

c. the controls stated in the Description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period January 1, 2022 to December 31, 2022, if subservice organizations and user entity controls assumed in the design of Oracle's controls operated effectively throughout the period January 1, 2022 to December 31, 2022.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Oracle, user entities of Oracle Enterprise Performance Management Cloud Services System during some or all of the period January 1, 2022 to December 31, 2022 and prospective user entities, independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organizations
- How the service organization's system interacts with user entities, subservice organizations, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization's controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst + Young LLP

March 1, 2023

SECTION III – DESCRIPTION OF ORACLE ENTERPRISE PERFORMANCE MANAGEMENT CLOUD SERVICES SYSTEM

BACKGROUND

Oracle provides products and services that address enterprise information technology (IT) environments. The products and services include 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 Oracle Cloud at Customer offering (an instance of Oracle Cloud in a customer's own data center). Accordingly, Oracle offers choice and flexibility to customers and facilitate the product, service and deployment combinations that best suit customers' needs. Customers include businesses of many sizes, government agencies, educational institutions and resellers that Oracle markets and sells to directly through a worldwide sales force and indirectly through the Oracle Partner Network.

Oracle Cloud Software-as-a-Service and Infrastructure-as-a-Service (SaaS and IaaS, respectively, and collectively, Oracle Cloud Services) offerings provide a comprehensive and integrated stack of applications and infrastructure services delivered via a cloud-based deployment model. Oracle Cloud Services integrate the software, hardware and services on a customer's behalf in a cloud-based IT environment that Oracle deploys, upgrades, supports and manages for the customer. 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.

Oracle also offers services to assist 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 the corporate strategy. Oracle believes that offering customers broad, comprehensive, flexible and interoperable deployment models for Oracle applications and infrastructure technologies is important to the growth strategy and better addresses customer needs relative to competitors, many of whom provide fewer offerings, more restrictive deployment models and less flexibility for a customer's transition to cloud-based IT environments.

DESCRIPTION OF SERVICES

Oracle Enterprise Performance Management Cloud (EPM) Service (System) available to customers may include the offerings described below. The actual services provided by Oracle depend on both the contractual agreement and the services provisioned for each customer.

Oracle EPM Cloud Services were designed as an open standards-based business application, making them highly adaptable. The standards-based technology enables businesses to respond effectively to change with flexible, modular, user-driven business software that is powered by business capabilities built on open standards. The EPM Service applications include:

- Oracle Planning and Budgeting Cloud Service (EPM PBCS)
- Oracle Enterprise Performance Reporting Cloud Service (EPM EPRCS)
- Oracle Enterprise Planning and Budgeting Cloud Service (EPM EPBCS)
- Oracle Financial Consolidation and Close Cloud Service (EPM FCCS)
- Oracle Account Reconciliation Cloud Service (EPM ARCS)
- Oracle Enterprise Data Management Cloud Service (EPM EDMCS)
- Oracle Profitability and Cost Management Cloud Service (EPM PCMCS)
- Oracle Tax Reporting Cloud Service (EPM TRCS)

Oracle Planning and Budgeting Cloud Service (EPM PBCS)
Oracle Planning and Budgeting Cloud Service is used to create custom planning and forecasting models or to use purpose-built planning models that include best practice processes, calculations, dashboards, and reports. Users can take advantage of predictive planning to identify and leverage patterns in their financial and operational data to forecast most likely outcomes. Intuitive business wizards allow users to evolve their planning processes as their business changes. Powerful analytics, dashboards, what-if, and predictive capabilities give insight into user's businesses.

Oracle Enterprise Performance Reporting Cloud Service (EPM EPRCS)
EPRCS is part of the Oracle EPM Cloud. The tool is built for comprehensive financial reporting, allowing managers to use data to tell a story and better convey information. EPRCS uses a methodical and collaborative approach to reporting — giving users the ability to define, author, review, and publish reports with relative ease. The owners of the report can easily monitor contributions made by others throughout the reporting lifecycle.

Oracle Enterprise Planning and Budgeting Cloud Service (EPM EPBCS)
EPBCS offers sophisticated modeling and predictive analytical capabilities that allow users to create multiple what-if versions and slice and dice data based on various what-if assumptions. EPBCS also has a rolling forecast wizard that makes it simple to implement a driver-based rolling forecast process.

Key features of EPBCS/Planning in the Oracle EPM Cloud include fully integrated financial statement planning across the income statement, balance sheet, and cash flow; Financial workforce planning for compensation spend by employee and/or job code; pre-built integration to Oracle HCM Cloud and cloud-to-cloud integration to third-party HCM solutions to align workforce and strategic priorities; Project financial planning for project-oriented industries and departments (e.g. IT, Marketing, R&D, etc.); and a Capital asset process for detailed planning on the impact of new and existing assets.

Oracle Financial Consolidation and Close Cloud Service (EPM FCCS)
Financial Consolidation and Close is a purpose-built business process available in the Oracle Fusion Cloud EPM for both effectively and efficiently managing the consolidation and close, end to end. No matter what the size of company, organizations can have 100% confidence in their financial consolidation, close and reporting processes. Financial Consolidation and Close helps ensure that processes are dependable and correct, timely and transparent, streamlined and efficient and compliant and auditable.

Oracle Account Reconciliation Cloud Service (EPM ARCS)
Account Reconciliation is a purpose-built business process available in the Oracle Fusion Cloud EPM designed to manage the global reconciliation process. It provides real-time visibility into the performance of reconciliations, ensuring that all reconciliations prepared are properly qualified. It also helps companies streamline and optimize performance by automating certain reconciliation tasks, including high volume transactional reconciliations and variance analysis. Account Reconciliation includes two modules: Reconciliation Compliance and Transaction Matching.

Oracle Enterprise Data Management Cloud Service (EPM EDMCS)
Oracle Enterprise Data Management Cloud represents connected applications to support dedicated, self-service, and fully integrated business perspectives to support application data management via a single pane of glass. Moreover, administrators can configure highly tailored, fit-for-purpose business perspectives to facilitate cross-application, change management experiences to align changes within a given business domain.

Oracle Profitability and Cost Management Cloud Service (EPM PCMCS)
Profitability and Cost Management, a purpose-built process available in the Oracle Fusion Cloud EPM, provides business users with a solution to automate and take ownership of allocation-based business processes such as customer/product profitability, management allocations, shared service costing, cost transparency initiatives, and legal entity allocations to support operational transfer pricing.

Oracle Tax Reporting Cloud Service (EPM TRCS)
Oracle EPM Tax Reporting provides comprehensive global tax reporting for medium to large multinational companies and includes Tax Provisioning, Country by Country Reporting, Workflow Management, Supplemental Data Management, and Dashboards and Key Performance Indicator reporting.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATION, AND MONITORING

CONTROL ENVIRONMENT

The control environment sets the tone of an organization and influences the overall control awareness. The control environment is embodied by the organization's awareness of the need for controls and the emphasis given to the appropriate controls through management's actions supported by its policies, procedures, and organizational structure. 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.

Oracle is a control conscious organization and has designed controls into its processes supporting the System. Oracle has developed internal standard operating procedures (SOPs) for its business. The SOPs describe the detailed activities and tasks undertaken by Oracle personnel when delivering services to its customers. The SOPs act as part of the control framework, but additionally provide direction for all activities performed. The SOPs are managed centrally and are available to all relevant personnel through the Intranet. The control environment also includes physical data centers used to house the computer systems of Oracle customers.

Policies and Standards

Oracle has developed internal policies that outline the corporate requirements and provide guidance regarding the procedural operation for all aspects of the business including human resources, security, change management, networks, incident management, etc. The policies are managed centrally and are available to all personnel via the corporate intranet.

In addition to corporate policies, Oracle has further designed and implemented a set of specific standards outlining detailed requirements for various processes undertaken and managed by Oracle personnel. These policies and standards form part of the control framework and additionally provide direction for all activities performed. The standards are managed centrally, reviewed at least annually and made available to all relevant personnel through the company's internal corporate network.

Commitment to Integrity and Ethical Values

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

Oracle has a Compliance and Ethics Program that includes a Code of Ethics and Business Conduct (the Code) that defines and implements the company's core values. Core values include integrity, ethics, compliance, mutual respect, teamwork, communication, innovation, customer satisfaction, quality, and fairness. The Code, which applies to all Oracle entities, supplements and in many cases goes beyond what is required to comply with laws and regulations. The Code 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 Code. The Code and the ACP 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 Code of Ethics and Business Conduct. The reporting site allows employees and non-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 are presented to the Finance and Audit Committee with specific reference to those items, including fraud, 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 originates with, and is the responsibility of, the Oracle Board of Directors. The Board of Directors provides oversight of Oracle operations and activities including oversight of the Finance and Audit Committee.

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 on its website Corporate Governance Guidelines, and 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 has developed an organizational structure to meet its needs in support of the control activities. Organizational charts are in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, security, operation, maintenance, and monitoring of the system. The current management structure has adequate diversification 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 are aligned with organizational objectives.

Oracle is supported by the following security groups that provide oversight of internal IT resources and suppliers:

- ***Security Organization***
  The Chief Corporate Architect, who reports directly to the Executive Chairman & Chief Technology Officer (CTO), manages the functional departments directly. The Global Information Security, Global Product Security, Global Physical Security and Oracle Security Architecture departments comprise Oracle Corporate Security, which provides independent security policy, guidance and compliance oversight to Oracle worldwide.
- ***Oracle Security Oversight Committee (OSOC)***
  The OSOC oversees the implementation of Oracle-wide security programs, including security policies and data privacy standards. The Committee is comprised of senior management from Lines of Business and security organizations. OSOC meetings are held at least annually to discuss and review security initiatives and directions.
- ***Oracle Global Information Security (GIS)***
  GIS is responsible for security oversight, compliance, enforcement, conducting information security assessments, leading the development of information security policy and strategy, as well as training and awareness at the corporate level. GIS security policies are available to employees on the GIS Policy Portal. GIS also serves as the primary contact for security incident response, providing overall direction for incident prevention, identification, investigation and resolution.
- ***Privacy and Security Legal***
  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 Oracle Data Privacy Policies.

The security organizations are responsible for administering the following processes to assure that security objectives are met:

- ***Corporate Security Solution Assurance Process***
  Oracle's IT organizations, GIS group and the Corporate Security Architecture group have developed a comprehensive information security management review process called the Corporate Security Solution Assurance Process (CSSAP). CSSAP is endorsed by the OSOC.

  CSSAP integrates three security review processes under a single process umbrella, consistently and transparently addressing corporate security requirements throughout the project life cycle.

  - Corporate Security Architecture Review Board (CSARB) – The objective of CSARB is to evaluate proposed corporate strategic projects and initiatives to help ensure alignment with (i) Oracle Corporate Security Architecture strategy, direction and intent and (ii) Oracle Corporate Security privacy and legal policies, procedures and standards
  - Information Technology Security Technical Review (IT STR) – The objective of IT STR is to evaluate new or changes to existing information technology projects and initiatives to help ensure they comply with Oracle corporate security policies, IT security standards and leading security practices.
  - Security Assessment Service for CSSAP Continuity – The objective of the Security Assessment Service is to validate that: (i) information security and legal controls are implemented according to the specifications reviewed and approved at the CSARB and IT STR, (ii) system or service meets compliance requirements with Corporate Security Policies, GIT Security Standards, Global Product Security and Best Practices and (iii) all security vulnerabilities identified are remediated.

Commitment to Competence
Oracle's commitment to employee competence begins with formal hiring practices designed to ensure that new employees are qualified for their job responsibilities which includes a robust background check. Background checks are 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 course. The orientations are available via a number of formats. Depending on the location, it may be an on-line e-course, a live web broadcast or during face-to-face inductions.

Ongoing training is available to all employees through a variety of courses delivered through web learning, Oracle University and external courses. Training for each employee is tailored to support his or her job role.

Important security information is distributed to key Oracle employees through the Security Aware newsletter. This newsletter is sent quarterly, at a minimum, to Information Security Managers (ISMs) who make the information available to their teams. The content of this communication may include references to new or changed security policies and is also used to emphasize important security matters.

In addition, Oracle conducts an annual appraisal and performance management process for all Oracle employees. The performance management process defines not only what Oracle employees are expected to do, but how work goals should be accomplished (competencies). It specifies what will be measured and how each Oracle employee's work fits into the larger business context.

Accountability
Oracle's commitment to an effective system of internal control begins with the Board of Directors and Finance and Audit Committee. The primary function of the Finance and Audit Committee is to provide advice with respect to the Corporation's financial matters, to oversee the accounting and financial reporting processes of the Corporation and the audits of the financial statements of the Corporation, to assist the Board of Directors in fulfilling its oversight responsibilities regarding finance, accounting, tax and legal compliance, and to 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.

RISK ASSESSMENT

Risk Identification

Control objectives relate to the risks identified by management that controls seek to mitigate when designing, implementing, and documenting their system. Management is responsible for identifying the risks that threaten achievement of the control objectives stated in management's description of the service organization's systems. Management has implemented a process for identifying relevant risks, which includes estimating the significance of identified risks, assessing the likelihood of their occurrence and deciding risk mitigating actions to address them.

Oracle establishes control objectives for management to identify potential events affecting their achievement. Risk management has placed into operation a process to set objectives and that the chosen objectives support and align with the organization's mission and are consistent with its risk framework. Objective setting enables management to identify measurement criteria for performance, with focus on success factors.

Regardless of whether an objective is stated or implied, Oracle's risk-assessment process considers risks that may occur to help ensure it is comprehensive. Oracle has evaluated significant interactions internally as well as between itself and relevant external parties to identify the risks that could affect the organization's ability to provide reliable service to its customers.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Business relationships with third-party vendors
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions
- Evaluation of the internal controls implemented at the colocation facility vendors.

Internal Factors

- Significant changes in policies, processes or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Use of contractors or other third parties
- Retention of qualified personnel
- Changes in management and personnel responsibilities.

Risk Analysis

Oracle's methodology for analyzing risks varies, largely because many risks are difficult to quantify. Nonetheless, the process includes:

- Estimating the significance of a risk
- Assessing the likelihood (or frequency) of the risk occurring
- Considering how the risk should be managed, including an assessment of what actions need to be taken.

Risk analysis is an essential process to Oracle's success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk and reasonable analysis of the costs associated with reducing the level of risk to an acceptable level. Necessary actions are then taken to reduce the significance or likelihood of the risk occurring.

Oracle's risk assessments take into account potential threat sources, vulnerabilities, and security controls in place or planned to determine the resulting level of residual risk posed to organizational operations, organizational assets or individuals based on the operation of the information system.

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control objectives have been defined for each significant risk area. Control activities are then defined to serve as mechanisms for managing the achievement of those objectives and help ensure the actions associated with those risks are carried out properly and efficiently.

INFORMATION AND COMMUNICATION

Information

Information is necessary for Oracle and its customers to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant information from both internal and external sources to support the functioning of internal control.

The following provides a summary of internal and external sources of information used in the System:

- Web applications provide the ability for customers to access reporting and make inquiries.
- Boundary protection mechanisms are configured to log activity that includes source and destination IP address, date and time, and incoming port to a centralized logging server.
- The Oracle Enterprise Manager (OEM) application is utilized to monitor operational performance of production servers.
- Oracle customers can access information online through My Oracle Support (MOS). MOS is Oracle's portal for technical support services. It is the primary means of logging an electronic Service Requests (SR) and offers a variety of support services and information for Oracle customers.

Communication

Oracle has implemented various methods of communication to provide employees the information they require to understand their individual roles and responsibilities and understand the importance of communicating significant. These methods include orientation for new employees, training for employees and the use of e-mail messages to communicate time-sensitive information. Employees are encouraged to communicate to their direct supervisor.

Oracle has also implemented various methods of communication to help provide assurance customers understand the roles and responsibilities in communication of significant events. These methods include regular meetings with representatives from customers, the use of e-mail messages and its customer contact line to communicate time-sensitive information. The Oracle public website also outlines details of the process for external users to inform Oracle of potential incidents relating to security and the availability of the services.

If incidents are communicated, personnel follow the documented incident response plan. Formal procedure changes are distributed to management before they are incorporated into the policy and distributed to relevant parties. Incidents are documented within a ticketing system and tracked by management until resolution.

MONITORING

Management performs monitoring activities to continuously assess the quality of internal control over time. Monitoring activities are used to initiate corrective action through department meetings, customer conference calls, and informal notifications. Management performs monitoring activities on a continuous basis, and the necessary corrective actions are taken as required to update company policy and procedures.

Monitoring can be done in two ways: through ongoing monitoring activities and separate evaluations. Greater effectiveness of ongoing monitoring results in less need for separate evaluations. Management determines the need for separate evaluations by considering the following: the nature and degree of changes occurring and their associated risks, the competence and experience of the people implementing the controls, and the results of the ongoing monitoring. Management has implemented a combination of ongoing monitoring and separate evaluations, as deemed necessary, to help ensure the internal control system maintains its effectiveness over time.

Ongoing Monitoring

Examples of Oracle's ongoing monitoring activities include the following:

- In carrying out its regular management activities, operating management obtains evidence that the system of internal control continues to function
- Communications from external parties and customers corroborate internally generated information or indicate problems
- Organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies
- Training, planning sessions and other meetings provide feedback to management on whether controls are effective
- Personnel are briefed on organizational policy statements and codes of conduct to communicate entity values.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons, such as major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often. Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. These assessments are considered by management, along with any other internal control evaluations. The findings of these efforts are utilized to help ensure follow-up actions are taken and subsequent evaluations are modified as necessary.

Policies and Governance

Customer-facing security practices, policies and documents are approved by senior management. These policies are reviewed or updated annually to help ensure they remain current and accurate.

Oracle Corporate security practices and policies are made available to customers via the Oracle Cloud Hosting and Delivery Policies accessible via the Oracle Contracts website. Employees have access to corporate security practices and policies via the internal corporate network. Oracle policies include but are not limited to the following areas:

- Administrative User Registration
- Privilege Management
- Review of Administrative Access Rights
- Administrative User Responsibilities
- Data Classification Policy
- Prevention of Unauthorized Access
- User Provisioning
- Risk Assessment
- Assigning responsibility and accountability for system security

- Requirements for testing, evaluating and authorizing system components
- Identification of applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements
- Policy which provides for sharing information with third parties
- Responsibility and accountability for developing and maintaining the entity's system security policies
- System Availability Requirements
- Assigning responsibility and accountability for availability
- Notification of issues related to system availability
- Training and access to necessary tools to manage system availability
- Business Continuity Management
- Capacity Management
- Desktop and Laptop Security Policy

Security Practices Documents
These documents provide an overview of the information security practices and procedures. Oracle Security Practices documents are reviewed or updated at least annually to help ensure they remain current and accurate. These policies are posted and made available to customers and personnel.

Data Classification
When new product offerings are made available to customers, the data gathered by the application is classified and documented according to the Oracle corporate policy.

The Oracle Data Processing Agreement for Cloud (DPA) to describe in detail how customer personal data is handled, such as:

- Scope
- Description of processing
- Purpose limitation
- Data controller rights and obligations
- Customer instructions
- Confidentiality
- Security
- Sub-processors and Oracle Affiliates
- Assistance with data subject rights
- Incident management and breach notification
- Data retention and deletion
- Audit rights and information requests.

Customer termination
Customer data is retained in accordance with the Cloud Services Agreement (CSA) until the data is deleted or rendered inaccessible within 6 months after the end of the Services Period defined in the customer order or actively monitored by senior management and worked through deletion. Exceptions are actively worked, tracked, and reviewed at least monthly by Oracle senior management until resolved. Confirmation of customer content deletion is provided to customers upon request.

Reporting Deficiencies
Deficiencies in management's internal control system may surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, but also to at least one

level of management above the directly responsible person. This process enables the individual to provide needed support or oversight for taking corrective action and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes the decision for addressing deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel.

Data Center Locations

The production infrastructure resides within the following Oracle Cloud Services data centers hosted by third-party colocation data centers across the globe.

Oracle Site ID	Data Center Hosting Provider (Colo) Site ID	Location	Data Center Hosting Provider
US1	ADC	Austin, TX, US	Oracle
EM2	AM2	Amsterdam, NL	Equinix
EM2	AM3	Amsterdam, NL	Equinix
EM2	AMS15	Amsterdam, NL	Digital Realty
EM8	AUH1	Abu Dhabi, UAE	Etisalat
US2	CH3	Elk Grove Village, IL, US	Equinix
US8	CH3F	Elk Grove Village, IL, US	Equinix
US2	CHI1	Chicago, IL, US	QTS
US9	IAD2G	Sterling, VA, US	QTS
US6	IAD36	Ashburn, VA, US	Digital Realty
US6	IAD37	Ashburn, VA, US	Digital Realty
EM3	LD5	Slough, UK	Equinix
EM1.UKG	LD5G	Slough, UK	Equinix
EM3	LGW14	Woking, UK	Digital Realty
EM2.UKG	LHR13G	Chessington, UK	Digital Realty
AP4	MEL11	Melbourne, AU	Digital Realty
US2	ORD13	Franklin Park, IL, US	Digital Realty
AP1	SY3	Sydney, AU	Equinix
AP1	SYD10	Sydney, AU	Digital Realty
CA2	TR3	Markham, Ontario, Canada	Cyxtera

ADMINISTRATIVE AND PERSONNEL PROCEDURES

Organizational Charts
Organizational charts are in place to communicate key areas of authority, responsibility, and reporting lines for personnel. These charts are online via Oracle's intranet and available to all employees.

Hiring Procedures
Human Resources (HR) is a corporate function at Oracle. HR representatives are assigned to the business areas within Oracle. HR utilizes the Oracle Human Resources Management System (HRMS) and Oracle Human Capital Management (Cloud HCM) (hereafter referred to as "HR Systems") for their operations. Personnel procedures vary according to local laws, employment regulations, and local Oracle policy.

There are formal procedures for hiring new employees (traditional new hire or through a merger and acquisition), which follow corporate directives and in-country regulations and processes. Across the organization, documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs. Job postings are advertised internally for a minimum of five days, or, in accordance with local regulations and local Oracle policy. Resumes are received and reviewed to select candidates for interviews. The manager and a recruiter, if requested by the manager, interview potential candidates.

After a candidate has been successfully identified, the offer process is initiated. There is a formal approval matrix that indicates the level of approval required for offers and transfers based on the terms of the transaction (e.g., position, salary, etc.) and the system workflow is configured based on the terms specified in the approval matrix. When a candidate is selected for the job opening, the offer request for that candidate is automatically routed using the aforementioned system workflow. On occasion, hiring approvals may also be obtained via e-mail, in accordance with the approval matrix.

Background checks are performed on candidates selected for hire in accordance with local laws and regulations, and local Oracle policy. Oracle's supplier agreements require the suppliers of contract personnel to perform background screening of non-direct Oracle workers (sub-contractors) before releasing an individual for assignment with Oracle to the extent permitted by local laws and regulations and local Oracle policy. In the event that a non-direct worker is hired as a direct Oracle employee, they are subject to the mandatory background checks for their location.

Oracle may utilize a third party to perform background checks on candidates for job openings. Generally, background checks are used to ascertain a candidate's education, previous employment, and may include a criminal records check. Additional checks may be conducted depending on local laws and regulations and local Oracle policy. Offers are released contingent upon satisfactory completion of Oracle's pre-employment background check process. If the background check, after an individualized assessment in accordance with applicable laws and agency guidance, produces disqualifying results and the candidate has not yet started work, the offer may be revoked; otherwise, if the individual has already been hired, they may be terminated. Internal transfers are not subject to a background check. For most countries, general HR processing and procedural variances may apply to students/interns, university/campus hires, and to existing employees of companies acquired by Oracle. For employees hired as the result of a merger and acquisition, background checks may be initiated after the individual has started work and may be limited to a criminal background check. Subject to applicable law, if the background check produces disqualifying results, the employee may be terminated. In some countries, local laws and regulations and local Oracle policy may prohibit the screening of merger and acquisition employees. International transfers may be subject to a background check, depending on their location, applicable laws and regulations, and only if they did not go through the screening process when they were originally hired at Oracle.

After acceptance of an offer, local HR reviews the appropriate documents to ascertain an applicant's right to work, in accordance with local laws and regulations and policy.

Each new employee is required to complete and sign a core set of new hire forms for their location, such as an employment agreement or equivalent and Propriety Information Agreement, prior to or on the day of hire (or as otherwise required under applicable law), in accordance with local procedures, laws, and regulations.

General HR processing and procedural variances may apply to existing employees of companies acquired by Oracle. Although it is Oracle's intent to have acquired company employees agree to Oracle's standard terms and conditions by way of signing an employment agreement and Proprietary Information Agreement, there may be instances where this is not achievable based on the circumstances of a particular acquisition or with a particular employee or set of employees. In many countries, acquired employees are not required to agree to changes to their employment terms and would remain on their existing terms and conditions.

In the cases where acquired employees, outside the US, do sign Oracle's standard employment agreement and Proprietary Information Agreement, the timing will vary due to local legislation, local procedures and complexities associated with a specific acquisition, and it is expected that it will be done after the local integration process.

Employees have job descriptions and responsibilities which define the necessary qualifications for their positions.

Training

New employees are supported by a new hire web site and orientation course. The orientations are available via a number of formats. Depending on the location, it may be an on-line e-course, a live web broadcast, or during face-to-face inductions.

Upon hire, employees are required to complete the Workplace Harassment Awareness, Code of Ethics and Business Conduct, Information Protection Awareness, the Anti-Corruption & Foreign Corrupt Practices Act, and Environment, Health, and Safety Awareness and potentially other courses that are required based on their location, role, and organization. Insider Trading training is also required for all employees globally. New hires are given 60 days to complete their training.

Oracle uses a Learning Management System (LMS) which provides course content, sends email reminders to employees, and allows for the tracking and reporting of all online training. It also permits existing employees to complete their training within the same timeframe and new training content is offered on an annual basis. Like new hires, existing employees are given 60 days to complete their training. In addition, a formal enforcement process has been adopted to address those employees that do not complete their mandated training within the allotted timeframe.

Ongoing training is available to all employees through a variety of courses including web learning, Oracle University and external courses. Training for each employee is tailored to support his or her job role.

Termination Procedures

A formal process exists for terminations. For voluntary terminations, it is the manager's responsibility to ensure the Voluntary Termination action is initiated once an employee renders his/her resignation. Involuntary terminations are managed by HR. Terminations are processed through the HR Systems and automated notifications are issued through the HR Systems or Clearance System. Oracle Identity Management (OIM) queries a termination view in the HR Systems every 24 hrs. For employees who have been terminated, the process will automatically disable the accounts managed by OIM (for example, e-mail, single sign on, VPN, as well as hosted servers, OCNA, etc.).

INFORMATION SECURITY

Information Security Policies and Procedures

Information security policies and procedures are in place to guide personnel in performing information security activities that include access management, password management, acceptable use, data retention and classification and confidentiality of information. These policies and procedures are reviewed by senior IT and operations personnel at least annually and are made available to employees via the corporate intranet.

Access Provisioning and Deprovisioning

Oracle's proprietary Oracle Identity Management (OIM) system is in place and configured to grant employee access requests to and within the production environment (including the operating system and database) and supporting tools after approval from product management.

As part of the employee onboarding process, access to the OIM system is granted, where users can request access to Oracle Cloud Network Access (OCNA) VPN, the production systems, and supporting tools.

Once an access request is submitted through the OIM system, the request is required to be approved by multiple levels of product management, dependent on the type of access being requested. The automated approval process within the OIM system is configured based on predefined approval requirements, and includes level one approval from the employee's manager, level two approval from cloud operations senior management, and level three approval from security services. The OIM system is configured to notify product management via e-mail when access requests are submitted and require approval.

Additionally, OIM is configured to automatically provision user access privileges once predefined approvals are received, required trainings have been completed and confidentiality agreements have been executed. Subsequently, when an employee is terminated, the OIM system is configured to revoke access as a component of the employee termination process. Access revocation is required to take place within 14 days of the employee's termination date. A quarterly review is performed to identify transactions where the HR transaction was recorded more than 14 days after the effective termination date and follow-up actions are executed as necessary.

Access Path and Authentication

Access to network devices and servers supporting the services requires Oracle users to use multi-factor authentication and traverse three levels of access control.

Oracle Cloud Network Access (OCNA)

The first step in the authentication path is the OCNA VPN. OCNA is a multi-tiered Demilitarized Zone (DMZ) environment inside a dedicated extranet isolated from Oracle's internal corporate network and VPNs for non-cloud services. It functions as a secure access gateway between the user and the target device. OCNA is comprised of a gateway subnet, tools subnet, and network subnet located in Oracle's DMZ and is protected by firewalls. OCNA has redundant gateways in various geographies worldwide.

- *Authentication* – Only approved users with a valid OCNA account can access OCNA. Two-factor authentication is required to authenticate to OCNA.
- *Authorization* – At the time of user account creation, attributes are defined to describe the specific entitlements that the user is authorized to access. The user is restricted to these resources when connected. The user's access must be approved by an appropriate approver prior to access being provisioned and access is revoked when the user is terminated. OCNA is configured to complete a security posture check to determine whether the endpoint is running up-to-date anti-virus software, has a local firewall enabled, and is in line with Oracle policies regarding software updates prior to permitting the endpoint to authenticate to the VPN.
- *Posture Check* - A security posture check is performed to validate a user's desktop or laptop machine is running up-to-date anti-malware software, has a local firewall and is in compliance with Oracle policies prior to granting access to OCNA.
- *Termination* – User access to OCNA is revoked within 14 days of termination. As a user cannot access the bastion servers once their OCNA access is revoked, revocation in OCNA results in termination of access to the system.

Bastion Server Authentication

The second step in the authentication path is authenticating to the relevant bastion server. Operator access is only permitted from bastion servers. The bastion servers are only permitted to accept connections from OCNA subnets. Only approved users with the required OIM entitlement can access the bastion servers. The user's access must be approved by an appropriate approver prior to the entitlement being provisioned. Authentication to the bastion servers is configured to require two-factor authentication, including the YubiKey universal serial bus (USB) token.

Accessing Production (database and operating system)

Once a user has authenticated to the relevant bastion server, they can then connect to the required individual production server operating systems via secure shell (SSH). Database users are able to authenticate to the production databases after first establishing connections to OCNA, the bastion hosts and the production server operating systems; but are also required to have an authorized user account and password, which is granted via membership as part of Oracle Identify Cloud Service (IDCS) groups. Production servers are configured to use centrally managed authentication systems and users must be a member of a specific IDCS group as defined in the configuration of the server to access them.

Customers receive single tenant pods with individual production servers and databases. Access to these is segregated as defined above and individual servers, including database servers, require individual authentication through SSH.

PowerBroker Privileged Access

The BeyondTrust PowerBroker utility tool is in place and utilized to grant users administrator-level privileges to production systems. The utility provides access to Linux and UNIX server operating systems by delegating administrative privileges and authorization without disclosing the "root" password. Administrator access within the production server operating systems and databases is granted based on the utility tool policies configured within the OIM system through an individual's PowerBroker policy. In addition, PowerBroker policies that grant access to the "root" or "oracle" privileged local accounts on the production environments which can be requested by development personnel are configured to expire 24 hours after being approved and provisioned.

OIM is configured to reject access requests to the privileged access entitlements, i.e., powerbroker policy entitlements, via two mechanisms:

- Entity key restriction: which enforces the rejection of requests from users who have write access to source code repositories at the time they are requesting the privileged access to production.
- Management chain restriction: which enforces the rejection of requests from users who do not belong to authorized organizations.

PowerBroker is configured to log user activity, including keystroke logging, for system administrators. User activity logs are retained indefinitely and reviewed by system administrators on an ad hoc basis.

Administrator access within the OIM system is restricted to identity management personnel and administrator access within OCNA is restricted to network and cloud security operations personnel.

Automatic Access Revocation

IDCS group entitlements that grant access to SSH to the production environment and PowerBroker policy entitlements that grant privileged access to the production environment are configured in OIM to be revoked at least every 90 days.

Once a user's access has expired, they are required to follow the normal user provisioning process through OIM to regain access.

CHANGE MANAGEMENT

Change Management Policies and Procedures

Documented change management policies and procedures are in place to help guide personnel in change management activities, including the documentation and approval of change requests, including emergency changes. These policies and procedures are reviewed by senior management at least annually and are made available to employees via the corporate intranet.

Release Notes

Release notes are made available to document and communicate specifications and new features for service packs and new versions of the application. Finalized release notes are published as the "What's New" document on the Oracle Cloud Readiness site two weeks prior to the quarterly release.

Change Tracking

All changes, including those for application, database and infrastructure related components, are tracked in Oracle's ticketing systems. The change request tickets within the change management system maintain specific details pertaining to the change request, including the change requestor, description of the change, affected production systems and product components, and testing information. Additionally, the change request tickets include the patching window for which the change request is scheduled to be applied to customer production systems.

Code Development

Development personnel perform program development and testing on application change requests within development and test environments that are logically and physically separate from the production environment.

Version control software is utilized to control developers' ability to access and implement changes to application code. Changes to source code result in the creation of a new version of the application code. Changes are capable of being rolled back to prior versions of the application code on an as-needed basis. Write access to the application source code within the version control software is restricted to user accounts accessible by authorized product support and development personnel.

Access to the version control software is managed through OIM and is configured to be revoked at least every 90 days. Once a user's access has expired, they are required to follow the normal user provisioning process to regain access.

Change Testing

Prior to implementation, product quality assurance (QA) personnel perform QA testing on application changes that require testing and update the application change request status and work history within the change management system with the testing results. Client data is not utilized for application change control testing. When application change requests are ready for implementation, operations and product management personnel document their requests to implement the application change (also referred to as application patches) within the change management system and submit the application change requests to IT and operations management for review and approval.

Infrastructure changes are tested based on the type of infrastructure change it is. Hardware related infrastructure changes, including hardware set up, optimization, and configuration, are changes that may not be tested in the pre-production environment. Post-production deployment analysis may be performed instead of pre-production testing for these changes.

Change Approval

Change management meetings are held to discuss application release planning and development activities. Weekly formal change reviews through a Change Advisory Board (CAB) are held across Cloud product lines of business to help ensure proper transparency with all key stakeholders. CAB members include subject matter experts from technical, business and support points of view. Formal approval for application releases is captured in a change request ticket prior to implementation to the production environment in addition to change management team participation during change review meetings. Infrastructure related changes require formal approval to be captured in a change request ticket before implementation to the production environment.

After approval, the application change request is scheduled for implementation and assigned to the cloud operations team via the change management system. IT and operations change management personnel notify the customer via the Cloud Admin tool whenever change requests are scheduled for implementation.

Segregation of Duties

Access to implement changes in the production environment is appropriately segregated from access to develop changes.

Access to implement changes in the production environment is granted based on PowerBroker entitlements provisioned by OIM. Event logs and keystroke logs are retained for instances of the access being used.

Developers requiring access to PowerBroker policies that grant access to the “root” or “oracle” privileged local accounts on the production environment require a justification prior to access being approved and are configured to expire 24 hours after being approved and provisioned.

COMPUTER OPERATIONS

Backup Policies and Procedures

Documented data backup policies and procedures are in place to guide personnel in processes including data backup and retention, backup monitoring and restoration procedures.

Backup Frequency and Monitoring

EPM Cloud Production environments are configured to automatically run a maintenance check on a daily basis. As part of the daily maintenance window, a daily backup known as an Artifact Snapshot, is created under the following conditions:

1. At least one user has logged in to the environment in the last 24 hours, or
2. 14 days have elapsed since a backup was created.

There are offline and online stages of the backup process. During offline backups, Essbase files are backed up for all EPM service except for EPM ARCS and EPM EDMCS. During online backup relational data is retrieved and stored on the file system. The offline and online backups are then combined into a single Artifact Snapshot.

A System Activity Report (SAR) is generated as a result of the daily maintenance window. The SAR contains the Automated Maintenance Window (AMW) table which shows all activities which were performed on the production environment during the maintenance window. Data backup completion status is configured to be captured in the SAR report. Backup failures are either auto-resolved by the Automated Maintenance Window (AMW) script or actively worked through resolution using the Oracle Bug Database (DB) ticketing system.

For EPM ARCS and EPM EDMCS, Essbase file (offline) backup is not performed because the two services do not use Essbase database management system and they do not have Essbase files. EPM ARCS and EPM EDMCS use file system and relational database to store data, which are covered by the online backup.

System Restoration Test

IT personnel perform restores of the production data backups to verify that system components can be recovered from system backups upon requests from customers.

Incident Response Policies and Procedures

Documented incident response policies and procedures are in place to guide personnel in server outage response, escalation, and resolution activities. Utilizing incident response policies and procedures in addition to an enterprise monitoring application, IT operations personnel monitor the availability and performance of production cloud systems on a daily basis. These policies and procedures are reviewed by senior management at least annually and are made available to employees via the corporate intranet.

System Configuration and Monitoring

Documented standard build procedures are utilized for creation, installation and maintenance of production servers. In addition, a configuration management tool is used to manage the servers consistently.

The availability and performance of production servers is monitored on a continuous basis by IT and operations personnel via monitoring tool. Monitoring tool Oracle Enterprise Manager (OEM) is in place and configured to monitor the performance and availability of customer production servers, and to notify IT and operations personnel via on-screen alerts and automated ticket creation whenever predefined thresholds are exceeded. Oracle Cloud Service Center (OCSC) personnel are staffed 24 hours per day to monitor alerts and possible issues are escalated for investigation and resolution.

Deviations, problems, and errors relevant to application and system processing reported by customers are responded, escalated, and resolved. A tooling system is used to track progress through resolution.

Antivirus

Oracle Cloud Security manages an enterprise McAfee antivirus solution. The McAfee antivirus agents on the bastion hosts are configured to perform periodic scans of the information system weekly. Any violations detected by the agent generate alerts to Oracle Cloud Security. Updates to virus definitions are configured to run daily.

Disaster Recovery

Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. Cloud operations personnel perform a disaster recovery test on an annual basis.

NETWORK MANAGEMENT

The production servers supporting the System are located within a separate network segment that is dedicated to cloud services. Firewall systems are in place to filter Internet traffic. Remote access to the production networks is required to pass through encrypted virtual private networks (VPN).

Firewalls
Firewalls are in place within the production cloud networks to filter unauthorized inbound network traffic from the Internet and are designed to deny any network connection that is not explicitly authorized by a firewall rule. High-availability firewall system clusters are in place to provide failover firewall services in the event of a firewall system failure. Externally routable IP addresses are not utilized for the hosted application and database servers.

Administrator access within the firewall systems is restricted to user accounts accessible by authorized IT security and network engineers.

The firewall system logs are reviewed for suspicious network activity by the Oracle Security Operations Center (SOC). In addition, Network engineers utilize a ticketing system to log and track configuration changes to network devices. Change requests follow a predefined approval workflow within the ticketing system based on the nature and impact of the change request. After the required approvals are obtained, the change request is automatically assigned to a system engineer for implementation via the ticketing system.

Intrusion Detection
Intrusion detection systems (IDS) are in place to monitor network traffic for potential security breaches. A Security Information and Event Management (SIEM) console is in place to consolidate event logs for assessment and enable Cloud Security personnel to follow up as necessary.

Vulnerability Scans
To help identify potential security vulnerabilities on the production cloud networks, network security management performs network vulnerability scans on at least a weekly basis. Operations management review and analyze the results of the network vulnerability scans through a customized tool, which is configured to consolidate the results for each production cloud network on a monthly basis. Oracle GIS, Privacy and Legal group representatives review the vulnerability scan results and manage the remediation activities.

Penetration Assessment
A third-party vendor performs an external application penetration assessment on an annual basis. Operations and IT management review the results of the penetration assessment and create remediation and mitigation plans where required.

Resolution of Vulnerabilities
Application Development team works on the remediation plans for the vulnerabilities identified in the weekly vulnerability scans and external penetration assessments. On a monthly basis, the results of vulnerability scans and remediation status is reported to Executive Vice President of Application Development to track the vulnerabilities through resolution.

Encryption
To protect data while in transit, web servers utilize transport layer security (TLS) encryption for web communication sessions. Further, remote access to the production cloud networks is restricted via an encrypted VPN to help ensure the privacy and integrity of the data passing over the public network. Administrator access within the VPN is restricted to user accounts accessible by authorized personnel.

Database Encryption
Production databases are encrypted in accordance with Oracle's policies and procedures.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

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

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 the following:

- Security and confidentiality principles inherent to the fundamental design of the Oracle System are intended to protect Your Content in accordance with the Oracle Cloud Services Agreement ("Nondisclosure" and "Protection of Your Content") and the Oracle Service Specifications available at http://www.oracle.com/us/corporate/contracts/cloud-services/index.html.
- Availability principles inherent to the fundamental design of the System are intended to monitor, detect, and address the functionality, security, integrity, and availability in accordance with the Oracle Cloud Services Agreement and the Oracle Service Specifications available at http://www.oracle.com/us/corporate/contracts/cloud-services/index.html.

Oracle 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’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 expected to be 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 System.

As a Software as a Service (SaaS) system, the system is designed based on a shared responsibility model where both Oracle, Sub-Service Organizations, 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, in the customer contract, and in the Complementary User Entity Controls (CUECs).

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Oracle IT general controls were designed with the assumption that certain controls would be implemented by user entities (or “customers”). This section describes additional controls that customers must have in operation to complement the controls of Oracle. The list of customer control considerations presented below and those presented with certain specified trust services criteria do not represent a comprehensive set of all the controls that should be employed by customers. Customers may be required to implement additional administrative or technical controls to meet their business and legal needs.

Applicable Trust Services Criteria	Complementary User Entity Controls (CUECs)
CC1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The customer is responsible for defining its organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of its application in accordance with applicable laws, regulations standards in order to meet its commitments and requirements as they relate to security, availability, and confidentiality.
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The customer is responsible for ensuring the completeness and accuracy of the financial data. The customer is responsible for application functionality, configuration, and transaction processing. The customer is responsible for determining their business processes and defining, or working with the implementer to define, any configuration controls required to support the business processes.
CC2.2 – COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The customer is responsible for communicating confidentiality commitments and requirements to internal and external users of its application.
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The customer is responsible for notifying Oracle of any unauthorized use of, and other known or suspected breach of, security, including compromised user accounts. The customer is responsible for reviewing incident response details provided by Oracle and to initiate inquiry or follow-up as appropriate. The customer is responsible for communicating confidentiality commitments and requirements to internal and external users of its application. The customer is responsible for submitting incident tickets (i.e. data restores) through the My Oracle Support (MOS) customer portal. Customer requests are recorded and tracked within an internal ticketing system through resolution. The ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting contracted services. Customer requests are managed according to established service level agreements.

Applicable Trust Services Criteria	Complementary User Entity Controls (CUECs)
CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The customer is responsible for all aspects of security relevant to its application. The customer is responsible for designing, developing, testing, implementing, operating and maintaining administrative and technical safeguards to prevent or detect unauthorized access, use, and disclosure during input, processing, retention, output, and disposition of data to, in or from its application. The customer is responsible for confidentiality of passwords and user IDs assigned by them. The customer is responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with Oracle's systems. The customer is responsible for managing application-level access for their employees throughout an employee's relationship with the entity (e.g., onboarding, termination, role changes, etc.).
CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The customer is responsible for administering application security rights. The customer is responsible for removing terminated employees' access. The customer is responsible for defining authorized application administrators within its application, ensuring that these privileges are restricted to authorized individuals, and for periodically reviewing the security configurations and access rights for appropriateness. The customer is responsible for managing application-level access for their employees throughout an employee's relationship with the entity (e.g., onboarding, termination, role changes, etc.).

Applicable Trust Services Criteria	Complementary User Entity Controls (CUECs)
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The customer is responsible for configuring application password parameters and complexity requirements. The customer is responsible for confidentiality of passwords and user IDs assigned by them. The customer is responsible for administering application security rights. The customer is responsible for removing terminated employees' access. The customer is responsible for defining authorized application administrators within its application, ensuring that these privileges are restricted to authorized individuals, and for periodically reviewing the security configurations and access rights for appropriateness. The customer is responsible for defining authorized application administrators within the application, and for periodically reviewing the access rights for all end users are appropriate. The customer is responsible for immediately notifying Oracle of any actual or suspected information security breaches, including compromised user accounts.
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The customer is responsible for any customized changes made to its environment including, but not limited to, virtual networks, operating systems, virtual machines, databases, storage, and applications. The customer is responsible for reviewing release notes and other notices of changes and to evaluate, and if necessary, take steps to mitigate, the effects of any changes. The customer is responsible for ensuring sufficient controls for the implementation of the application. The customer is responsible for ensuring the integration with systems external to the application. The customer is responsible for the change management process regarding specific customization(s). The customer is responsible for data changes (e.g. update, insertion and deletion of data). The customer is responsible for the configuration of their application and any third-party applications.

Applicable Trust Services Criteria	Complementary User Entity Controls (CUECs)
C1.1 – The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The customer is responsible for ensuring that they do not enter confidential data in support tickets and requests. The customer is responsible for designing, developing, testing, implementing, operating, and maintaining administrative and technical safeguards to prevent or detect unauthorized access, use, and disclosure during input, processing, retention, output, and disposition of data to, in or from its application. The customer is responsible for communicating confidentiality commitments and requirements to internal and external users of its application. The customer is responsible for confidentiality of passwords and user IDs assigned by them.
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The customer is responsible for notifying Oracle of their intent to discontinue the use of the Service after the end of the Service Period.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Oracle uses subservice organizations to provide data center hosting services. These data center facilities include controls over physical security supporting the System. This description includes only those controls expected at the subservice organizations and does not include controls at Oracle.

Trust Services Criteria	Complementary Subservice Organization Controls
Common Criteria 2.3	The subservice organization is responsible for informing Oracle of all physical security breaches, failures, identified vulnerabilities, and incidents.
Common Criteria 6.4	The subservice organization is responsible for restricting physical access to production systems.
Common Criteria 6.4	The subservice organization is responsible for restricting physical access to offline storage and backup media to help ensure that application and data files are securely stored.
Availability Criteria 1.2	The subservice organization is responsible for equipping the data center facilities with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events to help ensure that systems are maintained in a manner that helps ensure system availability.

SECTION IV – ORACLE ENTERPRISE PERFORMANCE MANAGEMENT CLOUD SERVICES SYSTEM CONTROLS, TEST PROCEDURES AND RESULTS OF TESTING

DESCRIPTION OF CRITERIA, CONTROLS, TESTS, AND RESULTS OF TESTING

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of Oracle. The Testing Performed and Results of Testing are the responsibility of the service auditor. Unless specifically documented by the caption “Results of Testing” in the column titled “Testing Performed and Results of Testing”, no deviations resulted from testing.

PROCEDURES FOR ASSESSING COMPLETENESS AND ACCURACY OF INFORMATION PRODUCED BY THE ENTITY (IPE)

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

Administrative and Personnel Procedures

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
1.01: Background checks are performed for new hires as described in the narrative.	Inquired of the control owner and ascertained background checks were performed for new hires as described in the narrative.	No deviations noted.	CC1.1 CC1.4
	Inspected the background check documentation for a sample of new hires selected from the HR Systems and ascertained the background checks were completed.	No deviations noted.	
1.02: 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.	Inquired of the control owner and ascertained each new employee was required to complete and sign an employment agreement or equivalent and a Proprietary Information Agreement, prior to or on the day of hire, in accordance with local procedures, laws, and regulations.	No deviations noted.	CC1.1 CC1.5
	Inspected the applicable documentation for a sample of new employees selected from the HR Systems and ascertained it was completed in accordance with local procedures, laws and regulations.	No deviations noted.	
1.03: New employees are required to complete the Code of Ethics and Business Conduct, Information Protection Awareness, and Anti-Corruption & Foreign Corrupt Practices Act online e-courses. New employees who do not complete these courses in a timely manner are identified on the exception list for follow-up.	Inquired of the control owner and ascertained new employees were required to complete the Code of Ethics and Business Conduct, Information Protection Awareness, and Anti-Corruption & Foreign Corrupt Practices Act online e-courses, and new employees who did not complete these courses in a timely manner were identified on the exception list for follow-up.	No deviations noted.	CC1.1 CC1.4 CC2.2

Administrative and Personnel Procedures			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the course records for a sample of new employees selected from the HR Systems and ascertained the new employees had completed the Ethics and Business Conduct, Information Protection Awareness, and Anti-Corruption & Foreign Corrupt Practices Act online e-courses or were identified on the exception list for follow-up.	No deviations noted.	
1.04: Employees are assigned a job description upon hire that defines their role and the necessary qualifications for their position.	Inquired of the control owner and ascertained employees were assigned a job description upon hire that defined their role and the necessary qualifications for their position.	No deviations noted.	CC1.3 CC1.4
	Inspected the job description for a sample of employees and ascertained a job description existed which defined the necessary qualifications for their position.	No deviations noted.	

Information Security

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
2.01: Documented information security policies are in place to guide personnel in areas that include the following: • Information security • Access management • Password management • Acceptable use • Data retention and classification • Confidentiality of information	Inquired of the control owner and ascertained documented information security policies were in place to guide personnel in areas that included the following: • Information security • Access management • Password management • Acceptable use • Data retention and classification • Confidentiality of information	No deviations noted.	CC2.1 CC2.2 CC5.3 CC6.1 C1.1
	Inspected the information security policies and ascertained documented information security policies were in place to guide personnel in areas that included the following: • Information security • Access management • Password management • Acceptable use • Data retention and classification • Confidentiality of information	No deviations noted.	
2.02: Oracle utilizes OIM for Oracle Cloud personnel to submit user account requests. The system routes the requests to the appropriate approver for approval. Upon approval the access provisioning system creates the user account on the selected environment.	Inquired of the control owner and ascertained Oracle utilized OIM for Oracle Cloud personnel to submit user account requests and that the system routed the requests to the appropriate approver and upon approval the access provisioning system created the user account for the selected environment.	No deviations noted.	CC5.2 CC6.1 CC6.2 CC6.3

Information Security			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the access provisioning system configuration and ascertained the system was configured to route access requests to the user's manager for approval.	No deviations noted.	
	Inspected the access provisioning system approval for a sample of access requests selected from the access provisioning system and ascertained they had received approval from the appropriate individuals configured within the account provisioning system.	No deviations noted.	
	Inspected the source system for a sample of user access requests and ascertained user access provisioned in the source system was the access requested and approved in OIM.	No deviations noted.	
2.03: The OIM system is configured to enforce the following user account and password controls: • Minimum password length • Password complexity	Inquired of the control owner and ascertained the OIM system was configured to enforce the following user account and password controls: • Minimum password length • Password complexity	No deviations noted.	CC6.1 CC6.2
	Inspected the Oracle Password Policy and ascertained it included details regarding the minimum password length and password complexity for user accounts.	No deviations noted.	
	Inspected the password settings configured in the account provisioning system and ascertained they were in adherence with the password policy requirements.	No deviations noted.	

Information Security

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
	Observed a user attempt to reset their password using characteristics that did not meet the password policy requirements and ascertained the user was unable to create a non-compliant password.	No deviations noted.	
2.04: Authentication to OCNA requires users to connect via two-factor authentication that includes the following: • Authorized user account • PIN • Individual token generator	Inquired of the control owner and ascertained authentication to OCNA required users to connect via two-factor authentication which included the following: • Authorized user account • PIN • Individual token generator	No deviations noted.	CC6.1 CC6.2 CC6.6
	Inspected the OCNA configuration and ascertained two-factor authentication was enabled.	No deviations noted.	
	Observed a user connect to the OCNA VPN and ascertained the user was required to use multi-factor authentication.	No deviations noted.	
2.05: Administrator access within OCNA is restricted to user accounts accessible by authorized network and cloud security operations personnel.	Inquired of the control owner and ascertained administrator access within the OCNA system was restricted to user accounts accessible by authorized network and cloud security operations personnel.	No deviations noted.	CC6.1 CC6.3
	Inspected the list of users with administrator access to the OCNA system and ascertained access was appropriately restricted to user accounts accessible only by network and cloud security operations personnel.	No deviations noted.	

Information Security

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
2.06: User-level access entitlements granting access to the production environment are configured to expire every 90 days.	Inquired of the control owner and ascertained user-level access entitlements granting access to the production environment were configured to expire every 90 days.	No deviations noted.	CC6.1 CC6.2 CC6.3
	Inspected the configuration for user-level access entitlements that grant access to the production environment and ascertained they were configured to expire at least every 90 days.	Deviations noted. Two (2) of thirty-two (32) user-level access entitlements were not configured to be revoked automatically after 90 days.	
Management response: Although the identified entitlements are not configured to expire every 90 days, manager approval is required in order for any user to obtain the access. The users who may be granted the user entitlements cannot make changes to any Oracle Enterprise Performance Management Cloud production environments unless they are also granted the applicable layered PowerBroker policies, which are justified, and approved by a manager prior to provisioning, and are configured to expire at least every 90 days after provisioning.			
2.07: Dynamic Access Policies are configured to validate that devices are running up-to-date anti-malware software, up-to-date software and have a local firewall installed prior to granting access to the infrastructure supporting the System. The VPN is configured to time out after 24 hours of inactivity.	Inquired of the control owner and ascertained Dynamic Access Policies were configured to validate devices were running up-to-date anti-malware software, up-to-date software and had a local firewall installed prior to granting access to the infrastructure supporting the System and the VPN was configured to time out after 24 hours of inactivity.	No deviations noted.	CC6.1 CC6.6 CC6.8
	Inspected the Dynamic Access Policies for OCNA and ascertained it was configured to check if end points were running up-to-date anti-malware software, up-to-date software, and had a local firewall installed prior to granting access to the infrastructure supporting the System.	No deviations noted.	

Information Security			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the VPN configuration and ascertained the VPN was configured to time out after 24 hours of inactivity.	No deviations noted.	
	Attempted to connect to OCNA from a mobile device and ascertained the connection was unsuccessful as the device did not meet the requirements of the Dynamic Access Policies.	No deviations noted.	
2.08: PowerBroker policies that grant access to the “root” or "oracle" privileged local account on the production environment, which can be requested by development personnel, are configured to expire 24 hours after being approved and provisioned.	Inquired of the control owner and ascertained PowerBroker policies that granted access to the “root” or "oracle" privileged local account on the production environment, which can be requested by development personnel, were configured to expire 24 hours after being approved and provisioned unless specified otherwise by the customer.	No deviations noted.	CC6.1 CC6.2 CC6.3 CC8.1
	Inspected the configuration in the account provisioning system and ascertained PowerBroker policies that grant access to the “root” or "oracle" privileged local account on the production environment were either configured to restrict access from developers or were configured to expire 24 hours after being approved and provisioned.	Deviations noted. Two (2) of eighteen (18) privileged access entitlements, which can be requested by developers were configured to expire after 30 days.	

Information Security

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
Management response: Although the identified entitlements are not configured to restrict developers from requesting access, a justification and manager approval are required in order for the requestor to be granted the access. The identified entitlements are configured to expire every 30 days and will be revoked automatically without a manager's recertification. The testing performed for the control “Access to implement changes into the production environment is appropriately segregated from access to develop changes.” did not identify any users holding the identified entitlements in conjunction with entitlements providing access to the version control software throughout the examination period.			
	Observed a developer request and obtain access to a PowerBroker policy that granted access to the “root'” and "oracle" privileged local account on the production environment and ascertained the user's access expired after 24 hours and the user was unable to authenticate with the PowerBroker policy.	No deviations noted.	
	Observed a user who did not belong to an authorized organization request access to a PowerBroker policy that grant access to privileged local account on the production environment and ascertained the user's request was denied.	No deviations noted.	
2.09: Privileged access to the production servers is configured to be revoked automatically at least every 90 days.	Inquired of the control owner and ascertained privileged access to the production servers was configured to be revoked automatically at least every 90 days.	No deviations noted.	CC6.1 CC6.2 CC6.3 CC8.1
	Inspected the configuration for PowerBroker Policy access entitlements that provided privileged access to the production servers and ascertained the access entitlements were configured to be automatically revoked at least every 90 days.	No deviations noted.	

Information Security			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Observed a user with privileged access entitlement and ascertained the user was unable to authenticate to the production server after the user's access expired per the expiry set for the entitlement.	No deviations noted.	
2.10: The ability to make changes to the configurations within OIM is limited to appropriate personnel.	Inquired of the control owner and ascertained the ability to make changes to the configurations within OIM was limited to appropriate personnel.	No deviations noted.	CC6.1 CC6.2 CC6.3
	Inspected the user access review covering users with access to modify OIM configurations and ascertained the users were reviewed and deemed appropriate.	No deviations noted.	
2.11: Access entitlements are configured to be automatically revoked upon termination of an employee.	Inquired of the control owner and ascertained access entitlements were configured to be automatically revoked upon termination of an employee.	No deviations noted.	CC6.2 CC6.3
	Inspected the termination jobs schedule and ascertained the jobs were scheduled to run on a defined periodic basis to revoke employee access upon termination.	No deviations noted.	
	Inspected termination details from OIM for a sample terminated user and ascertained the user's access was terminated timely.	No deviations noted.	
	Inspected the company directory for users with ability to modify the termination jobs schedule and ascertained the users were appropriate based on job title and organizational unit.	No deviations noted.	

Information Security			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
2.12: A quarterly review is performed to identify transactions where the HR transaction was recorded more than 14 days after the effective termination date.	Inquired of the control owner and ascertained a quarterly review was performed to identify transactions where the HR transaction was recorded more than 14 days after the effective termination date.	No deviations noted.	CC6.2 CC6.3
	Inspected the termination review documentation for a sample of quarters and ascertained the reviews were performed completely and timely by an appropriate reviewer and follow-up actions were executed, if applicable.	No deviations noted.	
2.13: Access to the management VPN supporting Cloud Applications environments must be renewed upon a change in manager or transfer of an employee or access is revoked.	Inquired of the control owner and ascertained access to the management VPN supporting Cloud Applications environments must be renewed upon a change in manager or transfer of an employee or access is revoked.	No deviations noted.	CC5.2 CC6.1 CC6.2 CC6.3
	Inspected the OIM configuration and ascertained OIM was configured to send the user's new manager a request to approve or reject the VPN access and to revoke the VPN access if no response from the new manager was provided within 14 days.	No deviations noted.	
	Observed for a user who had a manager change, OIM sent a request to the user's new manager to re-certify the VPN access and ascertained the VPN access was extended upon re-certification from the new manager.	No deviations noted.	

Information Security			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Observed for a user who had a manager change, OIM sent a request to the user's new manager to re-certify the VPN access and ascertained the VPN access was revoked upon rejection of the access extension request submitted to the new manager.	No deviations noted.	
	Observed a sample user who had a change in manager and ascertained VPN access is revoked as the user's manager failed to re-certify access within 14 days.	No deviations noted.	

Change Management			
Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
3.01: Documented change management policies and procedures are in place to guide personnel in the documentation and approval of changes, including emergency changes.	Inquired of the control owner and ascertained documented change management policies and procedures were in place to guide personnel in the documentation, and approval of changes, including emergency changes.	No deviations noted.	CC2.2 CC5.3 CC8.1
	Inspected the change management policies and procedures document and ascertained it contained details to guide personnel in the documentation and approval of changes, including emergency changes.	No deviations noted.	
3.02: Release notes are available to internal and external users to document and communicate specifications and new features for service packs and new versions of the application.	Inquired of the control owner and ascertained release notes were available to internal and external users to document and communicate specifications and new features for service packs and new versions of the application.	No deviations noted.	CC2.2 CC2.3 CC8.1
	Inspected the internal and external sites and ascertained release notes were available to internal and external users to document and communicate specifications and new features for service packs and new versions of the application.	No deviations noted.	
3.03: Development and testing efforts are performed in development and test environments that are logically and physically separate from the production environment.	Inquired of the control owner and ascertained development and testing efforts were performed in development and test environments that were logically and physically separate from the production environment.	No deviations noted.	CC6.1 CC8.1
	Inspected production environment details and ascertained they were logically and physically separate from development and test environments.	No deviations noted.	

Change Management			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
3.04: Version control software is utilized to restrict the ability to access and implement changes to source code. Users are authenticated via a user account and password before being granted access to the source code in the version control software.	Inquired of the control owner and ascertained version control software was utilized to restrict the ability to access and implement changes to source code and users were authenticated via a user account and password before being granted access to the source code in the version control software.	No deviations noted.	CC6.1 CC6.3 CC8.1
	Observed an authorized user authenticate via a user account and password and ascertained the user was granted access to the source code in the version control software.	No deviations noted.	
	Observed an unauthorized user attempt to authenticate to the version control software and ascertained the user was unable to access the source code in the version control software.	No deviations noted.	
3.05: Changes to source code result in the creation of a new version of the application code. Rollback versions exist in the event application code needs to be restored to a previous version.	Inquired of the control owner and ascertained changes to source code resulted in the creation of a new version of the application code and rollback versions existed in the event application code needed to be restored to a previous version.	No deviations noted.	CC8.1
	Inspected a version history for a sample change and ascertained a new version number was created for the code change and a prior version of the change was still available in the event of a rollback.	No deviations noted.	
3.06: Access to the source code repository is set to expire every 90 days.	Inquired of the control owner and ascertained access to the source code repository was set to expire every 90 days.	No deviations noted.	CC6.3 CC8.1

Change Management			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the configuration of entitlements providing access to the source code repository and ascertained they were set to expire every 90 days.	No deviations noted.	
3.07: Testing when required is completed for changes prior to implementation.	Inquired of the control owner and ascertained testing when required was completed for changes prior to implementation.	No deviations noted.	CC8.1
	Inspected the change ticket and testing documentation for a sample of application and infrastructure changes and ascertained testing when required was completed for changes prior to implementation.	No deviations noted.	
3.08: Changes are approved in accordance with the Change Management Policy.	Inquired of the control owner and ascertained changes were approved in accordance with the Change Management Policy.	No deviations noted.	CC8.1
	Inspected the change ticket approval documentation for a sample of application and infrastructure changes and ascertained changes were approved in accordance with the Change Management Policy.	No deviations noted.	
3.09: Change management meetings are held to discuss application release planning and development activities.	Inquired of the control owner and ascertained change management meetings were held to discuss application release planning and development activities.	No deviations noted.	CC8.1

Change Management			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the minutes from the change management meeting for a sample of weeks and ascertained change management meetings were held to discuss application release planning and development activities.	No deviations noted.	
3.10: Access to implement changes into the production environment is appropriately segregated from access to develop changes.	Inquired of the control owner and ascertained access to implement changes into the production environment was appropriately segregated from access to develop changes.	No deviations noted.	CC8.1
	Inspected the list of users with the ability to implement changes into the production environment and the list of users with the ability to develop changes throughout the examination period and ascertained access to implement changes into the production environment was appropriately segregated from access to develop changes.	No deviations noted.	
3.11: Write access to the version control software is restricted to user accounts accessible by authorized development personnel.	Inquired of the control owner and ascertained write access to the version control software was restricted to user accounts accessible by authorized development personnel.	No deviations noted.	CC8.1
	Inspected a sample of users with write access to the version control software and ascertained the version control software was restricted to authorized development personnel.	Deviation noted. One (1) of twenty-five (25) sampled users with write access to the version control software are not authorized development personnel.	

Change Management			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
Management response: The identified user's access to the version control software was revoked upon identification of the deviation. System generated activity logs were reviewed; the identified user did not perform any activity in the version control software.			
3.12: Client data is not utilized for application change control testing.	Inquired of the control owner and ascertained client data was not utilized for application change control testing.	No deviations noted.	CC6.1 CC8.1
	Inspected the Oracle Public Cloud Customer Data Handling Policy document and ascertained Oracle staff were directed to not utilize client data for application change control testing.	No deviations noted.	
	Inspected the application change testing environment and ascertained client data was not utilized within the testing environment.	No deviations noted.	

Computer Operations			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
4.01: An automated script is run daily on EPM Cloud environment to create backup under the following conditions: • At least one user has logged in the environment in the last 24 hours • 14 days have elapsed since a backup was created.	Inquired of the control owner and ascertained an automated script was run daily on EPM Cloud environment to create backup under the following conditions: • At least one user has logged in the environment in the last 24 hours • 14 days have elapsed since a backup was created.	No deviations noted.	A1.2 A1.3
	Inspected the centrally configured automated script and ascertained backups occurred when at least one user had logged in the environment in the last 24 hours and when 14 days had elapsed since the backup was created.	No deviations noted.	
	Inspected the centrally configured automated script for a sample of production pods and ascertained it was applied on each sample pod for backup to run daily on the EPM Cloud environment.	No deviations noted.	
	Inspected the company directory for a sample of users with ability to modify the backup configuration and ascertained the users were appropriate based on job title and organizational unit.	No deviations noted.	

Computer Operations

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
4.02: An automated system is configured to raise alerts for failed backup jobs and appropriate IT personnel monitor and resolve failed backups.	Inquired of the control owner and ascertained an alerting system was configured to notify Oracle personnel in the event of a backup failure.	No deviations noted.	CC2.1 A1.2 A1.3
	Inspected the centrally configured automated script for a sample of production pods and ascertained it was applied on each sample pod to identify and log failed backups.	No deviations noted.	
	Inspected the alerting script and ascertained it was configured to display the failed backup as alerts on a central dashboard.	No deviations noted.	
	Inspected the backup resolution evidence for a sample of logged failed backups and ascertained the backups were resolved or actively worked on.	From January 1, 2022 to March 31, 2022: Deviations noted. Evidence demonstrating that failed backups were resolved or actively worked on could not be provided due to the unavailability of data. From April 1, 2022 to December 31, 2022: No deviations noted.	

<table>
<tr><th colspan="4">Computer Operations</th></tr>
<tr><th>Control Description</th><th>Testing Performed</th><th>Results of Testing</th><th>SOC 2 Criteria</th></tr>
<tr><td colspan="4">Management response:
Backup logs are retained for 60 days. System logs required to demonstrate that backup failures are resolved timely were not available for the examination period due to the timing of testing the control.
The risk of unrecoverable data is addressed through the following mitigating control:
- IT personnel perform restores of production data backups to verify that system components can be recovered from system backups upon customer requests.</td></tr>
<tr><td></td><td>Inspected the company directory for a sample of users with ability to modify the script configurations and ascertained the users were appropriate based on job title and organizational unit.</td><td>No deviations noted.</td><td></td></tr>
<tr><td rowspan="2">4.03: Documented policies and procedures are in place to guide personnel in server outage response, escalation, and resolution activities.</td><td>Inquired of the control owner and ascertained documented incident response policies and procedures were in place to guide personnel in server outage response, escalation, and resolution activities.</td><td>No deviations noted.</td><td rowspan="2">CC2.2
CC4.1
CC4.2
CC5.3
CC7.3
CC7.4
CC7.5
CC9.1
A1.2
A1.3</td></tr>
<tr><td>Inspected the incident response policies and procedures and ascertained they were in place to guide personnel in server outage response, escalation, and resolution activities.</td><td>No deviations noted.</td></tr>
</table>

Computer Operations

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
4.04: Documented standard build procedures are utilized for creation, installation and maintenance of production servers. In addition, a configuration management tool is used to manage the servers consistently.	Inquired of the control owner and ascertained documented standard build procedures were utilized for creation, installation, and maintenance of production servers and a configuration management tool was used to manage the servers consistently.	No deviations noted.	CC2.2 CC5.3 CC7.1 CC8.1
	Inspected the operating system build procedures document and ascertained it detailed procedures relating to the creation, installation, and maintenance of production servers.	No deviations noted.	
	Inspected the configuration files for a sample of customer servers and ascertained a configuration management tool was used to manage the servers.	Deviation noted. For one (1) of twenty-five (25) sampled production servers, a configuration management tool was not used to manage the server.	

Management response:

The agent was reinstalled to the identified server. New procedures were implemented on 1/12/2023 to install the standard configuration management tool on servers.

System configurations can only be modified by users who have elevated access in the Cloud Application production environment. The risk of unauthorized configuration changes made to production environment is mitigated by the below logical access controls, which are tested to be operating effectively:

1) Oracle utilizes OIM for Oracle Cloud personnel to submit user account requests. The system routes the requests to the appropriate approver for approval. Upon approval the access provisioning system creates the user account on the selected environment.
2) Privileged access to the production servers is configured to be revoked automatically at least every 90 days.
3) Access entitlements are configured to be automatically revoked upon termination of an employee.
4) Access to implement changes into the production environment is appropriately segregated from access to develop changes.

Computer Operations			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the company directory for a sample of users with ability to modify the configurations used to manage the servers and ascertained the users were appropriate based on job title and organizational unit.	No deviations noted.	
4.05: Monitoring tools are used to monitor the customer production servers for performance and availability metrics.	Inquired of the control owner and ascertained the monitoring tools were used to monitor the customer production servers for performance and availability metrics.	No deviations noted.	CC2.1 CC4.1 CC4.2 CC7.1 CC7.2 CC7.3 A1.1 A1.2
	Inspected the monitoring tool configuration for a sample of production servers and ascertained a monitoring tool was used to monitor production servers for performance and availability metrics.	No deviations noted.	
	Inspected the company directory for a sample of users with ability to modify the threshold configurations set up and ascertained the users were appropriate based on job title and organizational unit.	Deviation noted. For one (1) of the seven (7) users selected for testing with access to modify the threshold configurations, their access was deemed inappropriate.	
Management response: The identified user was transferred to a new role on June 1, 2022 and was appropriately approved for the access to perform the job responsibilities as of June 1, 2022. The user's access was revoked on June 29, 2022.			
4.06: Monitoring tools are configured to notify appropriate personnel when predefined thresholds are exceeded on monitored systems and devices.	Inquired of the control owner and ascertained monitoring tools were configured to notify appropriate personnel when predefined thresholds were exceeded on monitoring systems and devices.	No deviations noted.	CC2.1 CC4.1 CC4.2

Computer Operations

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
	Inspected the monitoring tool alert notification configuration for a sample of production pods and ascertained they were configured to trigger alerts based on predefined performance and availability metrics.	No deviations noted.	CC7.1 CC7.2 CC7.3 A1.1
	Inspected the company directory for a sample of users with ability to modify alert notification configuration setup and ascertained the users were appropriate based on job title and organizational unit.	Deviation noted. For one (1) of the seven (7) users selected for testing with access to modify the threshold configurations, their access was deemed inappropriate.	
Management response: The identified user was transferred to a new role on June 1, 2022 and was appropriately approved for the access to perform the job responsibilities as of June 1, 2022. The user's access was revoked on June 29, 2022.			
	Inspected a sample ticket created in response to a predefined threshold being exceeded and ascertained the ticket was resolved.	No deviations noted.	
4.07: Backup media is encrypted in accordance with Oracle's policies and procedures.	Inquired of the control owner and ascertained backup media was encrypted in accordance with Oracle's policies and procedures.	No deviations noted.	CC6.1 CC6.4 CC6.7
	Inspected the Oracle Key Manager (OKM) configuration agents for a sample of colocations and ascertained OKM was configured to encrypt data written to tape.	No deviations noted.	

Computer Operations			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the company directory for a sample of users with access to encrypted backed up data and ascertained the users were appropriate based on job titles and organizational unit.	No deviations noted.	
4.08: Antivirus software is deployed on the bastion servers to detect and prevent the transmission of data or files that contain virus signatures recognized by the antivirus software. The antivirus software is configured to do the following: • Update antivirus definitions on at least a weekly basis • Scan the bastion servers on at least a weekly basis as specified in the Oracle Public Cloud Antivirus Standard	Inquired of the control owner and ascertained antivirus software was deployed on the bastion servers to detect and prevent the transmission of data or files that contain virus signatures recognized by the antivirus software. The antivirus software was configured to do the following: • Update antivirus definitions on at least a weekly basis • Scan the bastion servers on at least a weekly basis as specified in the Oracle Public Cloud Antivirus Standard	No deviations noted.	CC6.6 CC6.8 CC7.2
	Inspected the antivirus configuration for a sample of bastion servers and ascertained the scan for updates to antivirus definitions was configured to run on at least a weekly basis.	No deviations noted.	
	Inspected the antivirus scan configuration for a sample of bastion servers and ascertained the scan was configured to run on at least a weekly basis.	No deviations noted.	
	Inspected the monthly review performed of users with access to modify the antivirus scan and definition update configurations for a sample of months and ascertained the users were reviewed to ensure appropriateness.	No deviations noted.	

Computer Operations			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
4.09: Production databases are encrypted in accordance with Oracle's policies and procedures.	Inquired of the control owner and ascertained production databases were encrypted in accordance with Oracle's policies and procedures.	No deviations noted.	C1.1
	Inspected the database encryption configurations for a sample of production pods and ascertained the encryption configuration was in accordance with Oracle's policies and procedures.	No deviations noted.	
	Inspected the job titles and organizational unit for a sample of users who have access to modify database encryption configurations and ascertained the users were appropriate.	No deviations noted.	
4.10: Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inquired of the control owner and ascertained documented disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No deviations noted.	CC2.2 CC5.3 CC7.5 CC9.1 A1.2 A1.3
	Inspected the disaster recovery plan policies and procedures documents and ascertained they contained details to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No deviations noted.	
4.11: Disaster recovery plans are tested on at least an annual basis.	Inquired of the control owner and ascertained documented disaster recovery plans were tested on at least an annual basis.	No deviations noted.	CC7.5 CC9.1 A1.2 A1.3
	Inspected the disaster recovery plan test results and ascertained disaster recovery plans were performed at least annually and that corrective actions were initiated when necessary.	No deviations noted.	

Computer Operations			
Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
4.12: Customer data is retained in accordance with the Cloud Services Agreement (CSA) until the data is deleted or rendered inaccessible within 6 months after the end of the Services Period defined in the customer order. Exceptions to policy, such as contract renewal negotiations or legal or regulatory holds are actively worked, are tracked and reviewed monthly by Oracle senior management until resolved.	Inquired of the control owner and ascertained upon termination agreement, client data was retained in accordance with the Cloud Service Agreement (CSA) until the data was deleted or rendered inaccessible within 6 months after the end of the Services Period defined in the customer order and that exceptions were actively worked, tracked, and reviewed at least monthly by Oracle senior management until resolved.	No deviations noted	C1.2
	Inspected the decommissioning details for a sample of terminated customers and ascertained client data was archived and retained for 60 days post contract termination and then deleted within 6 months after the end of the Services Period defined in the customer order, actively monitored, or extended.	No deviations noted	
4.13: Customer data deletion exceptions are reviewed by senior managers monthly.	Inquired of the control owner and ascertained deletion exceptions are reviewed by senior managers monthly	No deviations noted	C1.2
	Inspected the Monthly Deletion Exceptions Review Meeting minutes and ascertained senior management reviewed customer subscriptions that were exceptions to the policy such as contract renewal negotiations, legal, or regulatory holds.	No deviations noted	
4.14: IT personnel perform restores of the production data backups to verify that system components can be recovered from system backups upon requests from customers.	Inquired of the control owner and ascertained IT Operations personnel performed restores of the production data backups to verify that system components could be recovered from system backups upon requests from customers.	No deviations noted	A1.2 A1.3

Computer Operations			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the ticket details for a sample of artifact snapshot data restore request tickets and ascertained artifact snapshot data restores were performed upon requests from customers.	No deviations noted	

Network Management

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
5.01: Firewall systems are in place to filter unauthorized inbound network traffic from the Internet.	Inquired of the control owner and ascertained firewall systems were in place to filter unauthorized inbound network traffic from the internet.	No deviations noted.	CC6.1 CC6.6 CC6.8
	Inspected the configuration of the security policy used for filtering unauthorized inbound network traffic for a sample of zone firewalls and ascertained firewall systems were in place to filter unauthorized inbound traffic from the internet.	No deviations noted.	
	Inspected the firewall configuration for a sample of firewall devices and ascertained radius authentication was set up on the firewall.	No deviations noted.	
	Inspected the company directory for a sample of users with ability to modify firewall configuration through radius authentication and ascertained the users were appropriate based on job title and organizational unit.	From January 1, 2022 to June 13, 2022: Deviations noted: For three (3) of the fifteen (15) users selected for testing with administrative access to the firewall systems through Radius, their access was deemed inappropriate. From June 14, 2022 to December 31, 2022: No deviations noted.	

<table>
<tr><th colspan="4">Network Management</th></tr>
<tr><th>Control Description</th><th>Testing Performed</th><th>Results of Testing</th><th>SOC 2 Criteria</th></tr>
<tr><td colspan="4">Management response:
The identified users' administrator access within the firewall systems were revoked. Access to network devices and servers supporting the service requires users to use multi-factor authentication and traverse three levels of access controls. The risk of unauthorized access to production data is addressed through the following mitigating controls implemented at the Bastion server, operating system, and database layers:
1) Oracle utilizes OIM for Oracle Cloud personnel to submit user account requests. The system routes the requests to the appropriate approver for approval. Upon approval the access provisioning system creates the user account on the selected environment.
2) The OIM system is configured to enforce the following user account and password controls:
- Minimum password length
- Password complexity
3) Privileged access to the production servers is configured to be revoked automatically at least every 90 days.
4) Access entitlements are configured to be automatically revoked upon termination of an employee.</td></tr>
<tr><td></td><td>Inspected the company directory for a sample of users with the ability to modify firewall configuration through local administrator accounts and ascertained the users were appropriate based on job title and organizational unit.</td><td>No deviations noted.</td><td></td></tr>
<tr><td rowspan="3">5.02: The firewall systems are configured to deny any type of network connection that is not explicitly authorized by a firewall rule.</td><td>Inquired of the control owner and ascertained the firewall systems were configured to deny any type of network connections that were not explicitly authorized by a firewall rule.</td><td>No deviations noted.</td><td rowspan="3">CC6.1
CC6.6
CC6.8</td></tr>
<tr><td>Inspected publicly available documents and ascertained default rules for the type of firewall in use were implicitly set to deny traffic.</td><td>No deviations noted.</td></tr>
<tr><td>Observed a user attempt to establish a connection which was not defined by the security policy and ascertained the firewall systems were configured to deny any type of network connection that was not explicitly authorized by a firewall rule.</td><td>No deviations noted.</td></tr>
</table>

Network Management			
Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
	Observed a user establish a connection which was defined by the security policy and ascertained the firewall systems were configured to allow any type of network connection that was explicitly authorized by a firewall rule.	No deviations noted.	
	Inspected the incident tickets for a sample of incidents and ascertained deviations, problems, and errors relevant to application and system processing reported by customers were responded, escalated, and resolved and a tooling system was used to track progress through resolution.	No deviations noted.	
	Inspected the listing of users with administrator access within the firewall systems and ascertained administrator access was restricted to appropriate IT operations personnel.	No deviations noted.	
5.03: Firewall configuration change requests are approved in accordance with the Change Management Policy.	Inquired of the control owner and ascertained firewall configuration change requests were approved in accordance with the Change Management Policy.	No deviations noted.	CC8.1
	Inspected the firewall configuration tickets for a sample of firewall configuration changes and ascertained the changes were approved in accordance with the Change Management Policy.	No deviations noted.	
5.04: An intrusion detection system (IDS) is in place to analyze network device logs and report possible or actual network security breaches.	Inquired of the control owner and ascertained an intrusion detection system (IDS) was in place to analyze network device logs and report possible or actual network security breaches.	No deviations noted.	CC2.1 CC6.1 CC6.6

Network Management

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
	Inspected the network architecture diagram and ascertained an IDS was in place to analyze network device logs and report possible or actual network security breaches.	No deviations noted.	CC7.2 CC7.3
	Inspected the IDS central console configurations for a sample of production pods and ascertained an IDS was in place to analyze network device logs and report possible or actual network security breaches.	No deviations noted.	
	Inspected the company directory for a sample of users with the ability to modify IDS configurations and ascertained the users were appropriate based on job title and organizational unit.	No deviations noted.	
5.05: An intrusion detection system (IDS) is configured to log network events to the SIEM.	Inquired of the control owner and ascertained an IDS was configured to log network events to the SIEM.	No deviations noted.	CC2.1 CC6.1 CC6.6 CC7.2 CC7.3
	Inspected the IDS sensor configuration for a sample of pods and ascertained the IDS was configured to log network events to the SIEM.	No deviations noted.	
5.06: Access to Cloud Applications environments is restricted to a management VPN and bastion hosts separate from Oracle's corporate network.	Inquired of the control owner and ascertained an encrypted VPN was required for remote access to the production environment to help ensure the security and integrity of the data passing over the public network.	No deviations noted.	CC6.1 CC6.6 CC6.7

Network Management

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
	Observed a user attempt to access a bastion in the production environment without being authenticated to the OCNA VPN and ascertained the user's access was denied.	No deviations noted.	CC6.8
	Observed a user's successful authentication to a bastion in the production environment using two-factor authentication after being connected to the OCNA VPN.	No deviations noted.	
	Inspected the configurations for a sample of bastions and ascertained connection to the production environment was configured to require OCNA VPN connection.	No deviations noted.	
5.07: Web servers utilize TLS encryption for web communication sessions.	Inquired of the control owner and ascertained web servers utilized TLS encryption for web communication sessions.	No deviations noted.	CC6.1 CC6.6 CC6.7
	Inspected the TLS certificate for a sample of colocation domains and ascertained connections to web servers were configured to utilize TLS encryption for web communication sessions.	No deviations noted.	
5.08: A vulnerability scan tool is configured to run external vulnerability scans of the production environment on at least a monthly basis.	Inquired of the control owner and ascertained a vulnerability scan tool was configured to run vulnerability scans of the production environment on at least a monthly basis.	No deviations noted.	CC2.1 CC3.2 CC5.1

Network Management			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the vulnerability scan configuration for a sample of colocations and ascertained a vulnerability tool was configured to run external vulnerability scans on at least a monthly basis.	No deviations noted.	CC5.2 CC6.8 CC7.1 CC7.2 CC7.4
	Inspected the monthly vulnerability scan reports for a sample of weeks and ascertained the vulnerability scans ran.	No deviations noted.	
	Inspected the monitoring documentation for a sample of months relating to vulnerabilities identified by the external vulnerability scans and ascertained vulnerabilities were tracked and monitored.	No deviations noted.	
	Inspected the company directory for a sample of users with the ability to modify the scan configurations and ascertained the users were appropriate based on job title and organizational unit.	No deviations noted.	
5.09: A third-party vendor performs an external penetration assessment on an annual basis.	Inquired of the control owner and ascertained a third-party vendor performed an external penetration assessment on an annual basis.	No deviations noted.	CC2.1 CC3.2 CC4.1 CC4.2 CC5.1
	Inspected the third-party penetration assessment report and ascertained external penetration assessment was completed on an annual basis.	No deviations noted.	

Network Management			
Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
	Inspected the third-party penetration assessment report and ascertained issues identified were being tracked in the Security Audit Analysis Response report through resolution.	No deviations noted.	CC5.2 CC6.8 CC7.1 CC7.2 CC7.4
5.10: Oracle Cloud Service Center (OCSC) personnel are staffed 24 hours per day to monitor alerts.	Inquired of the control owner and ascertained Oracle Cloud Service Center (OCSC) personnel were staffed 24 hours per day to monitor alerts.	No deviations noted.	CC4.1 CC4.2 CC7.1 CC7.2 CC7.3 CC7.4 A1.1 A1.2
	Inspected the Oracle personnel schedule for a sample of days and ascertained Oracle personnel were staffed 24 hours per day to monitor alerts for commercial pods.	No deviations noted.	
	Inspected the Oracle personnel schedule for a sample of days and ascertained Oracle personnel were staffed 24 hours per day to monitor alerts for UK government pods.	No deviations noted.	
	Inspected the Oracle personnel schedule for a sample of days and ascertained Oracle personnel were staffed 24 hours per day to monitor alerts for US government pods.	No deviations noted.	

Network Management

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
5.11: On a monthly basis, vulnerabilities identified as part of vulnerability scans and external penetration tests are reported to the Executive Vice President of Applications Development to track the vulnerabilities through resolution.	Inquired of control owner and ascertained on a monthly basis, vulnerabilities identified as part of vulnerability scans and external penetration tests were reported to the Executive Vice President of Applications Development to track the vulnerabilities through resolution.	No deviations noted.	CC3.2 CC4.1 CC4.2 CC5.1 CC5.2 CC6.8 CC7.1 CC7.2 CC7.4 CC7.5
	Inspected meeting agendas and calendar invitations for a sample of months and ascertained a monthly meeting occurred to report to the Executive Vice President of Application Development security compliance matters including high and critical vulnerabilities and penetration tests.	No deviations noted.	
5.12: Deviations, problems, and errors relevant to application and system processing reported by customers are responded, escalated, and resolved. A tooling system is used to track progress through resolution.	Inquired of the control owner and ascertained deviations, problems, and errors relevant to application and system processing reported by customers were responded, escalated, and resolved and a ticketing system was used to track progress through resolution.	No deviations noted.	CC6.8 CC7.1 CC7.2 CC7.3 CC7.4
	Inspected the incident tickets for a sample of customer-identified incidents and ascertained deviations, problems, and errors relevant to application and system processing reported by customers were responded, escalated, and resolved and a tooling system was used to track progress through resolution.	No deviations noted.	

Policy and Communication			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
6.01: 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.	Inquired of the control owner and ascertained 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.	No deviations noted.	CC1.1 CC1.5 CC5.3
	Inspected the Authority, Enforcement, Exceptions, and Violations Policy and ascertained it specified that Oracle employees and contingent workers were required to comply with all laws, regulations, contractual obligations, and Oracle policies and that Non-compliance with laws, regulations, and Oracle policies may result in disciplinary action up to and including termination.	No deviations noted.	
	Inspected the Authority, Enforcement, Exceptions, and Violations Policy and ascertained it specified that exceptions to an information security policy must be made as directed in the Corporate Security Exception Management Process.	No deviations noted.	

Policy and Communication			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
6.02: The Supplier Code of Ethics and Business Conduct and the Supplier and Physical Security Standards sets out the requirements that Suppliers and vendors are required to adhere to.	Inquired of the control owner and ascertained the Supplier Code of Ethics and Business Conduct and the Supplier and Physical Security Standards sets out the requirements that Suppliers and vendors are required to adhere to.	No deviations noted.	CC1.1 CC2.3 CC5.3 CC6.4 CC9.2
	Inspected the Supplier Code of Ethics and Business Conduct and Oracle Supplier Information and Physical Security Standards and ascertained it defined requirements that Suppliers and vendors are required to adhere to.	No deviations noted.	
6.03: The Oracle Data Processing Agreement describes the parties' respective roles for the processing and control of personal data that customers provide to Oracle. The policy is publicly available and indicates the date of the most recent update.	Inquired of the control owner and ascertained the Oracle Data Processing Agreement described the parties' respective roles for the processing and control of personal data that customers provided to Oracle and that the policy was publicly available and indicated the date of the most recent update.	No deviations noted.	CC2.3 CC5.3 CC9.2 C1.1
	Inspected the Oracle Data Processing Agreement and ascertained it described the parties' respective roles for the processing and control of personal data that customers provided to Oracle, was publicly available and indicated the date of the most recent update.	No deviations noted.	

Policy and Communication			
Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
6.04: Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, security, operation, maintenance, and monitoring of SaaS services.	Inquired of the control owner and ascertained organizational charts were in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, security, operation, maintenance and monitoring of SaaS services.	No deviations noted.	CC1.3
	Inspected the organizational chart and ascertained it was in place and communicated the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, security, operation, maintenance and monitoring of SaaS services.	No deviations noted.	
6.05: The security, confidentiality, privacy, and availability commitments for Oracle's Cloud Applications are included in service descriptions and service-level agreements with customers. A summary is published on Oracle's public website.	Inquired of the control owner and ascertained the entity's security, availability, and confidentiality commitments and the associated system requirements were documented in externally facing customer documents.	No deviations noted.	CC2.2 CC2.3 CC5.3 C1.1

Policy and Communication			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the Oracle Cloud Service Agreement and Oracle Cloud Hosting and Delivery Policies, which were available via an external website to customers and ascertained they contained information defining the entity's security, confidentiality, privacy and availability commitments.	No deviations noted.	
6.06: Documented escalation procedures for reporting security, availability, and confidentiality incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inquired of the control owner and ascertained documented escalation procedures for reporting security, availability, and confidentiality incidents were provided to internal and external users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	No deviations noted.	CC2.2 CC2.3 CC4.2 CC5.3 CC7.2 CC7.3 CC7.4 CC7.5 CC9.1 CC9.2 C1.1
	Inspected the contents of the Information Security Incident Reporting and Response Policy and the Global Information Security page and ascertained they included escalation procedures for reporting security, availability, and confidentiality incidents to guide internal and external users in identifying and reporting failures, incidents, concerns, and other complaints.	No deviations noted.	
6.07: Documented policies and procedures are in place to guide personnel in the retention of client data.	Inquired of the control owner and ascertained documented policies and procedures were in place to guide personnel in the retention of client data.	No deviations noted.	CC1.5 CC2.2 CC5.3

Policy and Communication			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the Oracle Information Management and Records Retention Policy and ascertained it included procedures to guide personnel in the retention of client data.	No deviations noted.	CC6.5 C1.1 C1.2
6.08: Oracle develops, documents, and disseminates an information protection policy which defines the requirements for classifying and handling confidential and customer information.	Inquired of the control owner and ascertained Oracle develops, documents, and disseminates an information protection policy which defines the requirements for classifying and handling confidential and customer information.	No deviations noted.	CC1.1 CC2.2 CC5.3 C1.1 C1.2
	Inspected the Oracle Information Protection Policy and ascertained it included requirements for the classification and handling of confidential information.	No deviations noted.	

Entity-Level Controls

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
7.01: The Oracle Corporate Governance Guidelines and Committee Charters for the Finance and Audit Committee, Independence Committee, Compensation Committee, and the Nomination and Governance Committee are publicly available and indicate the date of their most recent updates.	Inquired of the control owner and ascertained the Oracle Corporate Governance Guidelines and Committee Charters for the Finance and Audit Committee, Independence Committee, Compensation Committee, and the Nomination and Governance Committee were publicly available and indicated the date of their most recent updates.	No deviations noted.	CC1.1 CC1.2 CC2.3
	Inspected the corporate website and ascertained the Corporate Governance Guidelines and charters for the Finance and Audit Committee, Independent Committee, Compensation Committee, and Nomination and Governance Committee were posted and available to both internal employees and external customers and included the date of their most recent update.	No deviations noted.	
7.02: Oracle's Integrity Helpline provides a resource for reporting concerns or asking questions regarding compliance and ethics at Oracle. A summary of reported items is presented to the Finance and Audit Committee as appropriate.	Inquired of the control owner and ascertained Oracle's Integrity Helpline provided a resource for reporting concerns or asking questions regarding compliance and ethics at Oracle and a summary of reported items was presented to the Finance and Audit Committee as appropriate.	No deviations noted.	CC1.1 CC3.3
	Inspected the Oracle internal site and ascertained a link and phone numbers were available to report concerns or violations of the Code of Ethics, Business Conduct, or other issues online or by phone.	No deviations noted.	

Entity-Level Controls			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
	Inspected the most recent Finance and Audit Committee meeting agenda and ascertained it included the presentation of reported items.	No deviations noted.	
7.03: Organizational roles and responsibilities for the development, management, review and approval of information security policies and practices that are identified in the Security Organization Policy. This includes overall responsibility for approving security strategy, policy and initiatives – the Oracle Security Oversight Committee (OSOC); specific responsibilities for information security, physical security, product security and security infrastructure and architecture; and liaison between Line of Business (LoBs) and Global Information Security (GIS) on information security issues by means of LoB Information Security Management/Managers (ISMs).	Inquired of the control owner and ascertained organizational roles and responsibilities for the development, management, review and approval of information security policies and practices that were identified in the Security Organization Policy and this included overall responsibility for approving security strategy, policy and initiatives – the Oracle Security Oversight Committee (OSOC); specific responsibilities for information security, physical security, product security and security infrastructure and architecture; and liaison between Line of Business (LoBs) and Global Information Security (GIS) on information security issues by means of LoB Information Security Management/Managers (ISMs).	No deviations noted.	CC1.2 CC1.3 CC1.5

Entity-Level Controls

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
	Inspected the Security Organization Policy and ascertained it contained details of the organizational roles and responsibilities for the development, management, review, and approval of information security policies and practices including overall responsibility for approving security strategy, policy, and initiatives by the Oracle Security Oversight Committee (OSOC) including specific responsibilities for information security, physical security, product security, and security infrastructure and architecture and liaisons between Line of Business (LoBs) and Global Information Security (GIS) on information security issues by means of LoB Information Security Management/Managers (ISMs).	No deviations noted.	
7.04: Business Assessment & Audit (BA&A) conducts an annual Global Risk Assessment of key business processes at Oracle. Executive management and Committee members assess risk against two factors: likelihood of control / process issues and importance to business strategy.	Inquired of the control owner and ascertained Business Assessment & Audit (BA&A) conducted an annual Global Risk Assessment of key business processes at Oracle and that an executive management and Committee members assessed risk against two factors: likelihood of control / process issues and importance to business strategy.	No deviations noted.	CC3.1 CC3.2 CC3.4 CC5.1 CC5.2
	Inspected the annual Global Risk Assessment and ascertained it occurred within the past year and included input from executive management and Committee members.	No deviations noted.	

Entity-Level Controls

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
7.05: The Oracle supplier agreement templates require its suppliers to adhere to the Supplier Code of Ethics and Business Conduct which is available on the Oracle website.	Inquired of the control owner and ascertained Oracle supplier agreement templates required its suppliers to adhere to the Supplier Code of Ethics and Business Conduct which was available on the Oracle website	No deviations noted.	CC1.1 CC2.3 CC9.2
	Inspected the Oracle website and ascertained the Supplier Code of Ethics and Business Conduct was publicly accessible.	No deviations noted.	
	Inspected the Oracle supplier agreement templates and ascertained they contained a provision which required suppliers to adhere to the Supplier Code of Ethics and Business Conduct.	No deviations noted.	
7.06: Oracle requires its partners to adhere to the Partner Code of Ethics and Business Conduct which is available on the Oracle website	Inquired of the control owner and ascertained Oracle required its partners to adhere to the Partner Code of Ethics and Business Conduct which was available on the Oracle website.	No deviations noted.	CC1.1 CC2.3 CC9.2
	Inspected the Oracle website and ascertained the Partner Code of Ethics and Business Conduct was publicly accessible.	No deviations noted.	
	Inspected the Partner portal for a sample of partners selected from the Partner tool and ascertained the partner agreed to the Partner Code of Ethics and Business Conduct and the partner was in an approved status.	No deviations noted.	

Entity-Level Controls

Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
7.07: The Oracle Information Security Incident Reporting and Response Policy specifies the process for classification, prioritization and escalation of security incidents including reporting, managing and responding to security incidents including, as applicable, notification of affected customers. This policy also outlines the responsibilities of each team during the process.	Inquired of the control owner and ascertained the Oracle Information Security Incident Reporting and Response Policy specifies the process for classification, prioritization and escalation of security incidents including reporting, managing and responding to security incidents including, as applicable, notification of affected customers and the responsibilities of each team during the process.	No deviations noted.	CC7.3 CC7.4
	Inspected the Oracle Public Cloud Risk Management Standard and ascertained the policy specifies the process for classification, prioritization and escalation of security incidents including reporting, managing and responding to security incidents including, as applicable, notification of affected customers and the responsibilities of each team during the process.	No deviations noted.	
7.08: Risks mitigation policies and procedures are in place to guide personnel in performing risk assessments and mitigation.	Inquired of the control owner and ascertained risks mitigation policies and procedures were in place to guide personnel in performing risk assessments and mitigation.	No deviations noted.	CC2.1 CC2.2 CC3.1 CC3.2 CC3.3 CC3.4 CC5.1 CC5.2 CC9.1 CC9.2
	Inspected the Oracle Public Cloud Risk Management Standard and ascertained they contained policies and procedures to guide personnel when performing the risk assessment and mitigation process.	No deviations noted.	

Entity-Level Controls			
Control Description	**Testing Performed**	**Results of Testing**	**SOC 2 Criteria**
7.09: A formal risk assessment is performed annually to identify threats and risks that could impact the security, confidentiality, or availability of the system.	Inquired of the control owner and ascertained a formal risk assessment was performed annually to identify threats and risks that could impact the security, confidentiality, or availability of the system.	No deviations noted.	CC2.1 CC3.1 CC3.2 CC3.3 CC5.1 CC5.2 CC9.1
	Inspected the risk assessment and ascertained it was performed during the year, the identified risks were rated using a risk evaluation process, and were formally documented with mitigation strategies, for management review.	No deviations noted.	
7.10: The Oracle Corporation Board of Directors maintains a charter for the Committee on Independence Issues, which defines responsibilities and duties for evaluating the independence of members of the Board.	Inquired of the control owner and ascertained the Oracle Corporation Board of Directors maintains a charter for the Committee on Independence Issues, which defines responsibilities and duties for evaluating the independence of members of the Board.	No deviations noted.	CC1.1 CC1.2
	Inspected the charter for the Committee on Independence Issues and ascertained it defines responsibilities and duties for evaluating the independence of members of the Board.	No deviations noted.	
7.11: Oracle establishes and makes readily available to employees, suppliers, and contractors, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.	Inquired of the control owner and ascertained Oracle establishes and makes readily available to employees, suppliers, and contractors, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.	No deviations noted.	CC1.1 CC9.2

Entity-Level Controls			
Control Description	Testing Performed	Results of Testing	SOC 2 Criteria
	Inspected the Oracle Acceptable Use Policy for Systems and Resources policy and ascertained it details the rules that describe employees, suppliers, and contractors' responsibilities and expected behavior with regard to information and information system usage.	No deviations noted.	
7.12: Third party assessment organizations are contracted to assess the security controls of Oracle Cloud Applications and its environment of operation.	Inquired of the control owner and ascertained third party assessment organizations were contracted to assess the security controls of Oracle Cloud Applications and its environment of operation.	No deviations noted.	CC2.1 CC3.1 CC3.2 CC4.1 CC4.2
	Inspected the contractual agreement for a sample of audits and ascertained a third-party auditor/assessor assesses the security controls of Oracle Cloud Applications and its environment of operation.	No deviations noted.	

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
CC1.0 - Control Environment		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	1.01 1.02 1.03 6.01 6.02 6.08 7.01 7.02 7.05 7.06 7.10 7.11
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	7.01 7.03 7.10
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	1.04 6.04 7.03

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	1.01 1.03 1.04
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	1.02 6.01 6.07 7.03
CC2.0 - Communication and Information		
CC2.1	COSO Principle 13: The entity obtains or generates uses relevant, quality information to support the functioning of internal control.	2.01 4.02 4.05 4.06 5.04 5.05 5.08 5.09 7.08 7.09 7.12

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	1.03 2.01 3.01 3.02 4.03 4.04 4.10 6.05 6.06 6.07 6.08 7.08
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	3.02 6.02 6.03 6.05 6.06 7.01 7.05 7.06

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
CC3.0 – Risk Assessment		
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	7.04 7.08 7.09 7.12
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	5.08 5.09 5.11 7.04 7.08 7.09 7.12
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	7.02 7.08 7.09
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	7.04 7.08

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
CC4.0 – Monitoring Controls		
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	4.03 4.05 4.06 5.09 5.10 5.11 7.12
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	4.03 4.05 4.06 5.09 5.10 5.11 6.06 7.12

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
CC5.0 – Control Activities		
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	5.08 5.09 5.11 7.04 7.08 7.09
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	2.02 2.13 5.08 5.09 5.11 7.04 7.08 7.09
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	2.01 3.01 4.03 4.04 4.10

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
		6.01 6.02 6.03 6.05 6.06 6.07 6.08
CC6.0 – Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	2.01 2.02 2.03 2.04 2.05 2.06 2.07 2.08 2.09 2.10 2.13 3.03

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
		3.04 3.12 4.07 5.01 5.02 5.04 5.05 5.06 5.07
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	2.02 2.03 2.04 2.06 2.08 2.09 2.10 2.11 2.12 2.13

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	2.02 2.05 2.06 2.08 2.09 2.10 2.11 2.12 2.13 3.04 3.06
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	4.07 6.02
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	6.07
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	2.04 2.07 4.08 5.01

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
		5.02 5.04 5.05 5.06 5.07
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	4.07 5.06 5.07
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	2.07 4.08 5.01 5.02 5.06 5.08 5.09 5.11 5.12
CC7.0 – System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	4.04 4.05

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
		4.06 5.08 5.09 5.10 5.11 5.12
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	4.05 4.06 4.08 5.04 5.05 5.08 5.09 5.10 5.11 5.12 6.06
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	4.03 4.05 4.06

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
		5.04 5.05 5.10 5.12 6.06 7.07
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	4.03 5.08 5.09 5.10 5.11 5.12 6.06 7.07
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	4.03 4.10 4.11 5.11 6.06

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
CC8.0 – Change Management		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	2.08 2.09 3.01 3.02 3.03 3.04 3.05 3.06 3.07 3.08 3.09 3.10 3.11 3.12 4.04 5.03
CC9.0 – Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	4.03 4.10

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
		4.11 6.06 7.08 7.09
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	6.02 6.03 6.06 7.05 7.06 7.08 7.11

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	4.05 4.06 5.10
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	4.01 4.02 4.03 4.05 4.10 4.11 4.14 5.10
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	4.01 4.02 4.03 4.10 4.11 4.14

SOC 2 Criteria	Criteria Description	Oracle Specified Controls
C1.1	The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality.	2.01 4.09 6.03 6.05 6.06 6.07 6.08
C1.2	The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.	4.12 4.13 6.07 6.08