ORACLE NETSUITE

ORACLE AMERICA, INC.

SOC 2 REPORT

FOR

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

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS
RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

OCTOBER 1, 2024, TO SEPTEMBER 30, 2025

Attestation and Compliance Services

schellman
Quality, above all.

This report is intended solely for use by the management of Oracle America, Inc., user entities of Oracle America, Inc.'s services, and other parties who have sufficient knowledge and understanding of Oracle America, Inc.'s services covered by this report (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 Oracle America, Inc.'s ("Oracle" or the "service organization") accompanying description of its Application Hosting Services for the NetSuite Software-as-a-Service (SaaS) system, in Section 3, throughout the period October 1, 2024, to September 30, 2025 (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Oracle's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Oracle uses a subservice organization for cloud hosting and data backup services for the NetSuite application. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Oracle, to achieve Oracle's service commitments and system requirements based on the applicable trust services criteria. The description presents Oracle's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Oracle's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by 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 Oracle management to provide additional information and is not a part of the description. Information in Section 5 has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Oracle's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

Oracle is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Oracle's service commitments and system requirements were achieved. Oracle has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Oracle is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls 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 in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

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 relating to the engagement, including the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA 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 report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects:

- the description presents Oracle's Application Hosting Services for the NetSuite SaaS system that was designed and implemented throughout the period October 1, 2024, to September 30, 2025, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Oracle's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated

effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Oracle's controls throughout that period; and

- the controls stated in the description operated effectively throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Oracle's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Oracle's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Oracle, user entities of Oracle's Application Hosting Services for the NetSuite SaaS system during some or all of the period of October 1, 2024, to September 30, 2025, business partners of Oracle subject to risks arising from interactions with the Application Hosting Services for the NetSuite SaaS system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service organization;
- how the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- internal control and its limitations;
- complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- user entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- the applicable trust services criteria; and
- the risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

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

Schellman & Company, LLC

Columbus, Ohio
November 3, 2025

SECTION 2

NETSUITE SAAS MANAGEMENT'S ASSERTION

NetSuite SaaS Management's Assertion

We have prepared the accompanying description of Oracle's Application Hosting Services for the NetSuite SaaS system provided by the NetSuite global business unit of Oracle America, Inc., in Section 3, throughout the period October 1, 2024, to September 30, 2025 (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Application Hosting Services for the NetSuite SaaS system that may be useful when assessing the risks arising from interactions with Oracle's system, particularly information about system controls that Oracle has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Oracle uses a subservice organization for cloud hosting and data backup services for the NetSuite application. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Oracle, to achieve Oracle's service commitments and system requirements based on the applicable trust services criteria. The description presents Oracle's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Oracle's controls. The description does not disclose the actual controls at the subservice organization.

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

- the description presents Oracle's Application Hosting Services for the NetSuite SaaS system that was designed and implemented throughout the period October 1, 2024, to September 30, 2025, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Oracle's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of Oracle's controls throughout that period; and
- the controls stated in the description operated effectively throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Oracle's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Oracle's controls operated effectively throughout that period.

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.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

NetSuite designs its processes and procedures related to the Application Hosting Services for the NetSuite SaaS system ("SaaS" system) to meet its objectives for its SaaS services. Those objectives are based on the service commitments that NetSuite makes to user entities, the laws and regulations that govern the provision of the SaaS services, and the financial, operational, and compliance requirements that NetSuite has established for the services. The SaaS services of NetSuite are subject to the relevant regulatory and industry information and data security requirements in which NetSuite operates.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the subscription services agreement (SSA), Hosting and Support Delivery Policy (H&SD), terms of service (TOS), data processing agreement (DPA), as well as in the description of the service offering provided via the public-facing website. The principal security, availability, and confidentiality commitments are standardized and include the following:

- Maintain administrative, physical, and technical safeguards designed for the protection, confidentiality, and integrity of customer data.
- Maintain security policies and procedures that are consistent with applicable industry standards.
- Complete annual third-party security and compliance audits of the environment, including, but not limited to, the following:
    - System and Organization Controls (SOC) / International Standard on Assurance Engagements (ISAE) No. 3402 examinations.
    - Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) examinations.
    - International Organization for Standardization (ISO) 27001:2022 certification reviews.
    - Payment Card Industry Data Security Standard (PCI DSS) assessments.
- Maintain an availability service level commitment (SLC) for customers of 99.7% uptime for each calendar quarter.
- Maintain multiple, geographically separated data centers providing data mirroring, disaster recovery, and failover capabilities.
- Continuously monitor the production environment via network security controls designed to identify malicious traffic.
- Antivirus software to guard against trojans, worms, viruses, and other malware from affecting corporate systems.
- Performance of mandatory background checks, where legally allowed, and segregation of duties.
- Transmission of users' unique login credentials, as well as data in the resultant connection, via encrypted connections.

- Allows for implementation of role-based access permissions for customers.
- NetSuite retains customer data for the duration of contracted services and as needed to fulfill the applicable business purposes and securely disposes of customer data within 10 months upon expiration of the 60-day retrieval period.

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

NetSuite periodically reviews, and updates as deemed appropriate, the policies to address new and evolving security technologies, changes to industry standard practices, and changing security threats, provided that any such updates do not materially reduce the commitments, protections, or overall level of service provided to customers as described within the customer contracts. NetSuite's policies are readily available for employees to review and understand their responsibility for adhering to the associated organizational standards and security requirements.

In accordance with the assertion and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

This report covers the NetSuite Cloud Services system, as defined by, and provided in accordance with the customer's 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, 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.*

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 and Software

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
- OCI (Brazil East (sa-sao paulo)) – Sao Paulo, Brazil
- OCI (Brazil Southeast (sa-vinhedo)) – Vinhedo, Brazil

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.

People

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.

Procedures

System Development and Change Management

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 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

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 (HR) 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.

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

Documented information security policies and procedures are in place that address the following:

- Controls against malware
- Installation of software on operational systems
- Restrictions on software installation

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 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 Business and Technology Services 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

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

NetSuite has implemented data backup policies and configurations that define 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 performs monitoring of daily backups conducted by the Autonomous Database.

System Availability and Uptime

The standard NetSuite SLA specifies 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

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 which house 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.

Data

Customer Data Overview and Maintenance

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.

Customer Data Retention and Disposal

NetSuite's confidential information retention and disposal principal service commitments are documented and communicated in product overview documents made available within the SuiteAnswers portal. Per the commitments, upon termination of the NetSuite service, customer data residing in the production environment is retained in a readable state for 60 days. Customer data is available for retrieval during this period. Upon expiration of the 60-day retrieval period, customer data is securely overwritten or deleted from the production cloud service environments within 10 months.

Additionally, customer data that is due to be disposed of is monitored on a monthly basis. The review is performed to help ensure that data is disposed of in accordance with the disposal principal service commitments.

Physical Asset and Data Disposal

OCI is responsible for the removal of data and software stored on equipment (e.g., physical assets such as servers and drives) and to render such data and software unreadable.

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.

Subservice Organizations

The cloud hosting and data backup services for the NetSuite application services provided by OCI were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at OCI, alone or in combination with controls at NetSuite, and the types of controls expected to be implemented at OCI to achieve NetSuite's principal service commitments and system requirements based on the applicable trust services criteria.

Ref.	Control Activities Expected to be Implemented by OCI	Applicable Trust Services Criteria
CSOC.01	OCI is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the system resides.	CC6.1 – CC6.3, CC6.5 – CC6.6, CC7.2
CSOC.02	OCI is responsible for restricting physical access to data center facilities, backup data, and other system components such as virtual systems and servers.	CC6.4 – CC6.5
CSOC.03	OCI is responsible for the removal of data and software stored on equipment (e.g., physical assets such as servers and drives) and to render such data and software unreadable.	CC6.5
CSOC.04	OCI is responsible for implementing controls to restrict and protect information during transmission, movement, and removal from the underlying storage devices for its cloud hosting services where the system resides.	CC6.7
CSOC.05	OCI is responsible for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the system resides.	CC7.1
CSOC.06	OCI is responsible for monitoring physical access to data center facilities, backup data, and other system components such as virtual systems and servers.	CC7.2
CSOC.07	OCI is responsible for ensuring the data center facilities are equipped with environmental security safeguards.	A1.2

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 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 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 the 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 trust services criteria 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 determining 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 trust services criteria 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 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 address 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 on a quarterly basis 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 must return to normal or near-normal operations and to allow for the prioritization of available equipment and resources, in the event of a disruption.

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.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, and confidentiality categories.

Selection and Development of Control Activities

Control activities are deployed through the use of policies to establish what is expected and procedures that put policies into action. Documented policies and procedures are in place to guide personnel in the following:

- Identifying information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements, including designing and developing general technology control activities.
- Designing, developing, implementing, operating, maintaining, and monitoring of in-scope systems.
- Identifying business objective risks, assessing changes to the system, and developing risk management strategies as part of the risk assessment process.

Policies and procedures are formally documented and reviewed on an annual basis and are communicated to internal personnel via the company intranet. Additionally, sanction procedures are in place that address remedial actions for lack of compliance with security policies and procedures.

Security stakeholders perform a risk assessment on an annual basis that includes an analysis of risk mitigation control activities. The analysis considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold. A statement of applicability aligned with the requirements of ISO 27001 is in place to document the linkage between the risk assessment results and the security controls in place to mitigate identified risks. The statement of applicability is updated on an annual basis in conjunction with the risk assessment process.

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Oracle's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. 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.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the NetSuite SaaS system.

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
    - TOS
    - H&SD
    - 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.
- Vulnerability assessments and penetration tests of the perimeter network are performed to identify potential security vulnerabilities. The security department reviews the results and classifies and prioritizes issues identified for remediation.
- 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.

Subservice Organization Monitoring

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.

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.

System Incident Disclosures

No system incidents occurred during the period that were the result of controls that were not suitably designed or otherwise resulted in a significant failure of the achievement of one or more of the service commitments and systems requirements.

Complementary User Entity Controls

Oracle's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the NetSuite SaaS system provided by Oracle. The scope of the testing was restricted to the NetSuite SaaS system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period October 1, 2024, to September 30, 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 applicable trust services criteria 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 fieldwork. 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 audit 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 to ensure 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.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

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 either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria are presented in the "Subservice Organizations" within Section 3.

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	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.	Inspected the information security standard and evidence of communication to determine that a documented information security standard was in place, communicated via the company intranet, and reviewed during the period.	No exceptions noted.
		Inspected the information security standard to determine that the policies and procedures identified information required to support the functioning of internal control and achievement of objectives.	No exceptions noted.
CC1.1.2	Background checks are performed on new hires prior to the new hire employee's start date.	Inspected the background checks for a sample of employees hired during the period to determine that background checks were completed for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	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.
CC1.1.4	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.
CC1.1.5	Signed nondisclosure agreements are required before sharing information designated as confidential with third-party service providers.	Inspected the signed nondisclosure agreements for a sample of third-party service providers to determine that signed nondisclosure agreements were in place for each third-party service provider sampled.	No exceptions noted.
CC1.1.6	An employee sanction procedure is in place communicating that an employee may be terminated for noncompliance with a policy and / or procedure.	Inspected the employee sanction procedures documented to determine that an employee sanction procedure was in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	No exceptions noted.
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	Security organization policies are formally documented that describe the OSOC responsibilities and oversight of management's system of internal control.	Inspected the security organization policies to determine that security organization policies were formally documented that described the OSOC responsibilities and oversight of management's system of internal control.	No exceptions noted.
CC1.2.2	The OSOC has members who are independent from NetSuite and are objective in evaluations and decision making.	Inspected the members of the OSOC to determine that the OSOC had members who were independent from NetSuite and objective in evaluations and decision making.	No exceptions noted.
CC1.2.3	OSOC meetings are held on an annual basis to review internal control performance.	Inspected the most recent OSOC meeting minutes to determine that OSOC meetings were held during the period to review internal control performance.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	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.	Inquired of the IT security analyst regarding organizational structure to determine that organizational charts were in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system and that the organizational charts were communicated to employees and updated as needed.	No exceptions noted.
		Inspected the organization charts on the company intranet to determine that organizational charts were in place and communicated to employees via the company intranet.	No exceptions noted.
CC1.3.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place for each employment position sampled to define the skills, responsibilities, and knowledge levels required for particular jobs.	No exceptions noted.
CC1.3.3	An executive management team that is comprised of security personnel and executive staff has been established to guide the company in managing security risks.	Inspected the information security standard to determine that an executive management team that was comprised of security personnel and executive staff had been established to guide the company in managing security risks.	No exceptions noted.
CC1.3.4	OSOC meetings are held on an annual basis to review internal control performance.	Inspected the most recent OSOC meeting minutes to determine that OSOC meetings were held during the period to review internal control performance.	No exceptions noted.
CC1.3.5	Management has assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the security architect.	Inspected the information security standard to determine that management had assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the security architect.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place for each employment position sampled to define the skills, responsibilities, and knowledge levels required for particular jobs.	No exceptions noted.
CC1.4.2	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.	Inspected the information security standard and evidence of communication to determine that a documented information security standard was in place, communicated via the company intranet, and reviewed during the period.	No exceptions noted.
		Inspected the information security standard to determine that the policies and procedures identified information required to support the functioning of internal control and achievement of objectives.	No exceptions noted.
CC1.4.3	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.
CC1.4.4	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.	Inspected the security awareness training documentation and the security awareness training completion documentation for a sample of current employees to determine that each employee sampled completed security awareness training during the period.	No exceptions noted.
CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Management formally documents an 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.	Inspected the ISMS policies to determine that management formally documented an organizational strategy within ISMS policies and updated them during the period to align internal control responsibilities, performance measures, and incentives with company business objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.2	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.	Inspected the most recent internal audit documentation and evidence of management review to determine that internal audits were performed during the period in accordance with ISO 27001 requirements and that the audit results were documented and reviewed by management, including corrective action plans for identified control deficiencies.	No exceptions noted.
CC1.5.3	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place for each employment position sampled to define the skills, responsibilities, and knowledge levels required for particular jobs.	No exceptions noted.
CC1.5.4	OSOC meetings are held on an annual basis to review internal control performance.	Inspected the most recent OSOC meeting minutes to determine that OSOC meetings were held during the period to review internal control performance.	No exceptions noted.
CC1.5.5	An employee sanction procedure is in place communicating that an employee may be terminated for noncompliance with a policy and / or procedure.	Inspected the employee sanction procedures documented to determine that an employee sanction procedure was in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	No exceptions noted.
CC1.5.6	Management has assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the security architect.	Inspected the information security standard to determine that management had assigned the responsibility of the maintenance and enforcement of the entity security policies and procedures to the security architect.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.7	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 • Risk assessment results and risk treatment plan status	Inspected the most recent ISMS management review documentation to determine that management review meetings were held during the period to ensure the continuing suitability, adequacy, and effectiveness of the ISMS and included a consideration of topics that included the following: • Changes in external and internal issues that were relevant to the ISMS • Nonconformities and corrective actions • Monitoring and measurement results • Audit results • Fulfilment of information security objectives • Risk assessment results and risk treatment plan status	No exceptions noted.
Communication and Information			
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	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.	Inspected the information security standard and evidence of communication to determine that a documented information security standard was in place, communicated via the company intranet, and reviewed during the period.	No exceptions noted.
		Inspected the information security standard to determine that the policies and procedures identified information required to support the functioning of internal control and achievement of objectives.	No exceptions noted.
CC2.1.2	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.3	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.
CC2.1.4	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.
CC2.1.5	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.
CC2.1.6	The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management on at least an annual basis.	Inspected the most recent risk IT planning process documentation to determine that the entity's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2 – COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	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: • On what to communicate • When to communicate • With whom to communicate • Who shall communicate • The processes by which communication shall be affected	Inspected the ISMS policies and procedures to determine that documented ISMS policies and procedures were in place to guide personnel in the internal and external communications relevant to the ISMS that included the following: • On what to communicate • When to communicate • With whom to communicate • Who shall communicate • The processes by which communication shall be affected	No exceptions noted.
CC2.2.2	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.	Inspected the information security standard and evidence of communication to determine that a documented information security standard was in place, communicated via the company intranet, and reviewed during the period.	No exceptions noted.
		Inspected the information security standard to determine that the policies and procedures identified information required to support the functioning of internal control and achievement of objectives.	No exceptions noted.
CC2.2.3	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.
CC2.2.4	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.5	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.	Inspected the security awareness training documentation and the security awareness training completion documentation for a sample of current employees to determine that each employee sampled completed security awareness training during the period.	No exceptions noted.
CC2.2.6	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place for each employment position sampled to define the skills, responsibilities, and knowledge levels required for particular jobs.	No exceptions noted.
CC2.2.7	NetSuite's information security standard and incident response plan address the following to guide personnel throughout the security incident response process: • Responsibilities and procedures • Reporting information security events • Reporting information security weaknesses • Assessment of and decision on information security events • Response to information security incidents • Learning from information security incidents • Collection of evidence	Inspected the information security standard and incident response plan to determine that NetSuite's information security standard and incident response plan addressed the following to guide personnel throughout the security incident response process: • Responsibilities and procedures • Reporting information security events • Reporting information security weaknesses • Assessment of and decision on information security events • Response to information security incidents • Learning from information security incidents • Collection of evidence	No exceptions noted.
CC2.2.8	Formal problem management procedures have been established to address customer and internal incidents and problems reported.	Inspected the incident response plan to determine that formal problem management procedures had been established to address customer and internal incidents and problems reported.	No exceptions noted.
CC2.2.9	Internally reported security incidents are tracked and resolved.	Inspected the ticketing documentation for a sample of internally reported security incidents closed during the period to determine that internally reported security incidents were tracked and resolved for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.10	An ethics and compliance helpline and dedicated e-mail address and website are accessible by internal users to report incidents, concerns, and complaints.	Inspected the dedicated security website to determine that a helpline was accessible by internal users to report incidents, concerns, and complaints.	No exceptions noted.
CC2.2.11	OSOC meetings are held on an annual basis to review internal control performance.	Inspected the most recent OSOC meeting minutes to determine that OSOC meetings were held during the period to review internal control performance.	No exceptions noted.
CC2.2.12	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 • Risk assessment results and risk treatment plan status	Inspected the most recent ISMS management review documentation to determine that management review meetings were held during the period to ensure the continuing suitability, adequacy, and effectiveness of the ISMS and included a consideration of topics that included the following: • Changes in external and internal issues that were relevant to the ISMS • Nonconformities and corrective actions • Monitoring and measurement results • Audit results • Fulfilment of information security objectives • Risk assessment results and risk treatment plan status	No exceptions noted.
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	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: • On what to communicate • When to communicate • With whom to communicate • Who shall communicate • The processes by which communication shall be affected	Inspected the ISMS policies and procedures to determine that documented ISMS policies and procedures were in place to guide personnel in the internal and external communications relevant to the ISMS that included the following: • On what to communicate • When to communicate • With whom to communicate • Who shall communicate • The processes by which communication shall be affected	No exceptions noted.
CC2.3.2	A description of the SaaS system is provided to customers and users of the system in the help section of the NetSuite system.	Inspected the help section of the NetSuite system to determine that a description of the SaaS system was provided to customers and users of the system in the help section of the NetSuite system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.3	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 • TOS • SLC • DPA • Product overview documents on the customer-facing website	Inspected the product overview documents on the customer-facing website and customer contract templates to determine that the entity's security, availability, and confidentiality commitments and required obligations to its customers and other external users were documented and communicated via the following methods: • SSA • TOS • SLC • DPA • Product overview documents on the customer-facing website	No exceptions noted.
CC2.3.4	Signed nondisclosure agreements are required before sharing information designated as confidential with third-party service providers.	Inspected the signed nondisclosure agreements for a sample of third-party service providers to determine that signed nondisclosure agreements were in place for each third-party service provider sampled.	No exceptions noted.
CC2.3.5	Incident reporting procedures are communicated to external users via the SuiteAnswers portal.	Inspected the incident reporting procedures and evidence of communication to determine that incident reporting procedures were communicated to external users via the SuiteAnswers portal.	No exceptions noted.
CC2.3.6	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.	Inspected the customer portal to determine that customers were provided with access to a NetSuite support site to contact the NetSuite Support group with questions, requests, or other related issues via phone call or through the SuiteAnswers portal.	No exceptions noted.
		Inspected the ticketing documentation for a sample of externally reported security incidents closed during the period to determine that issues were logged and tracked in a ticket, which included details surrounding the problem description, issue priority, and status for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.7	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.
Risk Assessment			
CC3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Management formally documents an 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.	Inspected the ISMS policies to determine that management formally documented an organizational strategy within ISMS policies and updated them during the period to align internal control responsibilities, performance measures, and incentives with company business objectives.	No exceptions noted.
CC3.1.2	Management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to ensure they align with company's mission and are utilized as part of the annual risk assessment process.	Inspected the most recent risk assessment documentation and evidence of management review to determine that management formally documented and reviewed the company's commitments and the operational, reporting, and compliance objectives to ensure they aligned with the company's mission and were utilized as part of the risk assessment process during the period.	No exceptions noted.
CC3.1.3	Management holds quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the company-wide strategy meeting minutes for a sample of quarters during the period to determine that management held company-wide strategy meetings for each quarter sampled that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives.	No exceptions noted.
CC3.2 – COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.2	A formal risk assessment is performed on an annual basis, which identifies and assesses the criticality of information assets, including threats and vulnerabilities. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment and risk treatment documentation and evidence of management review to determine that a formal risk assessment was performed during the period that identified and assessed the criticality of information assets, including threats and vulnerabilities, and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review.	No exceptions noted.
CC3.2.3	Risk identification includes both internal and external factors and their impact on objectives.	Inspected the most recent risk assessment documentation to determine that risk identification included both internal and external factors and their impact on objectives.	No exceptions noted.
CC3.2.4	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.
CC3.2.5	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 #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.6	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.
CC3.3 – COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	No exceptions noted.
CC3.3.2	A formal risk assessment is performed on an annual basis that considers the potential for fraud. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment and risk treatment documentation and evidence of management review to determine that a formal risk assessment was performed during the period that considered the potential for fraud and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review.	No exceptions noted.
CC3.4 – COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management on at least an annual basis.	Inspected the most recent risk IT planning process documentation to determine that the entity's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management during the period.	No exceptions noted.
CC3.4.2	Management identifies and assesses changes that could significantly impact the system of internal control during the annual risk assessment process.	Inspected most recent risk assessment documentation to determine that management identified and assessed changes that could significantly impact the system of internal control during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.3	The NetSuite GBU architect reviews changes to vendors along with their completed audit reports on at least an annual basis and determines the impact of any changes in relation to the organization's objectives and the impact to internal control.	Inspected evidence of the most recent review of third-party audit reports and the related discussion of the review results for a sample of vendors to determine that the NetSuite GBU architect reviewed changes to each vendor sampled along with their completed audit reports during the period and determined the impact of any changes in relation to the organization's objectives and the impact to internal control.	No exceptions noted.
Monitoring Activities			
CC4.1 – COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	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.
CC4.1.2	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.
CC4.1.3	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.4	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.
CC4.1.5	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.
CC4.1.6	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.
CC4.1.7	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.8	The Business and Technology Services 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 Business and Technology Services performed an access review of users with remote access to identify unauthorized or terminated users on a quarterly bases and identified discrepancies during the review were investigated and remediated.	No exceptions noted.
CC4.1.9	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.	Inspected the most recent internal audit documentation and evidence of management review to determine that internal audits were performed during the period in accordance with ISO 27001 requirements and that the audit results were documented and reviewed by management, including corrective action plans for identified control deficiencies.	No exceptions noted.
CC4.1.10	OSOC meetings are held on an annual basis to review internal control performance.	Inspected the most recent OSOC meeting minutes to determine that OSOC meetings were held during the period to review internal control performance.	No exceptions noted.
CC4.1.11	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 data center and 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 data center and cloud hosting provider sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2 – COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	NetSuite's information security standard and incident response plan address the following to guide personnel throughout the security incident response process: • Responsibilities and procedures • Reporting information security events • Reporting information security weaknesses • Assessment of and decision on information security events • Response to information security incidents • Learning from information security incidents • Collection of evidence	Inspected the information security standard and incident response plan to determine that NetSuite's information security standard and incident response plan addressed the following to guide personnel throughout the security incident response process: • Responsibilities and procedures • Reporting information security events • Reporting information security weaknesses • Assessment of and decision on information security events • Response to information security incidents • Learning from information security incidents • Collection of evidence	No exceptions noted.
CC4.2.2	Formal problem management procedures have been established to address customer and internal incidents and problems reported.	Inspected the incident response plan to determine that formal problem management procedures had been established to address customer and internal incidents and problems reported.	No exceptions noted.
CC4.2.3	Internally reported security incidents are tracked and resolved.	Inspected the ticketing documentation for a sample of internally reported security incidents closed during the period to determine that internally reported security incidents were tracked and resolved for each incident sampled.	No exceptions noted.
CC4.2.4	Incident reporting procedures are communicated to external users via the SuiteAnswers portal.	Inspected the incident reporting procedures and evidence of communication to determine that incident reporting procedures were communicated to external users via the SuiteAnswers portal.	No exceptions noted.
CC4.2.5	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	Inspected the customer portal to determine that customers were provided with access to a NetSuite support site to contact the NetSuite Support group with questions, requests, or other related issues via phone call or through the SuiteAnswers portal.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	the problem description, issue priority, and status.	Inspected the ticketing documentation for a sample of externally reported security incidents closed during the period to determine that issues were logged and tracked in a ticket, which included details surrounding the problem description, issue priority, and status for each incident sampled.	No exceptions noted.
CC4.2.6	Management identifies and assesses changes that could significantly impact the system of internal control during the annual risk assessment process.	Inspected most recent risk assessment documentation to determine that management identified and assessed changes that could significantly impact the system of internal control during the period.	No exceptions noted.
CC4.2.7	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.
CC4.2.8	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 #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.9	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.
CC4.2.10	A nonconformity and corrective action procedure is in place to guide personnel in the following: • Reacting to the nonconformity to take action to control and correct it and deal with the consequences • Evaluating the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere • Implementing any action needed • Reviewing the effectiveness of any correction action taken • Making changes to the ISMS, if necessary • Retaining documented information of corrective actions, including the nature of the nonconformities and any subsequent actions taken as well as the results of any corrective action	Inspected the ISMS policies and procedures to determine that a nonconformity and corrective action procedure was in place to guide personnel in the following: • Reacting to the nonconformity to take action to control and correct it and deal with the consequences • Evaluating the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere • Implementing any action needed • Reviewing the effectiveness of any correction action taken • Making changes to the ISMS, if necessary • Retaining documented information of corrective actions, including the nature of the nonconformities and any subsequent actions taken as well as the results of any corrective action	No exceptions noted.
CC4.2.11	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.	Inspected the most recent internal audit documentation and evidence of management review to determine that internal audits were performed during the period in accordance with ISO 27001 requirements and that the audit results were documented and reviewed by management, including corrective action plans for identified control deficiencies.	No exceptions noted.
CC4.2.12	OSOC meetings are held on an annual basis to review internal control performance.	Inspected the most recent OSOC meeting minutes to determine that OSOC meetings were held during the period to review internal control performance.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.13	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 • Risk assessment results and risk treatment plan status	Inspected the most recent ISMS management review documentation to determine that management review meetings were held during the period to ensure the continuing suitability, adequacy, and effectiveness of the ISMS and included a consideration of topics that included the following: • Changes in external and internal issues that were relevant to the ISMS • Nonconformities and corrective actions • Monitoring and measurement results • Audit results • Fulfilment of information security objectives • Risk assessment results and risk treatment plan status	No exceptions noted.
Control Activities			
CC5.1 – COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC5.1.2	Security stakeholders perform a risk assessment on an annual basis that includes an analysis of risk mitigation control activities. The analysis considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.	Inspected the most recent risk assessment and risk treatment documentation to determine that security stakeholders performed a risk assessment during the period that included an analysis of risk mitigation control activities and that the analysis considered how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affected the selection and development of control activities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.3	Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment and risk treatment documentation to determine that assigned risk owners selected and developed control activities to mitigate the risks identified as part of the risk assessment process during the period and that the control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold.	No exceptions noted.
CC5.1.4	A statement of applicability aligned with the requirements of ISO 27001 is in place to document the linkage between the risk assessment results and the security controls in place to mitigate identified risks. The statement of applicability is updated on an annual basis in conjunction with the risk assessment process.	Inspected the most recent risk assessment and risk treatment documentation and the statement of applicability to determine that a statement of applicability aligned with the requirements of ISO 27001 was in place to document the linkage between the risk assessment results and the security controls in place to mitigate identified risks and that the statement of applicability was updated during the period basis in conjunction with the risk assessment process.	No exceptions noted.
CC5.2 – COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Documented policies and procedures are in place to guide personnel with regard to the design and development of general technology control activities.	Inspected the information security standard to determine that documented policies and procedures were in place to guide personnel with regard to the design and development of general technology control activities.	No exceptions noted.
CC5.2.2	Assigned risk owners select and develop control activities over technology to support the achievement of objectives as an output from the risk assessment performed on an annual basis. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment and risk treatment documentation to determine that assigned risk owners selected and developed control activities over technology to support the achievement of objectives as an output from the risk assessment performed during the period and that the control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.3	A statement of applicability aligned with the requirements of ISO 27001 is in place to document the linkage between the risk assessment results and the security controls in place to mitigate identified risks. The statement of applicability is updated on an annual basis in conjunction with the risk assessment process.	Inspected the most recent risk assessment and risk treatment documentation and the statement of applicability to determine that a statement of applicability aligned with the requirements of ISO 27001 was in place to document the linkage between the risk assessment results and the security controls in place to mitigate identified risks and that the statement of applicability was updated during the period basis in conjunction with the risk assessment process.	No exceptions noted.
CC5.3 – COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	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.	Inspected the information security standard and evidence of communication to determine that a documented information security standard was in place, communicated via the company intranet, and reviewed during the period.	No exceptions noted.
		Inspected the information security standard to determine that the policies and procedures identified information required to support the functioning of internal control and achievement of objectives.	No exceptions noted.
CC5.3.2	Operating policies and procedures are documented, updated on an annual basis, and communicated to relevant stakeholders that define information system baseline requirements and select measures, analytic techniques, and tools to be used in managing system security, availability, and confidentiality.	Inspected the information security standard to determine that operating policies and procedures were documented, updated during the period, and communicated to relevant stakeholders that defined information system baseline requirements and selected measures, analytic techniques, and tools to be used in managing system security, availability, and confidentiality.	No exceptions noted.
CC5.3.3	An employee sanction procedure is in place communicating that an employee may be terminated for noncompliance with a policy and / or procedure.	Inspected the employee sanction procedures documented to determine that an employee sanction procedure was in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Logical and Physical Access Controls			
CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	Architecture hardening standards are established and updated annually.	Inspected the information security standard to determine that architecture hardening standards were established and updated during the period.	No exceptions noted.
CC6.1.2	Standardized build scripts and configuration management tools are in place for system requirements, installation, and configuration settings of production servers.	Inspected the standardized build procedures, scripts, and configuration management tool configurations for a sample of production servers provisioned during the period to determine that standardized build scripts and configuration management tools were in place for system requirements, installation, and configuration settings of each server sampled.	No exceptions noted.
CC6.1.3	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.
CC6.1.4	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.
CC6.1.5	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.
CC6.1.6	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.7	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.
CC6.1.8	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.
CC6.1.9	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.
CC6.1.10	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.11	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.
CC6.1.12	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.
CC6.1.13	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.
CC6.1.14	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.
CC6.1.15	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.16	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.
CC6.1.17	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.
CC6.1.18	The Business and Technology Services 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 Business and Technology Services performed an access review of users with remote access to identify unauthorized or terminated users on a quarterly bases and identified discrepancies during the review were investigated and remediated.	No exceptions noted.
CC6.1.19	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 #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.20	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.
CC6.1.21	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.
CC6.1.22	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.
CC6.1.23	NetSuite employees with access to a customer's NetSuite application instance do not have access to implement changes to production.	Inspected the customer NetSuite application instance user account listings and compared it to the listing of user accounts with the ability to implement changes to production to determine that NetSuite employees with access to a customer's NetSuite application instance did not have access to implement changes to production.	No exceptions noted.
CC6.1.24	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.25	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.
CC6.1.26	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.
CC6.1.27	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.
CC6.1.28	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.
CC6.1.29	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 group configurations was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CSOC.01	OCI is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the system resides.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	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.
CC6.2.2	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.
CC6.2.3	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.
CC6.2.4	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.
CC6.2.5	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 #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.6	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.
CC6.2.7	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.
CC6.2.8	The Business and Technology Services 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 Business and Technology Services performed an access review of users with remote access to identify unauthorized or terminated users on a quarterly bases and identified discrepancies during the review were investigated and remediated.	No exceptions noted.
CSOC.01	OCI is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the system resides.		
CC6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	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.
CC6.3.2	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 #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.3	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.
CC6.3.4	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.
CC6.3.5	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.
CC6.3.6	The Business and Technology Services 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 Business and Technology Services performed an access review of users with remote access to identify unauthorized or terminated users on a quarterly bases and identified discrepancies during the review were investigated and remediated.	No exceptions noted.
CC6.3.7	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.8	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.
CC6.3.9	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.
CC6.3.10	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.
CC6.3.11	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.
CC6.3.12	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.
CSOC.01	OCI is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the system resides.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	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 data center and 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 data center and cloud hosting provider sampled.	No exceptions noted.
CSOC.02	OCI is responsible for restricting physical access to data center facilities, backup data, and other system components such as virtual systems and servers.		
CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CSOC.01	OCI is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the system resides.		
CSOC.02	OCI is responsible for restricting physical access to data center facilities, backup data, and other system components such as virtual systems and servers.		
CSOC.03	OCI is responsible for the removal of data and software stored on equipment (e.g., physical assets such as servers and drives) and to render such data and software unreadable.		
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	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.
CC6.6.2	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.
CC6.6.3	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 #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.4	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.
CC6.6.5	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.
CC6.6.6	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.
CC6.6.7	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.
CC6.6.8	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.9	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.
CC6.6.10	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.
CC6.6.11	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.
CC6.6.12	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 group configurations was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CSOC.01	OCI is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the system resides.		
CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Documented policies and procedures are in place to guide personnel on the procedures for the transmission, movement, and removal of customer data.	Inspected the information security standard to determine that documented policies and procedures were in place to guide personnel on the procedures for the transmission, movement, and removal of customer data.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.2	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.
CC6.7.3	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.
CC6.7.4	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.
CC6.7.5	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.
CC6.7.6	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 group configurations was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
CC6.7.7	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.
CSOC.04	OCI is responsible for implementing controls to restrict and protect information during transmission, movement, and removal from the underlying storage devices for its cloud hosting services where the system resides.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	A documented information security standard is in place that addresses the following: • Controls against malware • Installation of software on operational systems • Restrictions on software installation	Inspected the information security standard to determine that a documented information security standard was in place that addressed the following: • Controls against malware • Installation of software on operational systems • Restrictions on software installation	No exceptions noted.
CC6.8.2	Standardized build scripts and configuration management tools are in place for system requirements, installation, and configuration settings of production servers.	Inspected the standardized build procedures, scripts, and configuration management tool configurations for a sample of production servers provisioned during the period to determine that standardized build scripts and configuration management tools were in place for system requirements, installation, and configuration settings of each server sampled.	No exceptions noted.
CC6.8.3	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.
CC6.8.4	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.
CC6.8.5	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.8.6	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.
System Operations			
CC7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Architecture hardening standards are established and updated annually.	Inspected the information security standard to determine that architecture hardening standards were established and updated during the period.	No exceptions noted.
CC7.1.2	Standardized build scripts and configuration management tools are in place for system requirements, installation, and configuration settings of production servers.	Inspected the standardized build procedures, scripts, and configuration management tool configurations for a sample of production servers provisioned during the period to determine that standardized build scripts and configuration management tools were in place for system requirements, installation, and configuration settings of each server sampled.	No exceptions noted.
CC7.1.3	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.4	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.
CC7.1.5	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.
CC7.1.6	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.
CC7.1.7	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.
CC7.1.8	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.9	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.
CC7.1.10	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.
CSOC.05	OCI is responsible for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the system resides.		
CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.2	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.
CC7.2.3	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.
CC7.2.4	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.
CC7.2.5	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.
CC7.2.6	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.7	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.
CC7.2.8	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.
CC7.2.9	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.
CSOC.01	OCI is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the system resides.		
CSOC.06	OCI is responsible for monitoring physical access to data center facilities, backup data, and other system components such as virtual systems and servers.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	NetSuite's information security standard and incident response plan address the following to guide personnel throughout the security incident response process: • Responsibilities and procedures • Reporting information security events • Reporting information security weaknesses • Assessment of and decision on information security events • Response to information security incidents • Learning from information security incidents • Collection of evidence	Inspected the information security standard and incident response plan to determine that NetSuite's information security standard and incident response plan addressed the following to guide personnel throughout the security incident response process: • Responsibilities and procedures • Reporting information security events • Reporting information security weaknesses • Assessment of and decision on information security events • Response to information security incidents • Learning from information security incidents • Collection of evidence	No exceptions noted.
CC7.3.2	Formal problem management procedures have been established to address customer and internal incidents and problems reported.	Inspected the incident response plan to determine that formal problem management procedures had been established to address customer and internal incidents and problems reported.	No exceptions noted.
CC7.3.3	Internally reported security incidents are tracked and resolved.	Inspected the ticketing documentation for a sample of internally reported security incidents closed during the period to determine that internally reported security incidents were tracked and resolved for each incident sampled.	No exceptions noted.
CC7.3.4	Incident reporting procedures are communicated to external users via the SuiteAnswers portal.	Inspected the incident reporting procedures and evidence of communication to determine that incident reporting procedures were communicated to external users via the SuiteAnswers portal.	No exceptions noted.
CC7.3.5	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.	Inspected the customer portal to determine that customers were provided with access to a NetSuite support site to contact the NetSuite Support group with questions, requests, or other related issues via phone call or through the SuiteAnswers portal.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the ticketing documentation for a sample of externally reported security incidents closed during the period to determine that issues were logged and tracked in a ticket, which included details surrounding the problem description, issue priority, and status for each incident sampled.	No exceptions noted.
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	NetSuite's information security standard and incident response plan address the following to guide personnel throughout the security incident response process: • Responsibilities and procedures • Reporting information security events • Reporting information security weaknesses • Assessment of and decision on information security events • Response to information security incidents • Learning from information security incidents • Collection of evidence	Inspected the information security standard and incident response plan to determine that NetSuite's information security standard and incident response plan addressed the following to guide personnel throughout the security incident response process: • Responsibilities and procedures • Reporting information security events • Reporting information security weaknesses • Assessment of and decision on information security events • Response to information security incidents • Learning from information security incidents • Collection of evidence	No exceptions noted.
CC7.4.2	Formal problem management procedures have been established to address customer and internal incidents and problems reported.	Inspected the incident response plan to determine that formal problem management procedures had been established to address customer and internal incidents and problems reported.	No exceptions noted.
CC7.4.3	Internally reported security incidents are tracked and resolved.	Inspected the ticketing documentation for a sample of internally reported security incidents closed during the period to determine that internally reported security incidents were tracked and resolved for each incident sampled.	No exceptions noted.
CC7.4.4	Incident reporting procedures are communicated to external users via the SuiteAnswers portal.	Inspected the incident reporting procedures and evidence of communication to determine that incident reporting procedures were communicated to external users via the SuiteAnswers portal.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.5	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.	Inspected the customer portal to determine that customers were provided with access to a NetSuite support site to contact the NetSuite Support group with questions, requests, or other related issues via phone call or through the SuiteAnswers portal.	No exceptions noted.
		Inspected the ticketing documentation for a sample of externally reported security incidents closed during the period to determine that issues were logged and tracked in a ticket, which included details surrounding the problem description, issue priority, and status for each incident sampled.	No exceptions noted.
CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	NetSuite's information security standard and incident response plan address the following to guide personnel throughout the security incident response process: • Responsibilities and procedures • Reporting information security events • Reporting information security weaknesses • Assessment of and decision on information security events • Response to information security incidents • Learning from information security incidents • Collection of evidence	Inspected the information security standard and incident response plan to determine that NetSuite's information security standard and incident response plan addressed the following to guide personnel throughout the security incident response process: • Responsibilities and procedures • Reporting information security events • Reporting information security weaknesses • Assessment of and decision on information security events • Response to information security incidents • Learning from information security incidents • Collection of evidence	No exceptions noted.
CC7.5.2	Formal problem management procedures have been established to address customer and internal incidents and problems reported.	Inspected the incident response plan to determine that formal problem management procedures had been established to address customer and internal incidents and problems reported.	No exceptions noted.
CC7.5.3	Internally reported security incidents are tracked and resolved.	Inspected the ticketing documentation for a sample of internally reported security incidents closed during the period to determine that internally reported security incidents were tracked and resolved for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5.4	Incident reporting procedures are communicated to external users via the SuiteAnswers portal.	Inspected the incident reporting procedures and evidence of communication to determine that incident reporting procedures were communicated to external users via the SuiteAnswers portal.	No exceptions noted.
CC7.5.5	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.	Inspected the customer portal to determine that customers were provided with access to a NetSuite support site to contact the NetSuite Support group with questions, requests, or other related issues via phone call or through the SuiteAnswers portal.	No exceptions noted.
		Inspected the ticketing documentation for a sample of externally reported security incidents closed during the period to determine that issues were logged and tracked in a ticket, which included details surrounding the problem description, issue priority, and status for each incident sampled.	No exceptions noted.
Change Management			
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	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.
CC8.1.2	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 #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.3	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.
CC8.1.4	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.
CC8.1.5	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.
CC8.1.6	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.
CC8.1.7	As part of the scheduled minor releases, 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.
CC8.1.8	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.9	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.
CC8.1.10	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.
CC8.1.11	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.
CC8.1.12	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.
CC8.1.13	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.
CC8.1.14	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 #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.15	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.
CC8.1.16	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.
CC8.1.17	Customer data is not utilized in non-production environments during the normal course of business. If a customer data replica is required for debugging or testing purposes in non-production environments, an open case and explicit permission from the customer are required.	Inspected information security policy and SDLC process to determine that customer data was not utilized in non-production environments during the normal course of business and that an open case and explicit permission from the customer were required if a customer data replica was used for debugging or testing purposes in non-production environments.	No exceptions noted.
		Inspected the customer debugging process document and the customer case authorization process to determine that an open case and explicit permission from the customer were required if a customer data replica was used for debugging or testing purposes in non-production environments.	No exceptions noted.
		Inspected example test data to determine that customer data was not utilized in non-production environments during the normal course of business.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.18	The ability to directly access customer data replica, in an event of an emergency, is restricted to user accounts accessible by authorized personnel.	Inspected the override tool user account listings the assistance of the NetSuite GBU architect to determine that the ability to directly access customer data replica, in an event of an emergency, was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.19	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 device, traffic ruleset, and security list configuration changes implemented during the period to determine that each network device, 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.
CC8.1.20	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.
CC8.1.21	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.
Risk Mitigation			
CC9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented policies and procedures are in place to guide personnel in identifying, selecting, and developing risk management strategies specifically addressing the risks arising from potential business disruptions as a part of the risk assessment process.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying, selecting, and developing risk management strategies specifically addressing the risks arising from potential business disruptions as a part of the risk assessment process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.2	The annual risk assessment includes an evaluation of risk mitigation control activities for risks arising from potential business disruptions.	Inspected the most recent risk assessment and risk treatment documentation to determine that the risk assessment performed during the period included an evaluation of risk mitigation control activities for risks arising from potential business disruptions.	No exceptions noted.
CC9.1.3	A BIA is performed on an annual basis to identify critical process and develop mitigation strategies arising from potential business disruptions.	Inspected the most recent BIA documentation to determine that a BIA was performed during the period to identify critical process and develop mitigation strategies arising from potential business disruptions.	No exceptions noted.
CC9.2 – The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Vendor management policies are in place that address the following: • Specific requirements for a vendor and business partner • Due diligence process prior to accepting new vendors or business partners • Monitoring process to review vendor and business partner compliance on a periodic basis • Termination of contract The policy is reviewed and updated as needed during the annual risk assessment process.	Inspected the vendor management policies to determine that vendor management policies were in place that addressed the following and that the policies were reviewed and updated as needed during the period: • Specific requirements for a vendor and business partner • Due diligence process prior to accepting new vendors or business partners • Monitoring process to review vendor and business partner compliance on a periodic basis • Termination of contract	No exceptions noted.
CC9.2.2	The annual risk assessment process includes the analysis of potential threats and vulnerabilities introduced from doing business with vendors / business partners.	Inspected the most recent risk assessment and risk treatment documentation to determine that the risk assessment process performed during the period included the analysis of potential threats and vulnerabilities introduced from doing business with vendors / business partners.	No exceptions noted.
CC9.2.3	Signed nondisclosure agreements are required before sharing information designated as confidential with third-party service providers.	Inspected the signed nondisclosure agreements for a sample of third-party service providers to determine that signed nondisclosure agreements were in place for each third-party service provider sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.4	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 data center and 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 data center and cloud hosting provider sampled.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.0 - Additional Criteria for Availability			
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	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.
A1.1.2	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1.3	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.
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
A1.2.1	A formal risk assessment is performed on an annual basis, which identifies and assesses the criticality of information assets, including threats and vulnerabilities. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment and risk treatment documentation and evidence of management review to determine that a formal risk assessment was performed during the period that identified and assessed the criticality of information assets, including threats and vulnerabilities, and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review.	No exceptions noted.
A1.2.2	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.
A1.2.3	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.
A1.2.4	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 that defined the customer and application data backup and recovery schedules and procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.5	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.
A1.2.6	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.
A1.2.7	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.
A1.2.8	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.
A1.2.9	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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.10	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.
A1.2.11	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.
A1.2.12	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.
A1.2.13	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.
CSOC.07	OCI is responsible for ensuring the data center facilities are equipped with environmental security safeguards.		
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	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.	No exceptions noted.
A1.3.2	NetSuite has a documented procedure that includes procedures to align the company's disaster recovery and business continuity plans with customer commitments.	Inspected the information security standard and the availability commitments to determine that documented procedures were in place that included procedures to align the company's disaster recovery and business continuity plans with customer commitments.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3.3	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.

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.0 - Additional Criteria for Confidentiality			
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	The entity's customer data retention principal service commitments are documented and communicated in customer agreements.	Inspected the customer portal to determine that the entity's customer data retention principal service commitments were documented and communicated in customer agreements.	No exceptions noted.
C1.1.2	Documented data retention policies and procedures are in place to guide personnel on the procedures for the retention period of customer data.	Inspected the customer data retention policies to determine that documented data retention policies and procedures were in place to guide personnel on the procedures for the retention period of customer data.	No exceptions noted.
C1.1.3	Procedures are in place to help ensure that customer data is retained based upon the predefined retention periods and in accordance with the retention principal service commitments.	Inspected the ticketing documentation and system logs for a sample of customers offboarded during the period to determine that customer data was retained based upon the predefined retention periods and in accordance with the retention principal service commitments for each customer sampled.	No exceptions noted.
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	The entity's customer data disposal principal service commitments are documented and communicated in customer agreements.	Inspected the customer portal to determine that the entity's customer data disposal principal service commitments were documented and communicated in customer agreements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2.2	Documented data disposal policies and procedures are in place to guide personnel on the procedures for the disposal of customer data when the end of the retention period is reached.	Inspected the customer data disposal policies and procedures to determine that documented data disposal policies and procedures were in place to guide personnel on the procedures for the disposal of customer data when the end of the retention period was reached.	No exceptions noted.
C1.2.3	Procedures are in place to dispose of customer data from NetSuite databases upon termination of the services provided to the customer when the end of the retention period has been reached in accordance with the disposal principal service commitments. The results of the disposal of customer data are documented and tracked through resolution within the automated ticketing system or system logs.	Inspected the ticketing documentation and system logs for a sample of customers offboarded during the period to determine that customer data was removed from the NetSuite databases upon termination of the services provided to the customer when the end of the retention period had been reached in accordance with the disposal principal service commitments and that the results of the disposal of confidential information were documented and tracked through resolution within the automated ticketing system or system logs for each customer sampled.	No exceptions noted.
C1.2.4	Customer data that is due to be disposed of is monitored on a monthly basis. The review is performed to help ensure that data is disposed of in accordance with the disposal principal service commitments.	Inspected the evidence of customer data disposal monitoring for a sample of months during the period to determine that customer data that was due to be disposed of was monitored for each month sampled and that the review was performed to ensure that data was disposed of in accordance with the disposal principal service commitments.	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
A1.2.8	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.