ORACLE
NETSUITE

SOC 1 REPORT

FOR

APPLICATION HOSTING SERVICES FOR THE NETSUITE SOFTWARE-AS-A-SERVICE (SAAS)

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

FOR THE PERIOD SEPTEMBER 1, 2024, TO AUGUST 31, 2025

Attestation and Compliance Services

schellman
Quality, above all.

This report is intended solely for use by the management of Oracle America, Inc., its user entities (i.e., customers) that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of those user entities (each referred to herein as a “specified user”).

If the report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Oracle America, Inc.:

Scope

We have examined the description of the Application Hosting Services for the NetSuite Software-as-a-Service (SaaS) system provided by the NetSuite global business unit of Oracle America, Inc. ("Oracle" or "service organization") throughout the period September 1, 2024, to August 31, 2025 (the "description"), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on criteria identified in "Management's Assertion" in Section 2 (the "assertion"). The controls and control objectives included in the description are those that management of Oracle believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Application Hosting Services for the NetSuite SaaS system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates whether certain control objectives specified in the description 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, as applicable, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Oracle uses a subservice organization for cloud hosting and data backup services for the NetSuite application. The description includes only the control objectives and related controls of Oracle and excludes the control objectives and related controls of the subservice organization. The description also indicates whether certain control objectives specified by Oracle can be achieved only if complementary subservice organization controls assumed in the design of Oracle's controls are suitably designed and operating effectively, along with the related controls at Oracle. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section 5, "Other Information Provided by NetSuite" is presented by management of Oracle to provide additional information and is not a part of Oracle's description of its Application Hosting Services for the NetSuite SaaS system made available to user entities during the period September 1, 2024, to August 31, 2025. Information in Section 5 has not been subjected to the procedures applied in the examination of description of the Application Hosting Services for the NetSuite SaaS system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Application Hosting Services for the NetSuite SaaS system.

Service Organization's Responsibilities

In Section 2, Oracle has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Oracle is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period September 1, 2024, to August 31, 2025. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements in the United States of America related to the examination engagement. We have complied with those requirements.

We have also applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the IAASB and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements. 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 of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4 (the "Testing Matrices").

Opinion

In our opinion, in all material respects, based on the criteria described in Oracle's assertion in Section 2:

a. the description fairly presents the Application Hosting Services for the NetSuite SaaS system that was designed and implemented throughout the period September 1, 2024, to August 31, 2025;

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period September 1, 2024, to August 31, 2025, and as applicable, subservice organization and user entities applied the complementary controls assumed in the design of Oracle's controls throughout the period September 1, 2024, to August 31, 2025; and

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period September 1, 2024, to August 31, 2025, if, as applicable, complementary subservice organization and user entity controls assumed in the design of Oracle's controls operated effectively throughout the period September 1, 2024, to August 31, 2025.

Restricted Use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of management of Oracle, user entities of Oracle's Application Hosting Services for the NetSuite SaaS system during some or all of the period September 1, 2024, to August 31, 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Schellman & Company, LLC

Columbus, Ohio
October 7, 2025

SECTION 2

NETSUITE SAAS MANAGEMENT'S ASSERTION

ORACLE
NETSUITE

NETSUITE SAAS MANAGEMENT'S ASSERTION

We have prepared the description of Oracle America, Inc.'s ("Oracle") Application Hosting Services for the NetSuite SaaS system provided by the NetSuite global business unit of Oracle America, Inc throughout the period September 1, 2024, to August 31, 2025 (the "description"), for user entities of the system during some or all of the period September 1, 2024, to August 31, 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organization and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

Oracle uses a subservice organization for cloud hosting and data backup services for the NetSuite application. The description includes only the control objectives and related controls of Oracle and excludes the control objectives and related controls of the subservice organization. The description also indicates whether certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The description indicates whether certain control objectives specified in the description 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 Oracle. The description does not extend to controls of the user entities.

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

a. the description fairly presents the Application Hosting Services for the NetSuite SaaS system made available to user entities of the system during some or all of the period September 1, 2024, to August 31, 2025, as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, as applicable:

        (1) the types of services provided including, as appropriate, the classes of transactions processed;

        (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities of the system;

        (3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

        (4) how the system captures and addresses significant events and conditions, other than transactions;

        (5) the process used to prepare reports or other information provided for entities;

        (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;

        (7) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the Oracle's controls; and

(8) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided;

ii. includes relevant details of changes to the Application Hosting Services for the NetSuite SaaS system during the period covered by the description; and

iii. does not omit or distort information relevant to the scope of the Application Hosting Services for the NetSuite SaaS system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Application Hosting Services for the NetSuite SaaS system that each individual user entity of the system and its auditor may consider important in its own particular environment; and

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period September 1, 2024, to August 31, 2025, to achieve those control objectives if, as applicable, subservice organization and user entities applied complementary controls assumed in the design of Oracle's controls throughout the period September 1, 2024, to August 31, 2025. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of Oracle;

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

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

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Oracle America, Inc. (Oracle) has been developing and selling software for nearly five decades. Oracle's productions span multiple industries and business environments. Oracle currently employees over 160,000 employees worldwide, 18,000 support personnel, and 29,000 consulting personnel.

NetSuite is a global business unit (GBU) within the parent company Oracle. This GBU is referred to herein as "NetSuite" or "the Company."

NetSuite is a provider of a suite of cloud computing business management software. NetSuite enables mid-size companies and divisions of large enterprises to manage core business operations in a single system, which includes accounting / enterprise resource planning (ERP), customer relationship management (CRM), professional services automation (PSA), and Ecommerce. NetSuite delivers the application suite over the Internet as a subscription service using the SaaS or cloud computing on-demand model.

NetSuite maintains major offices in Austin, Texas; Redwood Shores, California; Centennial (Denver), Colorado; Burlington, Massachusetts; New York, New York; Makati City (Manila), Philippines; Tokyo, Japan; Mississauga (Toronto), Canada; London, England; Brno, Czech Republic; Singapore; Hong Kong; and Sydney, Australia.

Description of Services Provided

<u>The NetSuite Solution</u>

NetSuite's business management application suite provides an integrated solution for running the core functions of a business. The NetSuite application suite shares the same customer and transaction data, enabling seamless, cross-departmental business process automation, and real-time monitoring of core business metrics. Businesses can deploy the solution as a business management suite, or deploy specific applications such as financials / ERP, CRM, and Ecommerce that can be integrated with existing application investments. In addition, the financials / ERP, CRM, and Ecommerce capabilities provide users with real-time visibility and application functionality through dashboards tailored to their particular job function and access rights. Because the NetSuite offering is delivered as a cloud solution via the Internet, it is available wherever a user has Internet access, whether on a personal computer or a mobile device. The key elements of the NetSuite application suite are included below.

One Integrated Solution for Running a Business

The NetSuite integrated business application suite provides the functionality required to automate the core operations of medium-sized businesses, as well as divisions of large companies. This unified approach to managing a business enables companies to create cross-functional business processes, extend access to customers, partners, suppliers, or other relevant constituencies; and efficiently share and disseminate information in real-time. NetSuite customers can use the application suite to manage mission-critical business processes, including financials / ERP (finance, accounting, inventory, and payroll), CRM (sales, order management, marketing, and customer support), and Ecommerce (hosting, online stores, and website analytics) functions. NetSuite has tailored their offering to meet the specific needs of customers in the wholesale / distribution, manufacturing, retail, professional services, and software industries, to better serve those customers' distinct business requirements.

Role-Based Application Functionality and Real-Time Business Intelligence

NetSuite provides role-based dashboards that offer secure, tailored access to application functionality and business information aligned with each user's specific responsibilities. These dashboards are designed to enhance operational efficiency while adhering to strict access controls, ensuring that users only interact with data and features relevant to their role. For instance, a salesperson's dashboard enables management of contacts, leads, and forecasts, while a warehouse manager's dashboard facilitates shipping, receiving, and returns processes. Integrated business intelligence tools allow users to securely monitor key performance indicators, analyze operational data for trends and opportunities, and make informed, real-time decisions to improve business outcomes based on robust access protocols.

Cloud Delivery Model

NetSuite delivers the application suite over the Internet as a subscription service via the cloud, eliminating the need for customers to buy and maintain on-premise hardware and software. The suite is designed to achieve levels of reliability, scalability, and security for their customers that have typically only been available to large enterprises with substantial information technology (IT) resources. The application architecture maintains high levels of availability, scalability for customer growth, and provides a safe and secure environment for customer business-critical data and applications.

Flexible Deployment

As larger organizations increasingly choose cloud computing software to take advantage of the resulting cost savings and business efficiencies, NetSuite's solution can also be rapidly deployed as a standalone financial / ERP solution rather than as a business management suite. This flexible deployment allows businesses to use NetSuite's cloud-based financials / ERP capabilities within line of business and integrate it with their existing CRM / Ecommerce investments or grow into the suite over time. Global enterprises with entrenched enterprise-grade financial or ERP systems at headquarters can adopt a two-tier ERP strategy by deploying NetSuite OneWorld across subsidiaries, divisions, or international operations. This approach replaces fragmented systems with a unified, cloud-based solution—offering faster deployment, lower costs, and improved standardization across the business.

Customization and Configuration

NetSuite enables users to customize the application suite to the particular needs of their businesses. The NetSuite application suite can be configured by end-users without software programming expertise. As new versions of the application suite become available, each customer's customizations and configurations are maintained with little or no additional effort or expense required.

NetSuite Offerings

The main application offering is NetSuite, which is designed to provide the core business management capabilities that most customers require. NetSuite, NetSuite OneWorld, NetSuite CRM+, and SuiteCommerce are designed for use by most types of businesses. In addition, NetSuite sells additional cloud-based application modules that customers can purchase to obtain additional functionality required for their specific business needs.

NetSuite

NetSuite, which is targeted at medium-sized businesses and divisions of large companies, provides a single platform for financials / ERP, CRM, and Ecommerce capabilities. It contains a broad array of features that enable users to do their individual jobs more effectively. In addition, because users are transacting business on the same database system, NetSuite can automate processes across departments. For example, when a sales representative enters an order, upon approval it automatically appears on the warehouse manager's dashboard as an item to be shipped and, once the item has been shipped, it automatically appears on the finance manager's dashboard as an item to be billed. Each customer can automate its key business functions across multiple departments, including sales, marketing, service, finance, inventory, order fulfillment, purchasing, and employee management. As with other of NetSuite's offerings, users access the application and data through a role-based user interface, or dashboard, tailored to deliver specific functionality and information suitable for their position.

NetSuite OneWorld

NetSuite OneWorld is targeted at global businesses and divisions of large companies operating in multinational and multi-subsidiary environments. NetSuite OneWorld allows users to utilize NetSuite's single platform for financials / ERP, CRM, and Ecommerce capabilities in multi-currency environments across multiple subsidiaries and legal entities. NetSuite OneWorld provides the ability to manage multiple companies (legal entities), with potentially different currencies, taxation rules, and reporting requirements, within a single NetSuite account.

NetSuite OneWorld has global CRM capabilities that allow for management of multi-currency quotas, forecasts, commission payments, sales tax calculations, and real-time reporting for everyone in a global sales organization from the local sales representative to the regional vice president to the head of worldwide sales. Additionally, growing companies typically employ multiple sales channels for their global sales operations, so NetSuite OneWorld allows for automation of common sales channels employed internationally including direct sales, distribution partner networks, and Ecommerce. Marketing and customer support operations can also be managed globally using NetSuite OneWorld, so processes such as lead routing and trouble ticket assignment can easily be handled across

regions or in-country, with global customer visibility and real-time measurement of marketing and service operational performance.

NetSuite CRM+

NetSuite CRM+ provides traditional sales force automation, marketing automation, customer support, and service management functionality and is targeted at a wide range of companies, including companies larger than traditional medium-sized business customers. Medium-sized businesses may use NetSuite CRM+ as an entry point into the entire suite, while larger enterprises often implement it as an alternative to more limited CRM offerings. NetSuite CRM+ incorporates order management and many other financials / ERP and Ecommerce capabilities without requiring additional integration. This application provides users with a comprehensive, real-time view of customer interactions, whether on-premise or on-demand. NetSuite CRM+ also offers incentive management, project tracking, website hosting and analytics, and partner relationship management.

SuiteCommerce

The SuiteCommerce solution is built with the idea that Ecommerce is no longer a standalone channel but a core capability for retail and business-to-business (B2B) businesses. SuiteCommerce enables businesses to move from standalone transactional channels such as online, in-store, or telephone, to an integrated commerce solution that puts the customer at the center of the experience. SuiteCommerce captures preferences and transactions into rich customer profiles to support personalized marketing, merchandising, and promotions across multiple channels.

Add-On Modules

NetSuite also offers advanced capabilities that are part of the integrated suite but are typically sold separately. These modules allow NetSuite customers to specifically augment aspects of the application suite to enhance its relevance to their businesses.

SuiteCloud Platform

SuiteCloud is NetSuite's technology platform that allows customers, partners, and developers to tailor and extend the application suite to meet specific company, vertical, and industry requirements for personalization, business processes, and best practices. It allows partners to rapidly develop and distribute cloud-based products of their own, including industry-specific versions of the application suite. NetSuite provides partners building on SuiteCloud with a website – SuiteApp.com – that enables them to market and distribute their value-added solutions to NetSuite. The application development and customization environment is designed to continue to operate across version upgrades:

- *SuiteBuilder.* SuiteBuilder is an integrated set of easy-to-use, point-and-click tools that enables customers to tailor NetSuite to fit their company and industry requirements. SuiteBuilder enables users to customize fields, records and forms and add database tables, without the need for additional programming.
- *SuiteScript.* Customers, partners, and developers use SuiteScript to extend the suite with everything from simple functions to new business process flows and even entirely new applications. SuiteScript provides the benefits of a robust architecture and on-demand hosting efficiencies for interaction between standard and custom processes. SuiteScript introduces customization and tailoring capabilities that allow complex processes with branching logic and time-based decision trees to be automated.
- *SuiteFlow.* SuiteFlow provides a graphical web-based workflow environment to create tailored business processes, custom workflows, and approval processes, through a click-not-code interface. It enables the graphical creation, viewing, and management of workflow states, actions, rules, and branching conditions.
- *SuiteBundler.* SuiteBundler enables the reuse of customizations and applications built with the SuiteCloud platform. In addition, NetSuite customers can use SuiteBundler to share their SuiteCloud customizations with others.
- *SuiteTalk.* SuiteTalk is a web services API designed to enable seamless integration between external applications and NetSuite's robust platform. SuiteTalk provides developers with standardized methods to perform essential operations such as retrieving, creating, updating, and deleting NetSuite records, and managing key business processes. It utilizes widely adopted industry-standard protocols, including REST (Representational State Transfer) and SOAP (Simple Object Access Protocol), ensuring efficient and reliable communication between NetSuite and external systems.

- *SuiteApps.* SuiteApps are native NetSuite applications developed by third-party software vendors with NetSuite's SuiteCloud developer tools. Some SuiteApps are web services integration with other systems.

Client Support and Management

NetSuite's technical support organization, with personnel in North America, Europe, and Asia, offers support 24 hours a day, seven days a week. This system allows for skills-based and time zone-based routing to address general and technical inquiries across all aspects of NetSuite services. For NetSuite's direct customers, NetSuite offers tiered customer support programs depending upon the service needs of customer deployments. For customers purchasing through resellers, primary product support is provided by NetSuite resellers, with escalation support provided by NetSuite.

System Boundaries

The scope of the review is limited to the Application Hosting Services for the NetSuite SaaS system ("SaaS" system). The specific control objectives and related control activities included within the scope of this engagement can be found in Section 4 of this document.

This report covers the NetSuite Cloud Services system, as defined by, and provided in accordance with the customer's Subscription Service Agreement (SSA). Except as otherwise excluded in this section, this report covers all available modules and enabled features of the NetSuite SaaS system, as well as core functionality such as search and reporting. The NetSuite SuiteProjects Pro PSA SaaS system and Oracle NetSuite Payroll Service ("NetSuite Payroll") are covered in their own, separate, System and Organization Controls (SOC) 1 Type 2 reports and are not covered by this report. In addition, the following are also not covered by this report: (1) any third-party add-on modules (bundled or otherwise) including those provided by NetSuite / Oracle and subject to the NetSuite / Oracle Third-Party Terms; (2) products and/or services acquired by NetSuite / Oracle or provided by NetSuite / Oracle and subject to specific addenda or amendment to NetSuite's / Oracle's SSA; (3) products and/or services provided by a NetSuite / Oracle subsidiary; (4) products and/or services provided by NetSuite / Oracle which are placed in third-party digital distribution platforms and/or online marketplaces that are intended to provide mobile apps for mobile devices*; and (5) professional services configuration and customization of customer accounts, are not covered by this report.

**While any products and/or services that are placed in third-party digital distribution platforms and/or online marketplaces are developed by NetSuite and are subject to NetSuite's system development life cycle (SDLC) methodology; NetSuite is not responsible for the functionality of the product and/or service once it is placed in the ownership of any third-party digital distribution platforms and/or online marketplaces as they are no longer under NetSuite's direct control.*

NetSuite's SaaS user entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within the SaaS system; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

Customer requests for services are initiated and authorized by user entities by directly contacting the technical support organization. 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 (SLAs).

Modifications and changes to the standard reporting functionalities by the NetSuite SaaS system are subject to NetSuite's SDLC methodology and the related control activities within the System Development and Change Management control objective noted below.

AI Functionality
This report does not cover AI Functionality or AI Systems in NetSuite Cloud Services. Customers are responsible for their use of AI Functionality.

"AI Functionality" means artificial intelligence functionality supported by AI Systems in the Cloud Services. "AI System" means a system that (a) constitutes one or more specific machine-based model(s) that is designed to operate with varying levels of autonomy, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments (b) for the functionality specified in the Oracle NetSuite Written Materials for the Cloud Services.

Infrastructure

The production information systems are located at the following geographically separated, secure data center facilities:

- Oracle Cloud Infrastructure (OCI) (UK South (uk-london)) – London, United Kingdom
- OCI (Germany Central (eu-frankfurt)) – Frankfurt, Germany
- OCI (US West (us-phoenix)) – Phoenix, Arizona
- OCI (US East (us-ashburn)) – Ashburn, Virginia
- OCI (US Midwest (us-chicago)) – Chicago, Illinois
- OCI (Australia (ap-melbourne)) – Melbourne, Australia
- OCI (Australia (ap-sydney)) – Sydney, Australia
- OCI (India West (ap-mumbai)) – Mumbai, India
- OCI (India South (ap-hyderabad)) – Hyderabad, India
- OCI (Japan (ap-tokyo)) – Tokyo, Japan
- OCI (Japan (ap-osaka)) – Osaka, Japan
- OCI (UK Southwest (uk-cardiff)) – Cardiff, United Kingdom
- OCI (Netherlands West (eu-amsterdam)) – Amsterdam, Netherlands
- OCI (US West (us-sanjose)) – San Jose, California
- OCI (Canada (ca-toronto)) – Toronto, Canada
- OCI (Canada (ca-montreal)) – Montreal, Canada

Each data center acts as a local primary, and as a remote secondary, to other data centers. The secondary data center provides data mirroring, disaster recovery, and failover capabilities should the primary data center become non-operational. Data center facilities are operated by Oracle, which provide earthquake and fire protection, along with heating, cooling, and backup power. The NetSuite application is multi-tenant, and servers, storage, and hard drives are built on several layers of redundancy.

A combination of custom developed, externally supported, and wholly purchased applications support the SaaS system. Customer-facing hosted applications are run on application server and database software infrastructure licensed from Oracle Corporation, which are secured separately, both logically and physically, from other components of NetSuite's internal IT infrastructure.

Prior to authenticating to any application and database servers and/or databases, privileged users must establish a secure session via NetSuite Zero Trust remote access system using multi-factor authentication to the data center provider network, followed by authentication to a bastion host. Once authenticated to the bastion host, these privileged users directly access the application and database servers and databases with a user account and password. Lightweight Directory Access Protocol (LDAP) is utilized to centrally manage application and database server operating systems access and Oracle Enterprise is utilized for database access.

A combination of hardware and software-based tools have been deployed to protect the network and help control access to and maintain the integrity of data residing on its systems, including the use of Security-Lists and Network Security Groups which act as redundant virtual firewalls to filter incoming and outgoing traffic, open source security (OSSEC) host-based intrusion detection systems (HIDS) to monitor production servers for potential or actual

security events, virtual routers, virtual firewalls, near real-time monitoring, and audit logging and reporting via a central security information and event management (SIEM) tool. Additionally, web applications provide the ability for clients to access reporting and make inquiries. The applications process within an Internet-based web server, which utilizes transport layer security (TLS) 256-bit encryption and digital certificate security.

Functional Areas of Operations

The personnel supporting the SaaS system includes, but is not limited to, the following:

- Executive management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Operations – responsible for managing, monitoring, and supporting user entities' systems and information to maintain integrity and availability.
- Security – responsible for safeguarding user entities' systems and information through application, operations, and corporate security.
- Development – responsible for development of new functionality and assistance with release management.
- Quality assurance (QA) – responsible for testing and verification of new application functionality as well as regression testing.

Data Management

Data, as defined for the NetSuite system, includes customer and transaction data and applications hosted in the NetSuite application infrastructure. Users access the NetSuite application and data through a role-based user interface or dashboard, tailored to deliver specific functionality and information appropriate for their position. Customers are restricted to their account and data related to their account.

Data within the system is generated and uploaded by customers who submit information via API connections. The transmission of confidential data is secured via a TLS encrypted Internet connection. Each customer is responsible for administering their users and data which includes the accuracy, timeliness, and completeness of the data entered into the system. Transmitted data is subsequently stored in Oracle databases. The retention and subsequent destruction procedures of SaaS production data is driven by legal and regulatory business requirements. Customers have the ability to retrieve reports related to their respective environments via the SaaS system. If an error is identified, customers contact customer support and provide feedback to correct and resolve the issues.

Customer data stored within the system is considered "Confidential – Oracle Highly Restricted" and access to this information must be strictly restricted on a demonstrated need-to-know basis. As such, this is governed by the confidentiality agreements executed between NetSuite and customers or vendors. NetSuite's information classification and handling requirements are defined in the NetSuite global business unit (NSGBU) information security standard. The standard has four categories, including: Confidential – Oracle Highly Restricted, Confidential – Oracle Restricted, Confidential – Oracle Internal, and Public. Confidential – Oracle Highly Restricted data requires the highest level of security in accordance with relevant security policies, regulations, and contractual requirements.

Subservice Organizations

NetSuite utilizes the OCI Hosting and data backup services provided by Oracle. NetSuite's SaaS system was designed with the assumption that no subservice organization controls were required in the design of NetSuite's controls; therefore, no control objectives related to NetSuite's SaaS system are dependent upon complementary subservice organization controls that are suitably designed and operating effectively, along with the related controls at NetSuite.

NetSuite SaaS system infrastructure is hosted by the cloud hosting provider OCI for the London, United Kingdom, Cardiff, United Kingdom, Frankfurt, Germany, Phoenix, Arizona, Ashburn Virginia, Melbourne, Australia, Sydney, Australia, Tokyo, Japan, Osaka, Japan, Amsterdam, Netherlands, San Jose, California, Toronto, Canada, and Montreal, Canada cloud data center regions. Oracle provides cloud hosting services for NetSuite that include, but are not limited to, physical safeguards, bandwidth services, and environmental control systems. The cloud hosting services performed by Oracle are not within the scope of this examination. The accompanying description includes

only those control objectives and related controls of NetSuite and does not include control objectives and related controls of Oracle. No subservice organizations were included in the scope of this assessment.

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

CONTROL ENVIRONMENT

The control environment at Oracle is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the Oracle Security Oversight Committee (OSOC) and operations management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Oracle's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Oracle's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well by example. Specific control activities that Oracle has implemented in this area are described below:

- A documented information security standard is in place, communicated via the company intranet, and reviewed on an annual basis. The standard states that employees must abide by Oracle's Acceptable Use Policy for Company Resources and the Oracle Code of Ethics and Business Conduct.
- Background checks are performed on new hires prior to the new hire employee's start date.
- New employees with access to the corporate network are required to acknowledge the corporate security policies.
- Temporary worker providers must sign a confidentiality agreement before access to the corporate network can be granted to their provided resources.
- Signed nondisclosure agreements are required before sharing information designated as confidential with third-party service providers.
- An employee sanction procedure is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.

OSOC Oversight

Oracle's control consciousness is influenced by its audit activities and the OSOC. Attributes include the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors. Specific control activities that Oracle has implemented in this area are described below:

- Security organization policies are formally documented that describe the OSOC responsibilities and oversight of management's system of internal control.

- The OSOC is chaired by members who are independent from NetSuite and are objective in evaluations and decision making.
- OSOC meetings are held on an annual basis to review internal control performance.

Organizational Structure and Assignment of Authority and Responsibility

Oracle's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Oracle's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and designated lines of reporting. Oracle has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Oracle's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Specific control activities that Oracle has implemented in this area are described below:

- 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, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated as needed.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- An executive management team that is comprised of security personnel and executive staff has been established to guide the company in managing security risks.
- OSOC meetings are held on an annual basis to review internal control performance.
- Management has assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the security architect.

Commitment to Competence

Oracle management defines competence as the knowledge and skills necessary to accomplish tasks that define employee's roles and responsibilities. Oracle's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that Oracle has implemented in this area are described below:

- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- A documented information security standard is in place, communicated via the company intranet, and reviewed on an annual basis. The standard identifies information required to support the functioning of internal control and achievement of objectives.
- New employees with access to the corporate network are required to acknowledge the corporate security policies.
- Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate security policies.

Accountability

Oracle's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's

attitudes toward information processing, accounting functions, and personnel. Specific control activities that Oracle has implemented in this area are described below:

- Management formally documents an organizational strategy within information security management system (ISMS) policies and updates them on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives.
- Internal audits are performed annually in accordance with International Organization for Standardization (ISO) 27001 requirements. The audit results are documented and reviewed by management.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- OSOC meetings are held on an annual basis to review internal control performance.
- An employee sanction procedure is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.
- Management has assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the security architect.
- Management review meetings are held on an annual basis to help ensure the continuing suitability, adequacy, and effectiveness of the ISMS and include a consideration of topics that include, but are not limited to, the following:
    - changes in external and internal issues that are relevant to the ISMS;
    - nonconformities and corrective actions;
    - monitoring and measurement results;
    - audit results;
    - fulfilment of information security objectives; and
    - risk assessment results and risk treatment plan status.

Oracle's human resources (HR) policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Oracle has implemented in this area are described below:

- Management has established pre-hire screening procedures to govern the new hire process for employees.
- Management has established employee termination procedures to govern the termination process.

Risk Assessment

Objective Setting

The risk assessment process involves a dynamic process that includes identification and analyzation of risks that pose a threat to the organization's ability to perform the in-scope services. The process first starts with determining the organization's objectives as these objectives are key to understanding the risks and allows identification and analysis of those risks relative to the objectives. Management formally documents organizational strategy within ISMS policies and updates them on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives. Management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to help ensure they align with company's mission and are utilized as part of the annual risk assessment process. Additionally, management holds quarterly company-wide strategy meetings to discuss and align internal control responsibilities, performance measures, and incentives with company business objectives.

Risk Identification and Analysis

Management is responsible for identifying the risks that threaten achievement of the control objectives stated in the management's description of the services organizations systems. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. Management has thoughtfully identified control activities when designing, implementing, and documenting their system in order to mitigate risk and achieve the control objectives within scope.

Oracle establishes 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, an entity's risk-assessment process should consider risks that may occur. It is important that risk identification be comprehensive. Oracle has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities.

As part of an overall risk management strategy, NetSuite conducts information security risk assessments. Such assessments include technical reviews of threats, vulnerabilities, and risk mitigation practices. Asset tracking and identification is coupled with threat reviews to construct a threat assessment. Technical vulnerabilities are identified using network monitoring tools, centralized patch management, penetration tests, and other technical tools, by both internal groups and contracted third parties. Additionally, NetSuite relies on a documented practice-based protection strategy to mitigate identified risks.

Security stakeholders perform a risk assessment on an annual basis that includes an evaluation of control activities, business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Additionally, management identifies and assesses changes that could significantly impact the system of internal control during the annual risk assessment process.

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; and
- considering how the risk should be managed, including an assessment of what actions need to be taken.

Risk analysis is an essential process to the entity'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 costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring.

It is necessary to consider all the possible incidents and the impact each may have on the organization's ability to continue to deliver its normal business services. Risk assessment examines the possibility of serious situations disrupting the business operations and the potential impact of such events.

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
- 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

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud, including incentives, pressures, opportunities, and rationalizations to commit fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud; therefore, documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. Additionally, the risk assessment that is performed on an annual basis considers the potential for fraud.

Risk Mitigation

Business Disruption Risk Management

Risk mitigation activities include the ability to identify, select, and develop activities that sufficiently meet the identified risks. The organization has documented policies and procedures to guide personnel throughout this process. The risk assessment and mitigation activities also addresses the risks arising from potential business disruptions.

NetSuite has a documented process to ensure its disaster recovery and business continuity plans align with customer commitments. Operations personnel perform data restoration tests on a monthly basis to help ensure the recoverability of production data. For disaster recovery purposes, a subset of databases is restored from a secondary facility twice a year to validate the restore process and integrity of backup media and data.

In addition to the annual risk assessment process, NetSuite performs a business impact analysis (BIA) on an annual basis to identify critical business functions and describe what would be necessary to recover those functions, in the event of a disaster or disruption in service. NetSuite utilizes the BIA to identify how quickly essential business functions and/or processes have to return to normal or near-normal operations and to allow for the prioritization of available equipment and resources, were an event to occur.

Vendor Risk Management

Vendors and business partners are considered in risk assessment and mitigation activities. A vendor management policy outlines specific requirements for engaging vendors and business partners, the due diligence process before onboarding, ongoing monitoring of compliance, and contract termination procedures. This policy is reviewed and updated as needed during the annual risk assessment process. Prior to sharing information designated as confidential with third parties, nondisclosure agreements of confidentiality and protection are required to be signed.

NetSuite retains and reviews the cloud hosting provider's third-party audit reports, such as SOC reports, to monitor the design and operating effectiveness of the cloud hosting provider's relevant controls. If risks are raised beyond an acceptable level, NetSuite addresses the issues with the cloud hosting provider.

Integration with Control Objectives

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 that the actions associated with those risks are carried out properly and efficiently.

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Selection and Development of Control Activities

Control activities are a part of the process by which NetSuite strives to achieve its business objectives. NetSuite has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, control activities are established to meet the overall objectives of the organization.

The establishment of control activities is inclusive of general control activities over technology. The management personnel of NetSuite evaluate the relationships between business processes and the use of technology to perform those processes to determine the dependencies on technology. The security management processes for the technology, along with other factors, are analyzed to define and establish the necessary control activities to achieve control objectives that include technology.

The establishment of the control activities is enforced by defined policies and procedures that specifically state management's directives for NetSuite personnel. The policies serve as the rules that personnel must follow when implementing certain control activities. The procedures are the series of steps the personnel should follow when performing business or technology processes and the control activities that are components of those processes. After the policies, procedures and control activities are all established, each are implemented, monitored, reviewed, and improved when necessary.

NetSuite's control objectives and related control activities are included below and also in Section 4 (the "Testing Matrices") of this report.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

System Development and Change Management

Control Objective: Control activities provide reasonable assurance that changes to production application systems and programs are properly authorized, tested, approved, implemented, and documented.

NetSuite application development activities follow a standard SDLC methodology, which is used for software development and change management activities. NetSuite's SDLC standards and procedures govern the feature development and bug management processes.

Project Initiation

Application development and modification requests can be initiated for two purposes: (1) to enhance the software product (either adding a new functionality, modifying an existing functionality to improve ease of use or to extend the feature's abilities), or (2) to correct software defects. Enhancement suggestions come from multiple sources including customers, partners, employees, product management, software development, or software QA.

Major application development and modification projects are initiated by the Product Generation Process (PGP) cell and carried out by the product development teams, known as scrum teams. The PGP cell is comprised of executive management, management members from product management, software development, QA, release engineering, data center operations, and performance teams. The PGP cell meets periodically to discuss the status of projects and to identify and resolve issues. The results of the meetings are documented within meeting minutes. The scrum teams are cross-functional teams, comprised of representatives from each functional group involved in the implementation and maintenance of product features (development, QA, product management, and technical publications). Scrum teams meet as often as daily when new features are being developed and weekly thereafter.

NetSuite releases two major feature releases per year. NetSuite also releases add-on modules that provide industry and vertical-specific solutions, delivered in a repeatable, cost-efficient fashion, using its SuiteBundle technology. These add-on modules are developed using NetSuite's customization platform, packaged into a SuiteBundle, and can be delivered to individual customers. Changes to these bundles are documented and tracked in a bundle release record (BRR). Additionally, NetSuite releases small sets of defect or bug fixes, referred to as minor releases, every two to three weeks. When required, NetSuite can also release individual emergency bug fixes called "hot pushes" directly into the production environment for defects which need to be fixed before the next scheduled minor release. SuiteApps releases are made available to customers via the SuiteApps marketplace. Changes to the SuiteApps releases are documented and tracked in a SuiteApps release record (SARR).

Feature Releases

Feature releases include a set of features and bug fixes for the NetSuite application. Individual features are documented in feature records. Scrum teams provide a prioritized list of features being considered, and PGP approves the specific features to be developed and implemented. The overall feature release schedule is determined and authorized by the PGP cell.

During planning phases, the scrum teams collaborate on new feature requirements, which often involve iterative user workflow discussions, mock-ups, and demonstrations. For features which are eventually approved, the feature requirements are reviewed and prioritized at scrum team meetings.

At least one QA representative is assigned to each feature. QA engineers use the feature requirements to develop and execute test plans and document test results for the new features. Feature requirement documents and test plans evolve during the feature development and test cycle. Prior to implementing to production, QA provides approval within the feature record to integrate the feature into a code release batch.

In addition to testing the new functionality of features, QA also executes manual and automated regression tests for the entire feature release prior to implementation to production, which is documented within the product maintenance record (PMR) or BRR, as appropriate. Following final testing and approval for release to production, NetSuite upgrades customers to the new feature release version using a phased rollout approach, which means the application is upgraded to increasingly larger segments of the customer base until each customer has the newest version of the application.

The move to production is performed by the release team only after receiving approval from QA. After the implementation of feature, bundle releases, and SuiteApps releases, QA verifies that the feature, bundle releases, and SuiteApps release are operating as expected in production by performing post-implementation reviews.

Release notes updated user guides, and "sneak peaks" documentation are released to customers to describe how the new functionality works. User guides are updated for significant feature additions and extensions, published online, and communicated to the user base.

Minor Releases

Minor releases contain defect fixes for the NetSuite application. The overall minor release schedule is determined and authorized by the PGP cell.

Defects are documented in issue tickets and, when initiated from a customer case, cross-linked to that case. Defect fixes are typically released in either minor releases or in feature releases.

For issues initiated by personnel outside of the development team, QA confirms that the defect is valid then routes the issue to development. If a developer understands a defect / issue, the developer is authorized to bypass QA investigation and proceed with the development process. After the defect undergoes resolution and peer review by the development team, QA tests the resolution in a QA environment and verifies this within the issue record. Only after a successful resolution and verification will the minor release be approved by QA for release to production.

A PMR or BRR is created for each minor release. Prior to release, QA performs regression testing and documents evidence that testing was completed successfully and approved for release to production by the release team. Post-implementation, QA verifies that the minor release was implemented and operating correctly in production.

Hot Pushes (Emergency Bug Fixes)

Hot pushes resolve defects requiring immediate release to the production environment, most often to remediate an issue impacting a single customer or very limited number of specific customers. Scrum teams perform an analysis to determine the priority and risk of a potential hot push. Only high value and low risk changes are hot pushed to production.

Hot pushes are released to the production environment after they have been resolved, tested, reviewed, and approved to go-live. There is a list of authorized development and QA managers who can approve an issue to be a hot push candidate, based on the urgency of the fix, and the technical risk of the resolution. After a hot push candidate has been verified by the QA engineer, that QA engineer must explicitly document within the issue record that the fix is authorized to be released directly to the production environment.

Standard Reports

Standard reports are developed to give customers various views and details related to their data. Various teams are utilized to develop standard reporting based on demands of a broad customer base. Such reports and any related modifications are subjected to NetSuite's SDLC process to help ensure the accuracy of the data and that it is presented as intended. Standard reports are in read-only formats and secured to prevent unauthorized and inadvertent alterations.

Customers can opt to have their own customized reports; however, responsibility for the accuracy of customized reports rests with the customer.

Infrastructure Changes

Infrastructure changes include changes to NetSuite's production servers and databases supporting the NetSuite application and customer data and are managed by the engineering operations department. The release cell is responsible for the management, planning, and organization of upgrades and maintenance activities. The release cell is made up of staff of the various operations teams, such as the following: the release-deployment, systems engineering, network administrators, and database teams. The release cell is authorized to review and approve proposed changes (see PMR process). Other operations management and departments are involved on an as-needed basis, depending on the specific issues being addressed. Infrastructure changes are documented in PMRs. Authorization requirements are specified on the PMR.

Release cell meetings are held on a daily basis to discuss upcoming infrastructure changes. During these meetings, proposed changes are discussed, reviewed, and authorized by release cell authorized approvers. Generally, non-emergency infrastructure changes are scheduled and planned at least one week prior to being released into production. Some non-customer facing changes may be planned and scheduled for execution on a shorter notice.

Release cell approves changes unless classified as pre-authorized, automated, or emergency. Release cell defines the other required authorizations in the PMR, which could include authorization from PGP cell, security, operations,

performance, or QA. Additionally, if QA sign-off is required after the changes are completed, this requirement is also specified on the PMR.

In addition to testing, peer reviews of the exact steps which are to be followed to implement changes are performed to verify that the systems and implementation steps are complete and accurate. Completion of authorizations and reviews are indicated on the PMR. Once the required authorizations and reviews have been completed, the action owner will implement the change at the designated time. When required, QA verifies that the infrastructure change was implemented and that the relevant systems are operating as expected. If additional testing is required to be performed by engineering operations, it is documented within the PMR.

Segregated Environments and Access Restrictions

NetSuite has separate environments for its development, testing, and production activities. A version control tool, GitLab, is used to restrict access to program source code to appropriate individuals and provides controlled software versioning. Developers do not have write access to production. Write access to the production environment is restricted to authorized personnel through logical security controls, Security-Lists and Network Security Groups. The ability to release code to production is restricted to the release team.

Additionally, the ability to implement Bundles or SuiteApps to production is restricted to user accounts accessible by authorized release team personnel.

Logical Security

Control Objective: Control activities provide reasonable assurance that logical access to data, applications, system data, and networks is restricted to properly authorized individuals, and that security violations are identified, followed up, and resolved on a timely basis.

NetSuite's application systems are implemented in multi-tier client server architecture with server systems maintained by NetSuite. Customers use the Internet to access the applications where data exchange and transactions are processed in real-time. Logical security tools and/or native platform level security are used to help secure the platforms used by NetSuite to support computer operations. At a minimum, each platform has authentication controls requiring users to provide a valid user account and password to obtain access to platform resources. Additionally, access restrictions are in place on each platform that defines user access to specific resources by user or group level membership. Operations manages logical access for systems with customer data. This consists of the production environment hosting the database servers and application servers for NetSuite customers' application instances. Oracle Global IT (GIT) manages logical access for the corporate environment. NetSuite has a Business and Technology Services department that manages the NetSuite identity cloud service (IDCS) and NetSuite Zero Trust remote access system.

NetSuite employees are required to initially authenticate to the network through NetSuite Zero Trust remote access system with their unique user account and password (single sign-on identification or SSO-ID). Upon authentication to the network, remote users must log in to Oracle corporate VPN to access corporate resources. The login process and remote access systems are managed by Oracle GIT and NetSuite Business and Technology Services. Privileged users (administrators, operations personnel, etc.) requiring access to the application servers or database servers that host customer data must authenticate to NetSuite Zero Trust remote access system. NetSuite Zero Trust remote access system requires authorized entitlement and group role. Once users connect and authenticate to the production network, they are required to provide another set of credentials to access the application and database servers and/or databases. The logical security of the application and database servers is managed by operations. Due to the multi-layered structure of NetSuite's system architecture, logical access controls are split into two main categories:

- Corporate environment – logical access controls that are unique to the corporate environment (Oracle corporate network or Oracle corporate VPN, or NetSuite Zero Trust remote access system).
- Production environment – logical access controls that are unique to the production environment (application and database servers and databases access via NetSuite Zero Trust remote access system).

Logical access controls that are common to both corporate and production environments are documented in the "Policies and Standards" section below.

Policies and Standards

Information Security Standard

NetSuite has established a comprehensive information security standard that outlines security principles, objectives and actions required to protect the confidentiality, integrity, and availability of data. The standard is reviewed, at least annually, and changes are approved by NetSuite management.

It encompasses multiple security domains, including, but not limited to:

- Organization of information security
- Information asset management
- Human resources security
- Physical and environmental security
- Network security management
- Logical access control
- Information security incident management
- Business continuity management
- Legal compliance
- NetSuite universal SDLC

Security Awareness

NetSuite has established Oracle policy-aligned security standards that govern the administration of user access for employee new hires, transfers, and terminations. These standards require that user access be granted on a 'need-to-know' basis, commensurate with job responsibilities. NetSuite's employee agreement summarizes the security measures that employees are required to comply with. Newly hired employees and contractors are required to acknowledge the corporate security policies upon hire. Annual training cycles help ensure that NetSuite employees maintain currency on key security topics. Additionally, temporary worker providers must sign a confidentiality agreement before access to the corporate network can be granted to their provided resources.

User Credentials

NetSuite users are restricted via their user accounts and associated passwords with activities restricted to specific system resources. User accounts are assigned according to standard naming conventions and password security parameters have been established on the network, operating systems, and databases in compliance with the information security standard.

NetSuite also uses multi-factor authentication which provides an added layer of security for logging in to NetSuite application. The multi-factor authentication requires a user to enter a verification code after their NetSuite credentials.

Corporate Environment

User Administration Controls: Employee New Hires

Security standards have been established for access to NetSuite's corporate network. The Business and Technology Services department is notified by HR or the employee's manager of the new employee through the NetSuite application ticketing system. The network administrator will then set up the new user account with the appropriate access rights based on an authorized request from HR. Requests indicate whether access is to be granted based on job responsibility and department or assignment to specific groups and resources where additional approval is required. New hires are automatically provisioned with a NetSuite identity account after HR initiates employee onboarding in the HR system.

User Administration Controls: Terminations

Upon termination of employment, NetSuite corporate network access is disabled by Business and Technology Services. When an employee changes job responsibilities due to a transfer, the hiring manager / supervisor is responsible for notifying Business and Technology Services to help ensure user account access privileges are appropriately modified. Access to the NetSuite production environment supporting customer application data is automatically disabled upon termination of employment. Access to the NetSuite production environment supporting customer application data is automatically disabled upon termination of employment.

Periodic Review of Access

The Business and Technology Services department performs monitoring of users on the NetSuite production environment to identify unauthorized or terminated users. All access groups and permissions are automatically disabled via a scheduled batch job.

Antivirus Protection

Antivirus software clients are installed on workstations to help detect and prevent the transmission of data or files that contain virus signatures recognized by the antivirus software. The antivirus software is configured to monitor for updates to antivirus definitions and to update the workstations on a daily basis. In addition, the antivirus software is configured to perform a full scan of the workstations on a weekly basis.

Production Environment

Logical Security Controls: Access to NetSuite Databases

Customer application data resides in Oracle's relational database management system (RDBMS). Access to these files and related specialized utilities is restricted to authorized NetSuite employees.

OCI customer data residing in database tablespaces is encrypted at rest using transparent data encryption (TDE) with advanced encryption standard (AES). Access to cryptographic keys is restricted to user accounts accessible by authorized personnel. Individual secure shell (SSH) keys are required for users to authenticate to the database administrative user account.

Logical Security Controls: Production Servers

Access to the NetSuite production server environment is managed through native Oracle Enterprise Linux server operating system security controls.

Access control features include the ability to limit access by the following mechanisms:

- Groups
- Directories
- File ownership rights

User Administration Controls: Employee New Hires

For any new hire that requires access to the servers or databases supporting the customers' NetSuite applications, the department manager notifies security via a resource access form (RAF) in the ticketing system or group entitlement role for NetSuite Zero Trust remote access system in Oracle Identity Management (OIM). Within the RAF or OIM request, the department manager or director authorizes the users' access. The security department approves access to NetSuite Zero Trust remote access system, servers, and databases per the department manager's request. Privileged-level and administrative access to the production databases and servers is restricted to authorized employees based on job responsibilities.

User Administration Controls: Terminations

For terminated users with access to the servers or databases supporting customers' application instances, access is removed promptly by operations upon notification from managers or HR.

Periodic Review of Access

The Business and Technology Services (BTS) performs a quarterly access review of users with remote access on the production and database servers to identify unauthorized or terminated users. Identified discrepancies during the review are investigated and remediated. Additionally, the BTS reviews a system-generated user listing and the devices which the users have access to. Access is modified or removed as required.

System owners perform quarterly reviews of users with administrative access to databases to identify unauthorized or inappropriate access. Access is modified or removed as required.

Logical Security Controls: OCI Console

Access to the OCI Console is managed via Oracle single sign-on (SSO) database with multifactor authentication and is restricted to authorized NetSuite employees.

The Security Cell performs an access review of active users with break glass access to the OCI Console to identify unauthorized or terminated users on a semi-annual basis. Additionally, group owners perform an access review of active users with privileged non-break glass access to the OCI Console to identify unauthorized or terminated users on a quarterly basis.

Malware Protection

Malware protection controls are implemented on production servers through the use of endpoint detection and response (EDR) solutions. These tools provide continuous monitoring to detect, analyze, and respond to known and emerging malware threats that could impact the confidentiality, integrity, and availability of systems and data.

Malware definitions and detection capabilities are updated regularly to protect against evolving threats. Access to the EDR platform and related configuration settings is restricted to authorized personnel, and logging is enabled to support auditability and ongoing monitoring.

Network Security

Control Objective: Control activities provide reasonable assurance that the network architecture security controls, including network security configurations, have been implemented to safeguard IT resources and data and access to network security devices is restricted to authorized personnel.

NetSuite has implemented a variety of controls to provide network-based security measures to protect its enterprise network. The controls are in line with the NetSuite information security standard that is reviewed for updates and updated as necessary by the Security Cell and approved by NetSuite management. A combination of software-based tools has been deployed to protect the network and help control access to and maintain the integrity of data residing on its systems, including the use of virtual firewalls, virtual routers, near real-time monitoring, audit logging, and reporting.

NetSuite implements multiple layers of controls to secure, manage, and monitor the network environment. Risk levels for network areas are identified and security levels are set accordingly to maximize the level of confidentiality, integrity, and availability. Redundancy and high-availability configurations have also been designed into the controls and management functions to help ensure continuity of service.

NetSuite engages an industry-standard certificate authority (CA) to maintain and monitor the age of its certificates to help ensure that secure system access over TLS is maintained. This is managed via the Oracle Certificate Management portal maintained and owned by the Oracle PKI team. NetSuite maintains current digital certificates issued by DigiCert, Inc. for their customer-facing devices. In addition, NetSuite maintains current certificates for other web service connectivity (machine-facing applications) via trusted issuers. Lastly, web sessions to the NetSuite external network and customer web sessions are encrypted using TLS.

NetSuite's network monitoring tools include intrusion detection system (IDS), virtual firewalls, security lists, and syslog monitoring. A SIEM tool is utilized to ingest security and access-related events from production systems and configured to alert security personnel of potential security incidents. Verified security incidents are classified according to severity, documented in a ticketing system, and tracked through resolution.

Traffic to network resources is monitored and filtered based on Security-List and Network Security Group in tandem with policies configured in Illumio. Within the tool, there are established rules that limit communications through the rulesets. Illumio users are authenticated via a user account and password with the following enforced requirements: minimum password length, minimum password history, password expiration intervals, and password complexity. The ability to modify Illumio rulesets is restricted to security engineering personnel with the organization owner or global administrative roles.

Access to the production environment requires authorized remote access and enforces multi-factor authentication. Access to the application and infrastructure is managed via user groups and entitlements. Access is automatically provisioned after approval in the identity management system.

Within the NetSuite production environment, syslog captures a violation record for invalid access attempts and changes for key security events, such as changes to the security parameters. When warranted, these violations are reviewed by NetSuite security personnel and investigated. NetSuite security personnel evaluate the system logs on the application and database servers on a continuous basis. Anomalous activity incidents identified are investigated and followed up by NetSuite security personnel and findings are reported to management.

NetSuite maintains a network diagram that is updated as needed. Changes to the network configuration, traffic ruleset, Security-List and Network Security Group configurations follow the infrastructure change management procedure and require management approval and testing documented in a PMR prior to implementation.

The vulnerability management team performs vulnerability scans of the production network on at least a weekly basis to identify any possible vulnerabilities in the security of the production perimeter network. The vulnerability management team reviews the scan report and provides new findings to the operations personnel for any corrective actions to be taken, if necessary. In addition, management performs a penetration test of the perimeter network on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation, based upon factors such as potential impact, likelihood, velocity, and ease of remediation.

Virtual routers are implemented throughout the IT environment to control, and route approved types of network traffic. Security-Lists and Network Security Groups are maintained as virtual firewalls to help ensure that traffic being routed by NetSuite network resources is from approved or recognized types of traffic, sources, or services. NetSuite allows authorized NetSuite network personnel to prepare network configuration changes including Security-Lists, Network Security Group, and virtual router settings, these are reviewed in line with Change Management procedures including multi-levels of approval and security review prior to being deployed onto the network by authorized personnel.

NetSuite has micro-segmented portions of the network and implemented internal Security-Lists and Network Security Groups to further protect these segments, where deemed necessary. Access and authentication controls are implemented through OCI IAM policies, Break-Glass VPN servers, NetSuite Zero Trust remote access system, and applications to help ensure updates to the network configuration including virtual firewalls and Security-List and Network Security Group rulesets are only made by authorized personnel. Changes that are made to the network configuration including virtual routers, virtual firewalls, Security-Lists and Network Security Groups are subject to the NetSuite change management process and must be approved by authorized personnel prior to being deployed into the production environment. Changes are also reviewed after deployment into the production environment to help ensure accuracy. NetSuite tracks Security-List and Network Security Group changes within the codebase on an ongoing basis.

Virtual firewalls and routers have been implemented to provide a high level of security over the NetSuite network, applications, and data, utilizing the underlying OCI cloud industry standards with seamless failover of data traffic in the case of failure of any element. NetSuite has deployed multiple virtual firewalls in various network configurations to control network services and access to hosts within the network including external access to the NetSuite network.

NetSuite employs stateful inspection virtual firewalls at appropriate points on its network. These virtual firewalls produce logs of any activity flowing across the network segments which they separate. The firewall ruleset configuration, activity, and logs are tied to Security-Lists and Network Security Groups. Monitoring of virtual firewall events, Security-List and Network Security Group changes to detect any potential network security issues is performed by the security team as described above.

Security-Lists and Network Security Groups are configured to help ensure that traffic being routed by NetSuite network resources is from approved or recognized types of traffic, sources, or services. The ability to modify Security-List and Network Security Group configuration changes is restricted to user accounts accessible by authorized IT personnel utilizing NetSuite standard change management procedures. Security-List and Network Security Group configuration changes are logged within the SIEM tool and are reviewed on an ongoing basis by

NetSuite security personnel. Anomalies identified during the review are investigated and followed up by NetSuite security personnel, and findings are reported to management.

Data Backup and Restoration

Control Objective: Control activities provide reasonable assurance that system and application data is backed up on a timely basis and appropriately stored in a secured facility.

NetSuite has implemented data backup policies and configurations that defines customer and application data backup and recovery schedules and procedures to be followed. NetSuite performs systematic backup of its computer files and libraries based on the criticality and sensitivity of the systems and data. Backups of NetSuite's computer system files and libraries help ensure critical systems, applications, and data are available for restoration in the event of a system failure or disruption.

Procedures have been implemented to backup production program and data files according to a defined backup schedule.

The monitoring system is configured to send alert notifications to operations personnel when backup issues are identified.

A subset of databases is restored from a secondary facility on a quarterly basis as part of the disaster recovery dry run to validate the restore process and integrity of backup media and data. Additionally, A subset of databases is restored from the local cloud data center region on a monthly basis to validate the restore process and integrity of backup data. The operations team documents the details of each restore in the ticketing system and includes the procedures, results, and team resources used to verify the integrity of the restored data with the associated backup data.

ExaCS Database

The monitoring system is configured to send alert notifications to operations personnel when backup or replication issues are identified. The operations team monitors and tracks the issues to resolution in the ticketing system. Post-mortem reviews of any backup or replication problems or errors are conducted by operations on a weekly basis or as needed.

NetSuite performs and monitors the following recurring backups of the core NetSuite application to OCI block storage: daily incremental, weekly incremental, monthly incremental, and annual full.

Recurring daily incremental, weekly full, and monthly full backups of customer data to local object storage using OCI are performed and monitored. Additionally, customer data is configured to be replicated from the primary cloud data center region to an object storage in a separate data center location within the same geographical region.

The OCI backup system is configured to encrypt customer data, including backup, and replicated data, using TDE with AES. Access to cryptographic keys is restricted to user accounts accessible by authorized personnel.

ATP Database

Customer data and backup data are stored in the database with encryption at rest format, using TDE with AES. Additionally, NetSuite monitors daily backups performed by Autonomous Database.

System Availability and Uptime

Control Objective: Control activities provide reasonable assurance that system uptime is monitored on a regular basis with corrective action taken where required.

The standard NetSuite SLA provides for application availability metrics that NetSuite must meet. NetSuite has developed processes and procedures to document and track to resolution any system events that lead to interruptions in service availability. Details regarding the root cause, duration, immediate impact, residual impact, and process changes resulting from the post-mortem review are recorded in automated tracking systems and

meeting minutes. Planned downtime incidents for maintenance purposes are tracked to resolution through PMRs. Unplanned downtimes are monitored and tracked to resolution by the operations team using a system monitoring tool. The monitoring tool is configured to send automated alerts to notify the operations team of unplanned downtimes. Upon notification, the operations team researches the source and cause of downtime and notifies the database team of the affected databases. The site reliability engineering (SRE) team creates a downtime incident record in the ticketing system to document the databases affected by downtime, resolution procedures, and result. NetSuite provides timely uptime status to their customers via the status.netsuite.com website. The website is configured to provide a summary of average uptime for NetSuite customer databases on a daily basis.

Customer Authentication Requirements

Control Objective: Control activities provide reasonable assurance that customers are restricted to their specific account and data.

NetSuite employees do not have access to a customer's NetSuite application instance unless the customer has granted access to a NetSuite employee for support or in accordance with a professional service statement of work (SOW). NetSuite requires that customers manage and be ultimately responsible for their own logical access controls to their NetSuite account. The first administrator login for new customers to their NetSuite application instance is provisioned to a customer specified e-mail address, and not to a NetSuite employee or e-mail address. Authorized NetSuite personnel provision the initial administrator login using the NetSuite provisioning tool in NetSuite's application instance. The provisioning tool is configured to interface with customer databases and configure the customer's application instance without granting NetSuite employees access to the customer's application instance. Thereafter, any further user account administration is performed by the customer or their designee, as established by the customer.

NetSuite administrators can access the customer's applications only if the customer has granted the NetSuite administrator access for maintenance and support purposes, as agreed to within the SOW. Customers are restricted to their account and data related to that account. Tables housing customer data include the company ID associated with the corresponding customer. The structured query language (SQL) views used to extract data from these tables filter the data by unique company ID using the customer's login credentials. The views map the customer's viewing options to only their specific data. These access restrictions are tested before major releases to help ensure that any change or new release does not jeopardize the customer's confidential data.

Monitoring of Data Center Operations

Control Objective: Control activities provide reasonable assurance that controls at the cloud hosting provider organization are monitored, and additional NetSuite controls are applied to NetSuite contracted secured spaces.

NetSuite leverages OCI services provided by Oracle as third-party cloud hosting platform. NetSuite retains and reviews OCI audit reports, such as SOC reports, to monitor the design and operating effectiveness of the relevant controls. If risks are raised beyond an acceptable level, NetSuite addresses the issues with OCI.

Information and Communication Systems

Narratives, Procedure Manuals, and Network Diagram

NetSuite has adopted the use of narratives, procedure manuals, and network diagrams to document the end-to-end process flows of selected processes. These documents are developed to easily understand the processes by the users. These documents are made internally available to NetSuite users via NetSuite's intranet site. The security IT department has established a policy for data classification, handling, and labelling that is gathered, produced, and shared throughout the company. A data classification scheme is used to define an appropriate set of protection levels and communicate the need for special handling measures. There are four classifications: (1)

Confidential – Oracle Highly Restricted, (2) Confidential – Oracle Restricted, (3) Confidential – Oracle Internal, and (4) Public.

Communication

Documented ISMS policies and procedures are in place to guide personnel in the internal and external communications relevant to the ISMS that include, but are not limited to, the following:

- What to communicate
- When to communicate
- With whom to communicate
- Who shall communicate
- The processes by which communication shall be affected

Internal

NetSuite has implemented various methods of internally communicating information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

These methods include, but are not limited to, the following:

- A documented information security standard is in place, communicated via the company intranet, and reviewed on an annual basis. The standard identifies information required to support the functioning of internal control and achievement of objectives.
- New employees with access to the corporate network are required to acknowledge the corporate security policies.
- Temporary worker providers must sign a confidentiality agreement before access to the corporate network can be granted to their provided resources.
- Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate security policies.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- NetSuite's information security standard and incident response plan are utilized to guide personnel throughout the security incident response process.
- Formal problem management procedures have been established to address customer and internal incidents and problems reported.
- Internally reported security incidents are tracked and resolved.
- An ethics and compliance helpline and dedicated e-mail address and website are accessible by internal users to report incidents, concerns, and complaints.
- OSOC meetings are held on an annual basis to review internal control performance.
- Management review meetings are held on an annual basis to help ensure the continuing suitability, adequacy, and effectiveness of the ISMS.

External

NetSuite has also implemented various methods of communicating with external parties regarding matters affecting the functioning of internal control. These methods include, but are not limited to, the following:

- A description of the SaaS system is provided to customers and users of the system in the help section of the NetSuite system.
- The entity's security, availability, and confidentiality commitments and required obligations to its customers and other external users are documented and communicated via the following methods:
    - SSA
    - Terms of services (TOS)

- Hosting and Support Delivery Policy (H&SD)
- Data processing agreement (DPA)
- Product overview documents on the customer-facing website

- Signed nondisclosure agreements are required before sharing information designated as confidential with third-party service providers.
- Incident reporting procedures are communicated to external users via the SuiteAnswers portal.
- Customers contact the NetSuite Support group with questions, requests, or other related issues via phone call or through the SuiteAnswers portal. Issues are logged and tracked in a ticket, which includes details surrounding the problem description, issue priority, and status.
- The NetSuite system status website is configured to update the average uptime status for customer databases on a daily basis.

MONITORING

Monitoring Activities

Executive management monitors the quality of internal control performance as a normal part of their activities. Primary areas of control performance include (1) product development and release, (2) application availability, performance, and security, (3) regulatory and legal compliance, and (4) operational and financial targets.

Key tools for the monitoring and management of these areas are:

- participation on operational committees;
- monitoring key performance indicators (KPIs) and other metrics via real-time dashboards (e.g., automated defect number and severity monitoring);
- standardized system reports and automated alerts on operating effectiveness;
- regular updates from senior management;
- product scrum team meetings and roadmap reviews;
- compliance, security, and data center security cells; and
- departmental meetings.

Ongoing Monitoring

NetSuite selects, develops, and performs ongoing monitoring to ascertain whether the components of internal control are present and functioning.

Aspects of the ongoing monitoring procedures include the following:

- Unplanned downtimes are monitored and tracked to resolution through the use of downtime records in a system monitoring tool, which is configured to send automated alerts to notify the operations team of unplanned downtimes.
- The monitoring system is configured to send alert notifications to operations personnel when backup and replication issues are identified.
- A SIEM tool is utilized to ingest security and access-related events from production systems and configured to alert security personnel of potential security incidents. Verified security incidents are classified according to severity, documented in a ticketing system, and tracked through resolution.

- The Business and Technology Services department performs an access review of active users on the NetSuite network to identify unauthorized or terminated users on a weekly basis. Identified discrepancies are resolved in coordination with HR.
- The Business and Technology Services department performs an access review of active users on the production servers and databases supporting customer application data to identify unauthorized or terminated users on a quarterly basis.
- OSOC meetings are held on an annual basis to review internal control performance.
- Cloud hosting provider third-party audit reports are reviewed by the NetSuite GBU architect on an annual basis to determine the effectiveness of the cloud hosting provider control environment. Results of the reviews are documented and discussed at scrum and/or security compliance meetings.

Additional Evaluations

In addition to the monitoring activities mentioned above, management considers the need for evaluation of internal control system for a variety of reasons including major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. These evaluations vary in scope and frequency, depending on the significance of risks being addressed. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often.

These evaluations may take the form of self-assessments, often under the guidance of one or more of the security, IT compliance, internal audit, or legal departments, 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.

Internal audits are performed annually in accordance with ISO 27001 requirements. The audit results are documented and reviewed by management, including corrective action plans for identified control deficiencies. Additionally, OSOC meetings are held on an annual basis to review internal control performance.

Reporting Deficiencies

Deficiencies (nonconformities) in management's internal control system may surface from many sources, including NetSuite'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, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person, which are formally documented within NetSuite's nonconformity and corrective action process. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected in order to correct the nonconformity, deal with its consequences, and prevent its recurrence. In the event that control deficiencies are identified, management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and make the decision for addressing deficiencies based on whether the incident was isolated or requires a change in NetSuite's procedures or personnel. Should the deficiencies be classified as security incidents, NetSuite will invoke the incident response procedures. Additionally, formal problem management procedures have been established to address customer and internal incidents and problems reported. Incident reporting procedures are communicated to external users via the SuiteAnswers portal.

COMPLEMENTARY CONTROLS AT USER ENTITIES

NetSuite's SaaS system is designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to NetSuite's SaaS system to be solely achieved by NetSuite's control activities. Accordingly, user entities, in

conjunction with the SaaS system, should establish their own internal controls or procedures to complement those of NetSuite.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

Ref.	Control Activities Expected to be Implemented at User Entities	Related Control Objective
CUEC.01	User entities are expected to implement controls that ensure prompt communication of identified bugs or system functionality issues to NetSuite.	System Development and Change Management
CUEC.02	User entities are expected to implement controls that ensure user acceptance tests are conducted and that validation of such testing activities are complete, including validation of the accuracy and functionality of upgrades that have an impact to the user entity's NetSuite environment.	
CUEC.03	User entities are expected to implement controls that ensure changes to internal systems that interact with NetSuite systems are authorized, tested, approved, and implemented according to their change management procedures.	
CUEC.04	User entities are expected to implement controls that ensure the accuracy and appropriateness of the customizations which they apply to their NetSuite environment, including customized reports, are validated.	
CUEC.05	User entities are expected to implement controls that ensure security policies for interfacing, communicating with NetSuite, and accessing the NetSuite system are established and communicated to their employees and contractors.	Logical Security
CUEC.06	User entities are expected to implement controls that ensure password configuration settings and authentication requirements are established that meet their company, industry, and regulatory requirements.	
CUEC.07	User entities are expected to implement controls that ensure appropriate security controls within their NetSuite accounts are implemented. This includes, but is not limited to, evaluating, and implementing as deemed appropriate, password policy settings, mobile access policies, segregation of duties, the use of multi-factor authentication for securing sensitive roles and access, including technologies such as one-time password generating devices, IP address restrictions, VPN tunnels, etc.	
CUEC.08	User entities are expected to implement controls that ensure NetSuite is immediately notified of any actual or suspected information security breaches, including compromised user accounts.	
CUEC.09	User entities are expected to implement controls that ensure the installation and configuration of antivirus software and network firewalls for systems that interface with the NetSuite system.	Network Security
CUEC.10	User entities are expected to implement controls that ensure NetSuite is provided with an up-to-date and secure e-mail address and that the e-mails must be accepted from NetSuite at the e-mail address specified.	Customer Authentication Requirements
CUEC.11	User entities are expected to implement controls that ensure accurate and valid data is input into the NetSuite web-based application.	

NetSuite user entities are responsible for addressing additional control objectives that are not part of the scope of this report.

User entities should evaluate transaction processing risks associated with the NetSuite application and should address additional responsibilities including, but not limited to, the following:

Control Activities Expected to be Implemented at User Entities
User entities are expected to implement controls that ensure data input to the NetSuite web-based application is authorized, complete, and accurate.
User entities are expected to implement controls that ensure data output from the NetSuite web-based application is complete and accurate, such controls may include reviewing system reports, restricting access to configurations, reconciling accounts, etc.
User entities are expected to implement controls that ensure transactions processed by the NetSuite web-based applications exist, such controls may include reconciling funds and account balances to data from a source outside of the NetSuite web-based application to identify differences in actual client activity and data processed within the NetSuite web-based application.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the SaaS system provided by NetSuite. The scope of the testing included the applicable controls for the SaaS system considered to be relevant to the internal control over financial reporting of respective user entities. Schellman & Company, LLC (Schellman) conducted the examination testing over the period September 1, 2024, to August 31, 2025.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- the nature of the control and the frequency with which it operates;
- the control risk mitigated by the control;
- the effectiveness of entity-level controls, especially controls that monitor other controls;
- the degree to which the control relies on the effectiveness of other controls; and
- whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during testing. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant evidentiary matter records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible and evaluated for accuracy and completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned constitutes a test result that is the result of a change in the application of the control activity, a deficiency in the operating effectiveness of the control activity, or a disclosure related to the non-occurrence of the condition(s) that would warrant the operation of the control. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls at user entities, as this determination can only be made after consideration of controls in place at user entities, and other factors. Control considerations that should be implemented by user entities in order to complement the control activities and achieve the stated control objective are presented in the "Complementary Controls at User Entities" within Section 3.

System Development and Change Management

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to production application systems and programs are properly authorized, tested, approved, implemented, and documented.			
1.01	NetSuite application development practices follow a documented SDLC methodology which governs software development and change management activities that include, but are not limited to, the following: • Change requests • Testing of changes • Approval process • Change implementation • Emergency changes • Separation of duties	Inspected the SDLC policy and procedures to determine that documented policies and procedures were in place to guide personnel in performing software development and change management activities that included the following: • Change requests • Testing of changes • Approval process • Change implementation • Emergency changes • Separation of duties	No exceptions noted.
	Feature Releases		
1.02	Scrum teams identify, prioritize, and authorize features that are to be implemented in upcoming releases. Features are documented in a central tracking tool to monitor specific tasks to be completed within the SDLC process through implementation.	Inspected the feature records for a sample of features implemented within feature releases during the period to determine that each feature sampled was identified, prioritized, and authorized by the scrum team and was also documented within a central tracking system and monitored through implementation.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.03	QA engineers test and approve each feature in the feature release prior to implementation according to a test plan developed from the functional specifications.	Inspected the feature records for a sample of features implemented within feature releases during the period to determine that QA engineers tested and approved each feature sampled prior to implementation.	No exceptions noted.
1.04	Feature releases are documented in a PMR, regression testing is performed, and approval from QA is obtained prior to implementation to production.	Inspected the PMRs for a sample of feature releases implemented during the period to determine that each feature release sampled was documented in a PMR, tested, and approved by QA prior to implementation.	No exceptions noted.
1.05	Bundle releases are documented in a BRR, regression testing is performed, and approval from QA is obtained prior to implementation to production.	Inspected the BRRs for a sample of bundle releases implemented during the period to determine that each bundle release sampled was documented in a BRR, tested, and approved by QA prior to implementation.	No exceptions noted.
1.06	SuiteApps releases are documented in a SARR, regression testing is performed, and approval from QA is obtained prior to implementation to production.	Inspected the SARRs for a sample of SuiteApps releases implemented during the period to determine that each SuiteApps release sampled was documented in a SARR, tested, and approved by QA prior to implementation.	No exceptions noted.
1.07	After the release team implements a feature release, bundle release, or SuiteApps release to production, QA verifies that the new code version is implemented and operating successfully.	Inspected the PMRs for a sample of feature releases implemented during the period to determine that QA performed a post-implementation review for each feature release sampled.	No exceptions noted.
		Inspected the BRRs for a sample of bundle releases implemented during the period to determine that QA performed a post-implementation review for each bundle release sampled.	No exceptions noted.
		Inspected the SARRs for a sample of SuiteApps releases implemented during the period to determine that QA performed a post-implementation review for each SuiteApps release sampled.	No exceptions noted.
	Minor Releases		
1.08	As part of the scheduled minor release, individual bugs are investigated and authorized by QA for development. Once the bug is fixed, QA tests and approves the bug fix prior to implementation.	Inspected the issue records for a sample of bug fixes implemented during the period to determine that QA tested and approved each bug fix sampled prior to implementation.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.09	Minor releases are documented in a PMR, regression testing is performed, and approval from QA is obtained prior to implementation to production.	Inspected the PMRs for a sample of minor releases implemented during the period to determine that each minor release sampled was documented in a PMR, tested, and approved by QA prior to implementation.	No exceptions noted.
1.10	After the release team implements a minor release to production, QA verifies that the minor release is implemented and operating successfully.	Inspected the PMRs for a sample of minor releases implemented during the period to determine that QA performed a post-implementation review for each minor release sampled.	No exceptions noted.
	Hot Pushes (Emergency Bug Fixes)		
1.11	After an emergency bug is fixed, QA tests and approves the hot push prior to implementation to production by the release team.	Inspected the issue records for a sample of hot pushes implemented during the period to determine that QA performed testing and approved for each hot push sampled prior to implementation.	No exceptions noted.
	Infrastructure Changes		
1.12	The release cell meets on a daily basis to review, prioritize, and authorize upcoming infrastructure changes.	Inspected the release cell meeting minutes for a sample of dates during the period to determine that release cell meetings were held for each date sampled to review, prioritize, and authorize upcoming infrastructure changes.	No exceptions noted.
1.13	Infrastructure changes are documented in a PMR. Changes are approved by the release cell, unless pre-authorized or automated.	Inspected the PMRs for a sample of infrastructure changes implemented during the period to determine that each infrastructure change sampled was documented in a PMR, approved by the release cell, unless pre-authorized or automated.	No exceptions noted.
1.14	Infrastructure changes are tested prior to implementation to production and verified post deployment, as applicable.	Inspected the PMRs for a sample of infrastructure changes implemented during the period to determine that infrastructure changes were tested prior to implementation to production and verified post deployment, as applicable, for each infrastructure change sampled.	No exceptions noted.
	Segregated Environments and Access Restrictions		
1.15	NetSuite has logically separate environments for its application development, testing, and production activities.	Inspected the development, testing, and production environment network segmentation configurations to determine that the production environment was logically segmented from the development and testing environments.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.16	Direct access to the NetSuite production environment is restricted to user accounts accessible by authorized personnel through a role-based permissions model. The development team does not have write or update access to the production environment.	Inspected the production environment user account listings, including user accounts with the ability to implement code to production, and compared them to the developer user account listings with the assistance of the IT director to determine that direct access to the production environment was restricted to user accounts accessible by authorized personnel through role-based permissions and that developers did not have write or update access to the production environment.	No exceptions noted.
1.17	The ability to implement core features, minor releases, and hot pushes to production is restricted to user accounts accessible by authorized release team personnel.	Inspected the user account listings for a sample of production servers with the assistance of the IT manager to determine that the ability to implement core features, minor releases, and hot pushes to production was restricted to user accounts accessible by authorized release team personnel for each server sampled.	No exceptions noted.
1.18	The ability to implement bundles or SuiteApps to production is restricted to user accounts accessible by authorized release team personnel.	Inspected the release team user account listing with the assistance of the software development senior manager to determine that the ability to implement bundles or SuiteApps to production was restricted to user accounts accessible by authorized release team personnel.	No exceptions noted.
CUEC.01	User entities are expected to implement controls that ensure prompt communication of identified bugs or system functionality issues to NetSuite.		
CUEC.02	User entities are expected to implement controls that ensure user acceptance tests are conducted and that validation of such testing activities are complete, including validation of the accuracy and functionality of upgrades that have an impact to the user entity's NetSuite environment.		
CUEC.03	User entities are expected to implement controls that ensure changes to internal systems that interact with NetSuite systems are authorized, tested, approved, and implemented according to their change management procedures.		
CUEC.04	User entities are expected to implement controls that ensure the accuracy and appropriateness of the customizations which they apply to their NetSuite environment, including customized reports, are validated.		

LOGICAL SECURITY

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that logical access to data, applications, system data, and networks is restricted to properly authorized individuals, and that security violations are identified, followed up and resolved on a timely basis.			
2.01	NetSuite has established an overall information security standard, which is communicated to employees via the company intranet site and reviewed for updates, as necessary.	Inspected the information security standard and the most recent revision history to determine that an established information security standard was in place and updated as needed during the period.	No exceptions noted.
		Inspected the information security standard on the company intranet site to determine that an established information security standard was in place and communicated to employees via the company intranet site.	No exceptions noted.
	Corporate Environment		
2.02	New employees with access to the corporate network are required to acknowledge the corporate security policies.	Inspected the corporate security policy acknowledgment for a sample of employees hired during the period to determine that the corporate security policies were acknowledged for each employee sampled.	No exceptions noted.
2.03	Temporary worker providers must sign a confidentiality agreement before access to the corporate network can be granted to their provided resources.	Inspected the confidentiality agreement acknowledgment for a sample of temporary worker providers with access to the corporate network to determine that each temporary worker provider sampled signed a confidentiality agreement before access to the corporate network was be granted to their provided resources.	No exceptions noted.
2.04	A new hire is automatically provisioned with a NetSuite identity account after HR initiates employee onboarding in the HR system.	Inspected the automated provisioning configuration and an example job log during the period to determine that new hires were automatically provisioned with a NetSuite identity account after HR initiated employee onboarding in the HR system.	No exceptions noted.
2.05	Access to the NetSuite production environment supporting customer application data is automatically disabled upon termination of employment.	Inspected the automated account disablement configuration and an example log during the period to determine that access to the NetSuite production environment supporting customer application data was disabled upon termination of employment.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.06	Users are authenticated via corporate SSO and multi-factor authentication before being granted access to the NetSuite production environment.	Inspected the login screen and authentication configurations to determine that users were authenticated via corporate SSO and multi-factor authentication before being granted access to the NetSuite production environment.	No exceptions noted.
2.07	The Business and Technology Services department performs monitoring of users on the NetSuite production environment to identify unauthorized or terminated users. All access groups and permissions are automatically disabled via a scheduled batch job.	Inspected the batch job configurations and an example log during the period to determine that the Business and Technology Services department performed monitoring of users on the NetSuite production environment to identify unauthorized or terminated users and all access groups and permissions were automatically disabled via a scheduled batch job.	No exceptions noted.
	Production Environment		
2.08	The department manager authorizes and submits access requests to the security department prior to granting access to the servers and databases supporting customer application data.	Inspected the access requests for a sample of users granted access to the production database servers and databases supporting customer application data during the period to determine that the department manager authorized and submitted access requests to security department prior to granting access to the servers and databases supporting customer application data for each user sampled.	No exceptions noted.
2.09	Access to the servers and databases supporting customer application data is disabled by operations upon termination of employment.	Inspected the user account listings for a sample of production database servers and databases and employees terminated during the period to determine that access to the servers and databases supporting customer application data was disabled upon termination for each database server and database and employee sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.10	Users are authenticated via a user account and password before being granted access to the database and its supporting operating system. The operating system is configured to enforce the following password requirements: • Minimum password length • Minimum password history • Password expiration intervals • Password complexity • Invalid password account lockout threshold	Inspected the user account listings and authentication configurations for a sample of production database servers and databases to determine that users were authenticated via a user account and password before being granted access to the database and its supporting operating system for each database server and database sampled and that the operating system was configured to enforce the following password requirements: • Minimum password length • Minimum password history • Password expiration intervals • Password complexity • Invalid password account lockout threshold	No exceptions noted.
2.11	Administrative access privileges within the database server operating system are restricted to user accounts accessible by authorized personnel.	Inspected the administrator user account listings for a sample of production database servers with the assistance of the IT senior manager to determine that administrative access privileges within the operating system for each database server sampled were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
2.12	Administrative access privileges within the database are restricted to user accounts accessible by authorized personnel.	Inspected the administrator user account listings for a sample of production databases with the assistance of the IT director to determine that administrative access privileges within each database sampled were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
2.13	System owners review users with administrative access to databases to identify unauthorized or inappropriate access on a quarterly basis. Any action items as a result of the review are addressed.	Inspected the user access review results for a sample of quarters during the period to determine that for each quarter sampled system owners reviewed users with administrative access to databases and identified unauthorized or inappropriate access and action items as a result of the review were addressed.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.14	Group owners review users on the production database to identify unauthorized or inappropriate access on a quarterly basis. Any action items as a result of the review are addressed.	Inspected the user access review results for a sample of quarters during the period to determine that for each quarter sampled group owners reviewed users on the production database and identified unauthorized or inappropriate access and action items as a result of the review were addressed.	No exceptions noted.
2.15	Individual SSH keys are required for users to authenticate to the database administrative user account.	Inspected the SSH keys to determine that individual SSH keys were required for users to authenticate to the database administrative user account.	No exceptions noted.
2.16	Customer data is stored in the database with an encrypted at rest format. Access to cryptographic keys is restricted to user accounts accessible by authorized personnel.	Inspected the database encryption configurations and listing of user accounts with access to cryptographic keys with the assistance of the senior IT director and senior IT manager to determine that customer data was stored in the database with an encrypted at rest format and that access to cryptographic keys was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
2.17	The BTS performs an access review of users with remote access to identify unauthorized or terminated users on a quarterly basis. Identified discrepancies during the review are investigated and remediated.	Inspected the user access review results for a sample of quarters during the period to determine that the BTS performed an access review of users with remote access to identify unauthorized or terminated users and identified discrepancies during the review were investigated and remediated for each quarter sampled.	No exceptions noted.
2.18	A SIEM tool is utilized to ingest security and access-related events from production systems and configured to alert security personnel of potential security incidents. Verified security incidents are classified according to severity, documented in a ticketing system, and tracked through resolution.	Inspected the SIEM tool configurations, example events generated during the period, and the ticketing documentation for an example incident closed during the period to determine that a SIEM tool was utilized to ingest security and access-related events from production systems and configured to alert security personnel of potential security incidents and that verified security incidents were classified according to severity, documented in a ticketing system, and tracked through resolution.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.19	Direct access to the NetSuite production environment is restricted to user accounts accessible by authorized personnel through a role-based permissions model. The development team does not have write or update access to the production environment.	Inspected the production environment user account listings, including user accounts with the ability to implement code to production, and compared them to the developer user account listings with the assistance of the IT director to determine that direct access to the production environment was restricted to user accounts accessible by authorized personnel through role-based permissions and that developers did not have write or update access to the production environment.	No exceptions noted.
2.20	Users are authenticated via a user account, password, and two-factor authentication before being granted access to the OCI Console. The OCI Console is configured to enforce the following password requirements: • Minimum password length • Password complexity • Invalid password account lockout threshold	Inspected the OCI Console user account listing and authentication configurations to determine that users were authenticated via a user account, password, and two-factor authentication before being granted access to the OCI Console and that the OCI Console was configured to enforce the following password requirements: • Minimum password length • Password complexity • Invalid password account lockout threshold	No exceptions noted.
2.21	Administrative access privileges within the OCI Console are restricted to user accounts accessible by authorized personnel.	Inspected the OCI Console administrator user account listing with the assistance of the IT systems administrator to determine that administrative access privileges within the OCI Console were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
2.22	The Security Cell performs an access review of active users with break glass access to the OCI Console to identify unauthorized or terminated users on a semi-annual basis.	Inspected the most recent user access review results to determine that the Security Cell performed an access review of active users with break glass access to the OCI Console during the period to identify unauthorized or terminated users.	No exceptions noted.
2.23	Group owners perform an access review of active users with privileged non-break glass access to the OCI Console to identify unauthorized or terminated users on a quarterly basis.	Inspected the user access review results for a sample of quarters during the period to determine that group owners performed an access review of active users with privileged non-break glass access to the OCI Console to identify unauthorized or terminated users for each quarter sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Antivirus		
2.24	A central antivirus server is configured to manage antivirus software clients installed on workstations.	Inspected the central antivirus server dashboard and workstation antivirus configurations for a sample of current employees to determine that a central antivirus server was configured to manage antivirus software clients installed on the workstation for each employee sampled.	No exceptions noted.
2.25	The central antivirus server software is configured to monitor for updates to antivirus definitions and to update registered clients on a daily basis.	Inspected the central antivirus server software configurations and example recent update logs generated during the period to determine that the central antivirus server software was configured to monitor for updates to antivirus definitions and to update registered clients on daily basis.	No exceptions noted.
2.26	The central antivirus server software is configured to perform a full scan of registered clients on a weekly basis.	Inspected the central antivirus server software configurations and example recent scan logs generated during the period to determine that the central antivirus software was configured to perform a full scan of registered clients on a weekly basis.	No exceptions noted.
	Antimalware		
2.27	Malware protection controls are implemented on production servers through endpoint detection and response, which can detect, analyze, and respond to malware threats.	Inspected the malware protection configurations for a sample of production servers to determine that malware protection controls were implemented on each production server sampled through endpoint detection and response, which detected, analyzed, and responded to malware threats.	No exceptions noted.
CUEC.05	User entities are expected to implement controls that ensure security policies for interfacing, communicating with NetSuite, and accessing the NetSuite system are established and communicated to their employees and contractors.		
CUEC.06	User entities are expected to implement controls that ensure password configuration settings and authentication requirements are established that meet their company, industry, and regulatory requirements.		
CUEC.07	User entities are expected to implement controls that ensure appropriate security controls within their NetSuite accounts are implemented. This includes, but is not limited to, evaluating, and implementing as deemed appropriate, password policy settings, mobile access policies, segregation of duties, the use of multi-factor authentication for securing sensitive roles and access, including technologies such as one-time password generating devices, IP address restrictions, VPN tunnels, etc.		
CUEC.08	User entities are expected to implement controls that ensure NetSuite is immediately notified of any actual or suspected information security breaches, including compromised user accounts.		

NETWORK SECURITY

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the network architecture security controls, including network security configurations, have been implemented to safeguard IT resources and data and access to network security devices is restricted to authorized personnel.			
3.01	NetSuite maintains a current network device diagram.	Inspected the network device diagram and evidence of the most recent review to determine that network device diagram was reviewed during the period and documented current network configurations.	No exceptions noted.
3.02	Authenticated web communication sessions over public networks (or over the Internet) are encrypted via TLS.	Inspected the website encryption configurations for the NetSuite SaaS system to determine that authenticated web communication sessions were encrypted utilizing TLS.	No exceptions noted.
3.03	A SIEM tool is utilized to ingest security and access-related events from production systems and configured to alert security personnel of potential security incidents. Verified security incidents are classified according to severity, documented in a ticketing system, and tracked through resolution.	Inspected the SIEM tool configurations, example events generated during the period, and the ticketing documentation for an example incident closed during the period to determine that a SIEM tool was utilized to ingest security and access-related events from production systems and configured to alert security personnel of potential security incidents and that verified security incidents were classified according to severity, documented in a ticketing system, and tracked through resolution.	No exceptions noted.
3.04	NetSuite utilizes rule-based permissions, Security-Lists and/or Network Security Groups as virtual firewalls to permit and restrict access to the production network.	Inspected the network diagram and security list configurations to determine that NetSuite utilized rule-based permissions, Security-Lists and/or Network Security Groups as virtual firewalls to permit and restrict access to the production network.	No exceptions noted.
3.05	Traffic to network resources are monitored and filtered based on policies configured in Illumio. Within the tool, there are established rules that limit communications through the rulesets.	Inspected the Illumio policy configurations to determine that traffic to network resources was monitored and filtered based on policies configured in Illumio and that, within the tool, there were established rules that limited communications through the rulesets.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.06	Illumio users are authenticated via a user account and password with the following enforced requirements: • Minimum password length • Minimum password history • Password expiration intervals • Password complexity	Inspected the Illumio user account listing and authentication configurations to determine that Illumio users were authenticated via a user account and password with the following enforced requirements: • Minimum password length • Minimum password history • Password expiration intervals • Password complexity	No exceptions noted.
3.07	The ability to modify Illumio rulesets is restricted to security engineering personnel with the organization owner and global administrative roles.	Inspected the Illumio user account listing with the assistance of the information security director to determine that the ability to modify Illumio rulesets was restricted to security engineering personnel with the organization owner and global administrative roles.	No exceptions noted.
3.08	Changes to network configurations, traffic rulesets, and Security-List and Network Security Group configurations are documented in the ticketing system, tested, and approved by NetSuite security personnel, as necessary, prior to implementation to production.	Inspected the PMRs for a sample of network configurations, traffic ruleset, and security list configuration changes implemented during the period to determine that each network configuration, traffic ruleset, and security list configuration change sampled was documented in the ticketing system, tested, and approved by NetSuite security personnel, as necessary, prior to implementation to production.	No exceptions noted.
3.09	Vulnerability assessments of the perimeter network are performed on at least a weekly basis to identify potential security vulnerabilities. The security department reviews the results of the vulnerability assessments and classifies and prioritizes issues identified for remediation.	Inspected the vulnerability scanner configurations and an example scan completed during the period and evidence of management review and prioritization of identified issues for remediation to determine that vulnerability assessments of the perimeter network were performed on at least a weekly basis to identify potential security vulnerabilities and that the security department reviewed the results of the vulnerability assessments and classified and prioritized issues identified for remediation.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.10	Penetration testing of the perimeter network and application is performed on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation.	Inspected the most recent penetration test results and evidence of management review and prioritization of identified issues for remediation to determine that a penetration test of the perimeter network and application was performed during the period and that the security department reviewed the results of the penetration test and classified and prioritized issues identified for remediation.	No exceptions noted.
3.11	Access to the production environment requires authorized remote access and enforces multi-factor authentication.	Inspected the login screen and authentication configurations to determine that access to the production environment required authorized remote access and enforced multi-factor authentication.	No exceptions noted.
3.12	Access to the application and infrastructure is managed via user groups and entitlements. Access is automatically provisioned after approval in the identity management system.	Inspected the user groups and entitlements to determine that access to the application and infrastructure was managed via user groups and entitlements.	No exceptions noted.
		Inspected the automated provisioning configuration and example log during the period to determine that access was automatically provisioned after approval in the identity management system.	No exceptions noted.
3.13	The ability to modify Security-List and Network Security Group configurations is restricted to user accounts accessible by authorized IT personnel.	Inspected the OCI user account listing with the assistance of the IT system administrator to determine that the ability to modify Security-List and Network Security Group configurations was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CUEC.09	User entities are expected to implement controls that ensure the installation and configuration of antivirus software and network firewalls for systems that interface with the NetSuite system.		

DATA BACKUP AND RESTORATION

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system and application data is backed up on a timely basis and appropriately stored in a secured facility.			
4.01	NetSuite has a backup policy on customer and application data backup and recovery schedules and procedures.	Inspected the backup policy to determine that NetSuite had a backup policy in place on customer and application data backup and recovery schedules and procedures.	No exceptions noted.
4.02	The monitoring system is configured to send alert notifications to operations personnel when backup issues are identified.	Inspected the monitoring system notification configurations and an example alert notification generated during the period to determine that the monitoring system was configured to send alert notifications to operations personnel when backup issues were identified.	No exceptions noted.
4.03	A subset of databases is restored from a secondary facility on a quarterly basis to validate the restore process and integrity of backup media and data.	Inspected the restore report and ticketing documentation for a sample of quarters during the period to determine that a subset of databases was restored from a secondary facility to validate the restore process and integrity of backup media and data for each quarter sampled.	No exceptions noted.
4.04	A subset of databases is restored from the local cloud data center region on a monthly basis to validate the restore process and integrity of backup data.	Inspected the local cloud data center region restoration ticketing documentation for a sample of months during the period to determine that a subset of databases was restored from the local cloud data center region to validate the restore process and integrity of backup data for each month sampled.	No exceptions noted.
	ExaCS Database		
4.05	The automated backup system is configured to encrypt backup data as a component of the backup and replication process. Access to cryptographic keys is restricted to user accounts accessible by authorized personnel.	Inspected the backup encryption configurations and listing of user accounts with access to cryptographic keys with the assistance of the senior IT director and senior IT manager to determine that the automated backup system was configured to encrypt backup data as a component of the backup and replication process and that access to cryptographic keys was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.06	NetSuite performs and monitors the following recurring backups of customer data to local object storage: • Daily incremental backups • Weekly full backups • Monthly full backups	Inspected the customer data backup configurations and example recent backup logs generated during the period for a sample of production databases to determine that NetSuite performed and monitored the following recurring backups of customer data to local object storage for each database sampled: • Daily incremental backups • Weekly full backups • Monthly full backups	The test of control activity in February 2025 involved 25 samples of production databases, with one exception identified in monthly full backups. Further control testing was performed on 15 additional samples of production database with no exceptions noted.
4.07	The monitoring system is configured to send alert notifications to operations personnel when replication issues are identified.	Inspected the monitoring system notification configurations and an example alert notification generated during the period to determine that the monitoring system was configured to send alert notifications to operations personnel when replication issues were identified.	No exceptions noted.
4.08	An automated replication system is configured to asynchronously replicate customer data to an object storage in a separate data center location within the same geographical region.	Inspected the replication system configurations and example recent replication logs generated during the period for a sample of production databases to determine that an automated replication system was configured to asynchronously replicate customer data to an object storage in a separate data center location within the same geographical region for each database sampled.	No exceptions noted.
4.09	NetSuite performs and monitors the following recurring backups of the core NetSuite application to block storage: • Daily incremental • Weekly incremental • Monthly incremental • Annual full	Inspected the core NetSuite application backup configurations and example recent backup logs generated during the period to determine that NetSuite performed and monitored the following recurring backups of the core NetSuite application to block storage: • Daily incremental • Weekly incremental • Monthly incremental • Annual full	No exceptions noted.
	ATP Database		
4.10	Customer data and backup data are stored in the database with encryption at rest format.	Inspected the backup encryption configurations to determine that customer data and backup data were stored in the database with encryption at rest format.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.11	NetSuite performs monitoring of daily backups conducted by the Autonomous Database.	Inspected the backup configurations and example backup logs generated during the period to determine that NetSuite monitors periodic backups performed by the Autonomous Database.	No exceptions noted.

System Availability and Uptime

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system uptime is monitored on a regular basis with corrective action taken where required.			
5.01	Planned downtimes are documented and tracked to resolution through the use of PMRs.	Inspected the PMRs for a sample of planned downtime events during the period to determine that each planned downtime event sampled was documented and tracked to resolution through the use of PMRs.	No exceptions noted.
5.02	Unplanned downtimes are monitored and tracked to resolution through the use of downtime records in a system monitoring tool, which is configured to send automated alerts to notify the operations team of unplanned downtimes.	Inspected the downtime records for a sample of unplanned downtime events during the period to determine that each unplanned downtime event sampled was monitored and tracked to resolution through the use of downtime records.	No exceptions noted.
		Inspected the monitoring tool notification configurations and an example alert generated during the period to determine that the system monitoring tool was configured to send automated alerts to notify the operations team of unplanned downtimes.	No exceptions noted.
5.03	The NetSuite system status website is configured to update the average uptime status for customer databases on a daily basis.	Inspected the website update configurations and an example recent uptime report generated during the period to determine that the NetSuite system status website was configured to update the average uptime status for customer databases on a daily basis.	No exceptions noted.

CUSTOMER AUTHENTICATION REQUIREMENTS

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that customers are restricted to their specific account and data.			
6.01	Each customer has a unique company ID and customer data stored in the database is identified by the unique company ID.	Inspected a report of production customers added during the period and the related tables where customer data was stored for a sample of customers added during the period to determine that each customer sampled had a unique company ID and that customer data stored in the database was identified by the unique company ID.	No exceptions noted.
6.02	Customers' views are restricted to their account and data related to that account.	Inspected the customer database segregation configurations for a sample of customers added during the period to determine that each sampled customers' views were restricted to their account and data related to that account.	No exceptions noted.
6.03	NetSuite employees do not have access to a customer's NetSuite application instance unless the customer has granted access to a NetSuite employee for support or in accordance with a professional services SOW.	Inspected the application instance user account listing and SOWs for a sample of customers added during the period to determine that NetSuite employees did not have access to a customer's NetSuite application instance unless the customer had granted access to a NetSuite employee for support or in accordance with a professional services SOW for each customer sampled.	No exceptions noted.
CUEC.10	User entities are expected to implement controls that ensure NetSuite is provided with an up-to-date and secure e-mail address and that the e-mails must be accepted from NetSuite at the e-mail address specified.		
CUEC.11	User entities are expected to implement controls that ensure accurate and valid data is input into the NetSuite web-based application.		

MONITORING OF DATA CENTER OPERATIONS

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that controls at the cloud hosting provider organization are monitored, and additional NetSuite controls are applied to NetSuite contracted secured spaces.			
7.01	Cloud hosting provider third-party audit reports are reviewed by the NetSuite GBU architect on an annual basis to determine the effectiveness of cloud hosting provider control environments. Results of the reviews are documented and discussed at scrum and/or security compliance meetings.	Inspected evidence of the most recent review of third-party audit reports and the related discussion of the review results for a sample of cloud hosting providers to determine that the NetSuite GBU architect reviewed the audit reports and discussed the results at scrum and/or security compliance meetings during the period for each cloud hosting provider sampled.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY NETSUITE

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.06	NetSuite performs and monitors the following recurring backups of customer data to local object storage: • Daily incremental backups • Weekly full backups • Monthly full backups	Inspected the customer data backup configurations and example recent backup logs generated during the period for a sample of production databases to determine that NetSuite performed and monitored the following recurring backups of customer data to local object storage for each database sampled: • Daily incremental backups • Weekly full backups • Monthly full backups	The test of control activity in February 2025 involved 25 samples of production databases, with one exception identified in monthly full backups. Further control testing was performed on 15 additional samples of production database with no exceptions noted.
Management's Response:	In relation to this issue, NetSuite performed an analysis of the impact of the failed monthly back-ups. It was found that despite the failure, the weekly full backups were successfully completed, which covered the same data as the monthly full backup. Therefore, there is no gap in the data that was backed up. However, to address the issue, the default timeout setting for monthly backups was increased, and the monitoring for monthly backups was enabled. This has resolved the issue.		

BUSINESS CONTINUITY STRATEGY

NetSuite places a high value on providing continuity of service to its clients and applies a best practice planning approach to prepare for a myriad of situations and degrees of severity. NetSuite's service agreement commits to 99.7% uptime, exclusive of planned downtime. NetSuite's disaster recovery plan stands ready to be activated should an event affect any of the operation sites and cause a major, sustained, regional disruption. NetSuite has targeted appreciably low recovery time and recovery point objectives (RTOs / RPOs) for all events NetSuite declares as disasters.

NetSuite aims to align with international business continuity standards and guidelines and follows the Business Continuity Institute (BCI) Good Practice Guidelines (GPG) and the British Standards Institution's (BSI) Business Continuity Management (BCM) lifecycle. Six key areas of business continuity are covered in the lifecycle process. Some of NetSuite's strategies for addressing those areas are described in part below.

Network

NetSuite delivers a highly available network leveraging OCI's global cloud infrastructure. OCI is physically hosted in multiple regions, each region is comprised of one or more availability domains (ADs) and the ADs are connected by a secured, low latency, high-bandwidth network. Each region is interconnected with other regions through a private, redundant, OCI-managed backbone, and traffic between regions and ADs is encrypted. OCI network infrastructure has built-in redundancy ensuring network services are highly available with global traffic shaping to ensure optimal application connectivity and performance. For customer-facing networks, the NetSuite data centers have multiple external links provided via the OCI global cloud infrastructure, each with a capacity of not less than ten (10) Gigabit per second (GBPS). The networks are designed such that multiple connections can simultaneously fail without any impact on user experience. This redundancy provides reliable connectivity with no data transmission bottlenecks to or from the data.

Systems

As a part of NetSuite's disaster recovery program for the production environment and platforms, NetSuite maintains an up-to-date disaster recovery plan and conducts disaster recovery exercises at least twice per year. The purpose of disaster recovery exercises is to validate the ability to simulate the failover process wherein services are transferred from the primary data center to the secondary data center utilizing established operational and disaster recovery procedures and documentation.

Data Center

NetSuite reviews cloud hosting providers' third-party audit reports to monitor the design and operating effectiveness of the data center and cloud hosting providers' relevant controls. OCI Hosting services are designed to follow the Uptime Institute Tier 3 or Tier 4 Standards, and N+2 redundancy for critical equipment operation. NetSuite is delivered using a redundant data center infrastructure using a pair of redundant primary data centers each serving as a backup for the other. The infrastructure utilizes carrier-class components designed to support millions of users. Extensive use of high availability servers and OCI network technologies providing a highly redundant, carrier-neutral network strategy, help to minimize the risk of single points of failure, and provide a highly resilient environment with appreciably high uptime and performance. NetSuite implements numerous tiers of data redundancy. NetSuite maintains regional data centers with production data replicating to a remote disaster recovery data center per region. Should there be a catastrophic failure at either facility NetSuite would initiate its disaster recovery process.

To protect against localized, intra-data center failures, every server maintains internal data redundancy at the storage layer and external redundancy via immediate storage to secondary servers, which themselves maintain internal data redundancy. Production customer data is replicated in near-real-time to remote redundant servers, which again maintains internal data redundancy. From each data center facility, production customer data is automatically backed up.

OTHER SERVICES PROVIDED BY NETSUITE

Professional Services Automation

NetSuite SuiteProjects Pro is a product of NetSuite to help professional services companies manage their employees and projects. Towards that end, NetSuite has developed an object-oriented, web software platform for creating a customizable data management application for professional services organizations.

The goal of PSA is to assist professional service organizations manage core tasks such as project management, time billing, invoicing, contract management, etc. PSA application modules are provided to clients primarily through a SaaS model or through the installation of an integrated Internet appliance on the client's internal network. NetSuite is responsible for the installation of updates to the application code through a remote management process that produces rapid feature enhancements. NetSuite's PSA application may be distributed to clients in different levels of functionality, including NetSuite SuiteProjects Pro PSA Enterprise Cloud Service, NetSuite SuiteProjects Pro PSA Professional Cloud Service, NetSuite SuiteProjects Pro PSA T&E Cloud Service, or NetSuite SuiteProjects Pro PSA Custom Cloud Service:

- NetSuite SuiteProjects Pro PSA Enterprise Cloud Service: NetSuite SuiteProjects Pro PSA Enterprise Cloud Service edition provides the modules necessary to support companies running a global organization, including advanced resources, projects, timesheets, expenses, invoices, advanced financials, workspaces, purchases, and reporting. Also included is access to NetSuite SuiteProjects Pro mobile tools for iPhone, Android, and the desktop application.
- NetSuite SuiteProjects Pro PSA Professional Cloud Service: NetSuite SuiteProjects Pro PSA Professional Cloud Service provides mid-sized organizations PSA solutions, including the modules of the Enterprise Edition, except for advanced resources, advanced financials, purchases, and NetSuite SuiteProjects Pro mobile tools. The modules not automatically included in Professional can be purchased a la carte.
- NetSuite SuiteProjects Pro PSA T&E Cloud Service: NetSuite SuiteProjects Pro PSA T&E Cloud Service edition provides basic time tracking and expense tracking capabilities to clients via the following modules: timesheets, expenses, and reporting.
- NetSuite SuiteProjects Pro PSA Custom Cloud Service: If a client wishes to build a suite of modules different than those above, a custom suite of modules is offered in which each module is sold a la carte.

Transactions are initiated and authorized by the client via the web-based SuiteProjects Pro application. The application will record, process, or correct transactions based on the input from the clients. The client is responsible for the transaction lifecycle and for ensuring that the application is used according to their management's intentions.

Professional Services and Support

Professional Services

NetSuite has developed consulting and implementation services to assist its customers with integrating and importing data from other systems, changing their business processes to take advantage of the enhanced capabilities enabled by the NetSuite integrated suite, implementing those new business processes within their organization, and configuring and customizing the application suite for their business processes and requirements.

NetSuite's consulting and implementation methodology leverages the nature of the suite's cloud delivery model software architecture, the industry-specific expertise of the NetSuite professional services employees and the design of the platform to simplify, streamline, and expedite the implementation process. NetSuite generally employs a joint staffing model for implementation projects whereby the organization involves the customer actively in the implementation process. NetSuite believes this better prepares its customers to support the application throughout their use of the NetSuite service. In addition, because the service is cloud-based, NetSuite professional services employees can remotely configure the application for most customers based on telephonic consultations. NetSuite's network of partners also provides professional services to its customers.

Training

A variety of training services, ranging from complimentary self-paced recorded training to real-time customer classes, to customized end-user training, are offered. Training offerings are designed to facilitate the successful adoption of the suite throughout the customer's organization.

NetSuite Payroll

The Oracle NetSuite Payroll Service (NetSuite Payroll) is a comprehensive full-service payroll solution for businesses with personnel employed in the United States (U.S.). NetSuite Payroll is an add-on module of the NetSuite solution and integrates with NetSuite. The payroll module shares the same customer and transaction data as the core solution, enabling payroll process automation and providing timely updates of payroll's impact to core business figures and metrics. Businesses can configure the payroll solution to pay wages based on timecards, commission statements, expense statements, earnings, deductions, and employer contributions. NetSuite Payroll provides paycheck calculations of earnings, deductions, and taxes based on employer, employee pay, and tax configurations, and records paycheck transactions within the general ledger (if desired by the customer). As part of the full payroll service offering, NetSuite Payroll provides direct deposit services, paychecks and earnings statements printing, payroll tax filings, payroll tax deposits, 1099s, W-2s, and other payroll-related services.