ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle NetSuite Cloud Service in Oracle Cloud Infrastructure (OCI)

April 2023 | Version 1.01

PURPOSE STATEMENT

Developed by the Cloud Security Alliance, the Cloud Assessment Initiative Questionnaire (CAIQ) provides a standard template for cloud services provider to accurately describe their security practices. The CAIQ format is largely based on the Cloud Controls Matrix (CCM), which lists a set of fundamental cloud controls. The use of CAIQs allow customers to review the security practices of their cloud services providers to determine the risks associated with the use of these services. Additional information about the CCM and CAIQ can be found on the Cloud Security Alliance site and downloaded at https://cloudsecurityalliance.org/research/artifacts/.

The answers contained in this CAIQ version 3.1 are related to specific Oracle cloud services as listed in the "Oracle cloud Services in Scope" section below.

The Oracle Corporate Security site provides additional information and is referenced in the CAIQ answers throughout this document. This site is available to the public: https://www.oracle.com/corporate/security-practices/.

If you have specific questions about this document, please engage with your Oracle account representative.

DISCLAIMER

This document (including responses related to the specified Oracle services) is provided on an "AS IS" basis without warranty of any kind and is subject to change without notice at Oracle's discretion. You may use this document (including responses related to the specified Oracle services) for informational purposes only to assist in your internal evaluation of the specified Oracle services. This document does not create, nor form part of or modify, any agreement or contractual representation between you and Oracle, or the Oracle authorized reseller, as applicable. In the event you purchase Oracle services, the relevant contract(s) between you and Oracle, or the Oracle authorized reseller, as applicable, will determine the scope of services provided and the related governing terms and conditions. Oracle and its licensors retain all ownership and intellectual property rights in and to this document and its contents, and you may not remove or modify any markings or any notices included herein of Oracle's or its licensors' proprietary rights.

It remains solely your obligation to determine whether the controls provided by the Oracle services meet your requirements. Please also note that any Yes/No responses, and any computed "In Place" indicators, must be read in the context of the supplied comments and qualifications, and, given the diversity and complexity of the services, will not be absolute or applicable in all instances. The explanation and/or supporting documentation comprise Oracle's response and control regardless of the scoring or any Yes/No response. The responses provided in this document apply solely to the services specifically listed and other products or services may have different controls.

ORACLE CLOUD SERVICES IN SCOPE

This document applies to the Oracle NetSuite Cloud Service in Oracle Cloud Infrastructure (OCI) hosted at Oracle data centers or third-party data centers retained by Oracle. Customers can find the data center where their data is stored by logging into their NetSuite account and going to Setup > Company > Company Information.

The scope is applicable to the following Oracle NetSuite services:

ERP/CORE

- Revenue Management
- CRM – SFA
- CRM – Marketing
- CRM – Support
- Adv Revenue Management
- Contract Renewals
- SuiteBilling
- Electronic Bank Payments
- Adv Procurement
- Financial Management – GL
- Financial Management – AP
- Financial Management – AR
- Fixed Assets
- Dunning Letters
- OneWorld
- PBCS (Analytics)
- Basic Projects
- Inventory
- Adv Inventory
- Adv Mfg: Adv Ship Notice
- Adv Mfg: Batch Process

- Adv Mfg: Discrete
- Adv Mfg: Quality Management
- Manufacturing WIP And Routings
- Incentive Compensation
- Demand Planning
- Adv Order Management
- WMS
- Work Orders & Assemblies
- Grid Order Management
- Quality Management
- Sales Orders
- Purchase Orders
- Time Tracking
- Expenses
- Advanced Financials
- Electronic Invoices
- Advanced Software

Platform/Infrastructure

- SuiteAnalytics Connect (ODBC)
- SuiteCloud Plus (SC+)

CRM +

- Premium Customer Center

PSA

- Resource Allocation
- Advanced Projects
- Job Costing

SuiteCommerce

- Site Builder
- Adv Partner Center
- SuiteCommerce Standard
- SuiteCommerce Advanced (SCA)
- SuiteCommerce Instore (SCIS)

TABLE OF CONTENTS

CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ)

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Application & Interface Security: Application Security	AIS-01.1	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle cloud. Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience. To ensure that Oracle products are developed with consistently high security assurance, and to help developers avoid common coding mistakes, Oracle employs formal secure coding standards. For more information, see https://www.oracle.com/corporate/security-practices/assurance/
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	Security testing of Oracle code includes both functional and non-functional activities for verification of product features and quality. Although these types of tests often target overlapping product features, they have orthogonal goals and are carried out by different teams. Functional and non-functional security tests complement each other to provide comprehensive security coverage of Oracle products. Static security analysis of source code is the initial line of defense used during the product development cycle. Oracle uses a commercial static code analyzer, as well a variety of internally developed tools, to catch problems while code is being written. Products developed in programming languages and platforms (J2EE, .NET) are scanned to identify possible security issues. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	Oracle Developers use static and dynamic analysis tools to detect security defects in Oracle code prior to production. Identified issues are evaluated and addressed in order of priority and severity. Oracle management tracks metrics regarding issue identification and resolution. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Oracle Software Security Assurance (OSSA) policies require that third-party components (e.g., open source components used in the Oracle Clouds or distributed in traditional Oracle product distributions) be appropriately assessed for security purposes. Additionally, Oracle has formal policies and procedures which define requirements for managing the safety of its supply chain, including how Oracle

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Corporate Security Architecture manages a variety of programs and leverages multiple methods of engaging with leadership and operational security teams responsible for Oracle operations, services, cloud, and all other lines of business. An example program for managing the security of Oracle's architecture is the Corporate Security Solution Assurance Process (CSSAP). CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle, so that projects are aligned with: • Pre-review: the risk management teams in each line of business must perform a pre-assessment of each project using the approved template • CSSAP review: the security architecture team reviews the submitted plans and performs a technical security design review. • Security assessment review: based on risk level, systems and applications undergo security verification testing before production use Customer remains solely responsible for its regulatory compliance in its use of any Oracle cloud services. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
Application & Interface Security: Customer Access Requirements	AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	For information on the delivery of the cloud service, please refer to Oracle NetSuite Cloud Services Contracts page - https://www.oracle.com/corporate/contracts/cloud-services/netsuite/ Customer remains solely responsible for its regulatory compliance in its use of any Oracle cloud services. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
	AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	Customer remains solely responsible for its regulatory compliance in its use of any Oracle cloud services. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
Application & Interface Security: Data Integrity	AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?	Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. They discuss general security knowledge areas such as design principles, cryptography and communications security, common vulnerabilities, etc. The Standards provide specific guidance on topics such as data input validation, user management, and more. All Oracle developers must be familiar

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			with these standards and apply them when designing and building products. The coding standards have been developed over a number of years and incorporate best practices as well as lessons learned from continued vulnerability testing by Oracle's internal product assessment team. Oracle NetSuite is tested throughout the application's development phases to help ensure these validation techniques are applied. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/
	AIS-03.2	Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Data input and output validation requirements are documented in Oracle's Secure Coding Standards. Oracle NetSuite is tested throughout the application's development phases to help ensure these validation techniques are applied. For more information, see Oracle's Secure Coding Practices: https://www.oracle.com/corporate/security-practices/assurance/development and https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
Application & Interface Security: Data Security / Integrity	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	The Oracle corporate security architect helps set internal information-security technical direction and guides Oracle's IT departments and lines of business towards deploying information security and identity management solutions that advance Oracle's Information Security goals. An example program for managing the security of Oracle's architecture is the Corporate Security Solution Assurance Process (CSSAP). CSSAP is a security review process developed by Corporate Security Architecture, Global Information Security, Global Product Security, Oracle Global IT, and Oracle's IT organizations to provide comprehensive information-security management review. CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle, so that projects are aligned with: • Pre-review: the risk management teams in each line of business must perform a pre-assessment of each project using the approved template • CSSAP review: the security architecture team reviews the submitted plans and performs a technical security design review • Security assessment review: based on risk level, systems and applications undergo security verification testing before production use
Audit Assurance & Compliance:	AAC-01.1	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources, etc.) for reviewing the	Oracle NetSuite maintains an audit plan that includes third-party audits and assessments (e.g., ISO, SOC, PCI DSS). Third-party audit reports provide an opinion on Oracle NetSuite's implemented security controls.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Audit Planning		efficiency and effectiveness of implemented security controls?	For more information, see: https://www.oracle.com/corporate/cloud-compliance/
	AAC-01.2	Does your audit program take into account effectiveness of implementation of security operations?	The effectiveness of implemented security operation controls is within the scope of the audit plan described in previous section.
Audit Assurance & Compliance: Independent Audits	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	Audit reports about Oracle cloud services are periodically published by Oracle's third-party auditors. Reports may not be available for all services or all audit types or at all times. Customer may request access to available audit reports through a self-service portal in the customer's NetSuite Account Center. Customer remains solely responsible for its regulatory compliance in its use of any Oracle cloud services. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	Oracle maintains teams of specialized security professionals for the purpose of assessing the security strength of the company's infrastructure, products, and services. These teams perform various levels of complementary security testing: **Operational security scanning** is performed as part of the normal systems administration of all Oracle's systems and services. This kind of assessment largely leverages tools including commercial scanning tools as well as Oracle's own products (such as Oracle Enterprise Manager). The purpose of operational security scanning is primarily to detect unauthorized and insecure security configurations. **Penetration testing** is also routinely performed to check that systems have been set up in accordance with Oracle's corporate standards and that these systems can withstand their operational threat environment and resist hostile scans that permeate the Internet. Penetration testing can take two forms: **Passive-penetration testing** is performed using commercial scanning tools and manual steps. It is usually performed via the Internet and usually with the minimum of insider knowledge. Passive testing is used to confirm the presence of known types of vulnerabilities with sufficient confidence and accuracy to create a test case that can then be used by development or cloud operations to validate the presence of the reported issue. During passive-penetration testing, no exploitation is performed on production environments, other than that minimally required to confirm the issue. For example, a SQL injection will not be exploited to exfiltrate data. **Active-penetration testing** is more intrusive than passive-penetration testing and allows for the exploitation of discovered vulnerabilities. It is also broader in scope than passive penetration testing as the security teams are typically allowed to pivot from one system to another. Obviously, active penetration testing is closely controlled so as to avoid unintentional impacts on production systems.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Oracle requires that external facing systems and cloud services undergo penetration testing performed by independent security teams. Global Information Security's Penetration Testing Team performs penetration tests and provides oversight to all lines of business in instances where other internal security teams or an approved third-party perform penetration testing activities. This oversight is designed to drive quality, accuracy, and consistency of penetration testing activities and their associated methodology. Oracle has formal penetration testing requirements which include test scope and environment definition, approved tools, findings classification, categories of exploits to attempt via automation and manual steps, and procedures for reporting results. Before a line of business is allowed to bring a new system or cloud service into production, Oracle requires that the remediation of significant penetration test findings be completed. Information about penetration tests of Oracle's corporate systems and cloud services is Oracle Confidential and is not shared externally.
	AAC-02.4	Do you conduct internal audits at least annually?	Oracle Business Assessment & Audit periodically conducts internal and other planned audits on Oracle Global Business Units (GBUs), including Oracle NetSuite. Internal audit results are reported to Oracle's management.
	AAC-02.5	Do you conduct independent audits at least annually?	Audit reports about Oracle cloud Services are periodically published by Oracle's third-party auditors. Reports may not be available for all services or all audit types or at all times. Customer may request access to available audit reports trough a self-service portal in the customer's NetSuite Account Center.
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	Customers may request for the executive summary of Oracle NetSuite's penetration testing results through a self-service portal in their NetSuite Account Center.
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	Audit reports about Oracle cloud services are periodically published by Oracle's third-party auditors. Customer may request access to available audit reports through a self-service portal in the customer's NetSuite Account Center.
Audit Assurance & Compliance: Information System Regulatory Mapping	AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure	Oracle Legal closely monitors the global regulatory landscape to identify legislation applicable to Oracle, including regional and local teams monitoring changes in relevant jurisdictions. Oracle Legal partners with Corporate Security and other organizations to manage Oracle's compliance to regulatory obligations across all lines of business. For more information, see https://www.oracle.com/legal/ In addition, Oracle Global Trade Compliance (GTC) is responsible for import and export oversight, guidance, and enforcement to enable worldwide trade compliant processes across Oracle, in order to uphold and protect Oracle's global trade

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		compliance with relevant regulatory requirements?	privileges and ensure the success of Oracle's business. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-trade-compliance.html Customer remains solely responsible for its regulatory compliance in its use of any Oracle cloud services. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
Business Continuity Management & Operational Resilience: Business Continuity Planning	BCR-01.1	Does your organization have a plan or framework for business continuity management or disaster recovery management?	Oracle's Risk Management Resiliency Policy authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The RMRP's objective is to establish a business resiliency framework to help provide an efficient response to business interruption events affecting Oracle's operations .
	BCR-01.2	Do you have more than one provider for each service you depend on?	Oracle's third-party colocation data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.
	BCR-01.3	Do you provide a disaster recovery capability?	Documented policies are in place governing disaster recovery processes. Oracle NetSuite maintains an up-to-date disaster recovery plan and conducts periodic disaster recovery exercises. These documents are classified as Confidential – Oracle Internal.
	BCR-01.4	Do you monitor service continuity with upstream providers in the event of provider failure?	Oracle Supplier Information and Physical Security Standards requires that suppliers maintain Disaster Recovery and Business Continuity plans which encompass the scope of products and services provided to Oracle. Suppliers are required to test these plans at least annually, and notify Oracle of any potential or realized business interruptions which impact services to Oracle. For more information, see https://www.oracle.com/corporate/suppliers.html
	BCR-01.5	Do you provide access to operational redundancy reports, including the services you rely on?	The Risk Management Resiliency Program (RMRP) objective is to establish a business-resiliency framework to help provide an efficient response to business-interruption events affecting Oracle's operations. The RMRP is implemented and managed locally, regionally, and globally. The RMRP program Is comprised of four Risk Management functions:

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			1. Emergency Response, managed by Facilities Environment, Health and Safety Program 2. Crisis Management, managed by Global Physical Security 3. Business Continuity Management, managed by the corporate RMRP Program Management Office 4. Disaster Recovery, managed by Global Information Technology Oracle's Information Technology organization conducts an annual DR exercise designed to assess our DR plans. Lessons learned from the exercise are implemented as deemed appropriate into standard operations and DR procedures as appropriate. These reports are Oracle Confidential. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
	BCR-01.6	Do you provide a tenant-triggered failover option?	Oracle NetSuite offers automated failover for Oracle NetSuite-triggered failover. Customer-triggered failover must be requested manually through the customer support portal.
	BCR-01.7	Do you share your business continuity and redundancy plans with your tenants?	Oracle's corporate Disaster Recovery (DR) plans focus on the resiliency of computing infrastructure supporting Oracle's internal operations and cloud services. Oracle's production data centers are geographically separated and have component and power redundancy, with backup generators in place for availability of data center resources in case of an impacting event. Oracle's DR plans leverage this separation of data centers in conjunction with other recovery strategies to both protect against disruption and enable recovery of services. This plan is Oracle Confidential. Oracle's Information Technology organization conducts an annual disaster recovery exercise designed to assess our DRP. Lessons learned from the exercise are implemented as deemed appropriate into standard operations and disaster recovery procedures as appropriate.
Business Continuity Management & Operational Resilience: Business Continuity Testing	BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Functional business continuity planning is managed by the Risk Manager within each Line of Business (LoB). The critical LoBs are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. The RMRP program requires that identified LoBs: • Identify relevant business interruption scenarios, considering essential people, resources, facilities and technology

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• Conduct a Business Impact Analysis that specifies a Recovery Time Objective and Recovery Point Objective (if appropriate to the function) and identifies the organization's business continuity contingencies strategy • Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Revise business continuity plans based on changes to operations, business requirements, and risks • Educate personnel about their contingency planning controls and procedures • Conduct an exercise to test the efficacy of the plan, as well as participate in a cross-functional annual exercise assessing the capability of multiple organizations to collaborate effectively in response to events • Implement their business continuity plans as needed • Analyze lessons learned for continual improvement of plans and procedures • Obtain approval from the LoB's executive In addition, all LoBs are required to: • Identify relevant business interruption scenarios, including essential people, resources, facilities and technology • Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information. • Obtain approval from the LoB's executive
Business Continuity Management & Operational Resilience: Power / Telecommunications	BCR-03.1	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	Corporate business continuity policy, standards, and practices are governed by the Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and are generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance. Additionally, Oracle reviews the data center and cloud hosting provider third-party audit reports on an annual basis to determine the effectiveness of the data center and cloud hosting provider control environments as part of its SOC and ISO audit programs. For more information about the centralized RMRP program and the risk management activities within geographies and lines of business, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
	BCR-03.2	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure	Oracle's third-party colocation data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		utility services and mitigate environmental conditions?	stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), and geopolitical considerations among other criteria. Oracle maintains a redundant network infrastructure, including DNS servers to route between primary and secondary sites, network devices, and load balancers. Oracle's third-party colocation data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.
Business Continuity Management & Operational Resilience: Documentation	BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Lines of business are required maintain operational and technical documents and make these available to relevant personnel.
Business Continuity Management & Operational Resilience: Environmental Risks	BCR-05.1	Is physical damage anticipated and are countermeasures included in the design of physical protections?	Oracle's third-party colocation data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), and geopolitical considerations among other criteria.
Business Continuity Management & Operational Resilience: Equipment Location	BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	Oracle's third-party colocation data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Business Continuity Management & Operational Resilience: Equipment Maintenance	BCR-07.1	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	Oracle has implemented a Risk Management Resiliency Program (RMRP) that requires Lines of Business (LoBs) to have a Business Continuity (BC) plan and Disaster Recovery (DR) plan. These documents are classified as Confidential – Oracle Internal. Oracle's third-party colocation data centers are responsible for maintaining the physical datacenter and equipment. The providers' third-party audit reports are reviewed annually by Oracle to determine the effectiveness of the data center provider control environment.
	BCR-07.2	Do you have an equipment and datacenter maintenance routine or plan?	Oracle's third-party colocation data centers are responsible for maintaining the physical datacenter and equipment. The providers' third-party audit reports are reviewed annually by Oracle to determine the effectiveness of the data center provider control environment. Additionally, Oracle Global Physical Security uses a risk-based approach to physical and environmental security. The goal is to balance prevention, detection, protection, and response, while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained.
Business Continuity Management & Operational Resilience: Equipment Power Failures	BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Oracle's third-party colocation data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidates build sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), and geopolitical considerations among other criteria. Oracle's third-party colocation providers are responsible for protecting physical equipment from utility service outages by implementing the appropriate physical environment controls. Third-party audit reports are reviewed annually by Oracle to determine the effectiveness of the data center provider control environment. Oracle selects redundant, independent network providers, each of which is further independently specified for sufficient capacity, for each of its third-party colocation datacenters.
Business Continuity Management & Operational Resilience:	BCR-09.1	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities,	Corporate business continuity policy, standards, and practices are governed by the Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and are generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Impact Analysis		disruption tolerance, RPO and RTO etc) ?	
	BCR-09.2	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	Functional business continuity planning is managed by the Risk Manager within each Line of Business (LoB). The critical LoBs are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes.
Business Continuity Management & Operational Resilience: Policy	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Functional business continuity planning is managed by the Risk Manager within each Line of Business (LoB). The critical LoBs are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes.
Business Continuity Management & Operational Resilience: Retention Policy	BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	Oracle NetSuite's technical features allow customer to enforce customer data retention policies. Customers are responsible for carrying out activities to enforce data retention in accordance with their own internal retention policies or as required by law.
	BCR-11.2	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	Customers are responsible for managing retention of data during their use of Oracle cloud services.
	BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Oracle NetSuite has implemented data backup policies and configurations that define data backup and recovery schedules, and procedures to be followed. For disaster recovery purposes, Oracle NetSuite maintains an up-to-date disaster recovery plan and conducts periodic disaster recovery exercises.
	BCR-11.4	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	Oracle has identified certain critical internal infrastructure systems that are backed up and can be restored. For these systems, Oracle performs the following backups as applicable: • Database: Full and incremental backups. • Archive logs: Full and incremental backups In addition, source code repository backups are performed on recurring basis that vary by environment.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			Oracle also implements additional strategies for certain critical internal systems, such as: • Application failover • Current copy of the production database at a secondary site using solutions such as Oracle Data Guard, which manages the two databases. Oracle Data Guard provides remote archiving, managed recovery, switchover, and failover features • Redundant middle or application server tiers consisting of a set of servers to distribute application functionality across multiple host machines • Physical backup media such as tape is periodically relocated to a secure offsite location
	BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	Oracle NetSuite is a software as a service (SaaS). As such, managing its virtual infrastructure is not available to customers. Oracle NetSuite has appropriate processes and procedures in place to manage virtual machines, including a capability to restore to previous configurations, if needed.
	BCR-11.6	Does your cloud solution include software/provider independent restore and recovery capabilities?	Oracle NetSuite has defined data backup policies and procedures and implemented configurations that support the appropriate data backup and retention schedules. For disaster recovery purposes, Oracle NetSuite maintains an up-to-date disaster recovery plan and conducts recovery exercises at least twice per year. Outside of disaster recovery purposes, restoring customer data from backups on an ad-hoc basis is outside the scope of Oracle NetSuite's services. Customers may submit a request for assistance with these activities, but additional fees may apply.
	BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	Oracle's Information Technology organization conducts an annual DR exercise designed to assess our DR plans. Lessons learned from the exercise are implemented as deemed appropriate into standard operations and DR procedures as appropriate.
Change Control & Configuration Management: New Development / Acquisition	CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	The Oracle corporate security architect helps set internal information-security technical direction and guides Oracle's IT departments and lines of business towards deploying information security and identity management solutions that advance Oracle's Information Security goals. The corporate security architect works with Global Information Security and Global Product Security, and the development Security Leads to develop, communicate, and implement corporate security architecture roadmaps. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Change Control & Configuration Management: Outsourced Development	CCC-02.1	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	Not applicable. Development of Oracle NetSuite is not outsourced to external business partners.
	CCC-02.2	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	Not applicable. Development of Oracle NetSuite is not outsourced to external business partners.
Change Control & Configuration Management: Quality Testing	CCC-03.1	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	NetSuite's process includes quality change control and testing procedures. These procedures are specified to explicitly include system availability, confidentiality, and integrity. These procedures are periodically reviewed and validated by third-party auditors. Customers may request audit reports through a self-service portal in their NetSuite Account Center.
	CCC-03.2	Is documentation describing known issues with certain products/services available?	Oracle NetSuite maintains an internal record of reported issues or defects related to the Oracle NetSuite Service. Any issues impacting customer environments are referenced and communicated to customers in case records. Customers can monitor availability of the Oracle NetSuite Service through an online status dashboard: https://status.netsuite.com
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Triage and remediation of reported bugs and vulnerabilities for all Oracle NetSuite customers is included in Oracle NetSuite's customer support services which provides case, issue, and bug management. Additionally, Oracle NetSuite performs vulnerability scans and penetration tests of its application and operating systems. Any vulnerabilities noted are addressed in accordance with Oracle NetSuite' vulnerability management and patching processes, which are periodically assessed by third-party auditors.
	CCC-03.4	Do you have controls in place to ensure that standards of quality are being met for all software development?	Oracle NetSuite has implemented a robust Quality Assurance (QA) process that is incorporated throughout its Software Development Lifecycle (SDLC). Feature Testing and Regression Testing are performed to validate that relevant security controls and application features are working as intended. Additionally, Oracle NetSuite provides different testing environments to handle varying types of developments (e.g., feature, fixes, etc.). The principle of separation of duties (SOD) is maintained throughout Oracle NetSuite's SDLC. Additionally, NetSuite's SDLC and change management process align with the Oracle Software Security Assurance (OSSA) to ensure that quality standards are being met.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			More information can be found here: https://www.oracle.com/corporate/security-practices/assurance/
	CCC-03.5	Do you have controls in place to detect source code security defects for any outsourced software development activities?	Not applicable. Development of the Oracle NetSuite SaaS application is not outsourced.
	CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	Oracle Secure Operations Standard requires compliance with Oracle Secure Configuration rules, which mandates, among other things that debugging and test code elements be removed from released software. For more information about Oracle Software Security Assurance, see https://www.oracle.com/corporate/security-practices/assurance/
Change Control & Configuration Management: Quality Testing	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Oracle NetSuite uses a configuration management tool that monitors all production systems and detects any unauthorized installation of software in production systems. Corporate level controls are in-place to restrict installation of unauthorized software on endpoint devices.
Change Control & Configuration Management: Production Changes	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	Oracle NetSuite documents its production change management procedures in its software services agreement (SSA) and updates its Service Level Commitment procedures, including customer roles, rights, and responsibilities, publicly at: https://www.oracle.com/corporate/contracts/cloud-services/netsuite/contracts.html#slc
	CCC-05.2	Do you have policies and procedures established for managing risks with respect to change management in production environments?	Oracle has established risk management policies and procedures and change management standards including procedures for evaluating and mitigating identified risks.
	CCC-0.5.3	Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	Oracle NetSuite has technical measures in place within the change management process so that changes in production environments adhere to Service Level Commitments (SLC).
Data Security & Information Lifecycle Management:	DSI-01.1	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from	Oracle NetSuite is a software as a service. Information on machine tagging and configuration are not visible to customers. Internally, however, Oracle NetSuite maintains a monitoring of its system inventories and observes data classification.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Classification		booting/instantiating/transportin g data in the wrong country)?	
	DSI-01.2	Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	Oracle NetSuite is a software as a service. Information on machine tagging and configuration is not visible to customers. These are monitored and maintained internally.
Data Security & Information Lifecycle Management: Data Inventory / Flows	DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	Oracle NetSuite maintains an internal documentation of its data flows within the application and infrastructure network and systems. These are periodically reviewed and validated by our auditors.
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	Oracle NetSuite does not migrate Customer data to another geographical region without Customer consent or unless required for statutory/legal reasons. Oracle has a process in place to ensure that migration of Customer data to another geographical region is reviewed and approved based on Oracle-established criteria and any applicable legal requirements.
Data Security & Information Lifecycle Management: E-commerce Transactions	DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	Oracle NetSuite uses standardized, non-proprietary encryption algorithms for protection of customer data and updates its approved encryption algorithms annually or upon public identification of weaknesses in its selected algorithms. Currently, Oracle NetSuite has standardized on Advanced Encryption Standard (AES) 256 encryption algorithm for customer data moving through public networks. Oracle NetSuite is compliant with Payment Card Industry Data Security Standard (PCI DSS) requirements on encryption of data transmitted across open public networks.
	DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Encryption is the process of rendering data unreadable without the specific key to decrypt the data. Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption when data is at rest (in storage) on laptops, devices, and removable media. Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to only use up-to-date versions of approved security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Data Security & Information Lifecycle Management: Handling / Labeling / Security Policy	DSI-04.1	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?	Oracle's formal Information Protection Policy provides guidelines for all Oracle personnel and business partners regarding information classification schemes and minimum handling requirements associated with those classifications. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
	DSI-04.2	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	Oracle categorizes confidential information into three classes—Internal, Restricted, and Highly Restricted—with each classification requiring corresponding levels of security controls, such as encryption requirements for data classified as Restricted or Highly Restricted.
	DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Oracle has formal requirements for managing data retention. These operational policies define requirements per data type and category, including examples of records in various Oracle departments.
Data Security & Information Lifecycle Management: Nonproduction Data	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Oracle NetSuite has procedures in place to ensure customer production data is not replicated or used in non-production environments. Oracle NetSuite may internally replicate customer production data for the purposes of validating customer issues and remediations after receiving permission from the customer. Such temporary replicas have the same or better security, geographical, and compliance protections as the originals. Customers who purchase account sandbox instances will have replica versions of their data within their sandbox environment for their own use.
Data Security & Information Lifecycle Management: Ownership / Stewardship	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	Oracle has formal requirements for managing data retention. These operational policies define requirements per data type and category, including examples of records in various Oracle departments. Oracle's mandatory training instructs employees about the company's Information Protection Policy. This training also tests employee understanding of information asset classifications and handling requirements. Employees must complete this training when joining Oracle and must periodically repeat it thereafter. Reports enable managers to track course completion for their organizations.
Data Security & Information Lifecycle Management: Secure Disposal	DSI-07.1	Do you support the secure deletion (e.g., degaussing/ cryptographic wiping) of archived and backed-up data?	Oracle's Media Sanitation and Disposal Policy defines requirements for the removal of information from electronic storage media (sanitization), and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. Electronic storage media include laptops, hard drives, storage devices, and removable media such as tape.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Please refer to Oracle NetSuite Cloud Services Contracts page: https://www.oracle.com/corporate/contracts/cloud-services/netsuite/contracts.html
Datacenter Security: Asset Management	DCS-01.1	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	Oracle categorizes confidential information into three classes—Internal, Restricted, and Highly Restricted—with each classification requiring corresponding levels of security controls, such as encryption requirements for data classified as Restricted or Highly Restricted.
	DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. Oracle's Information Systems Asset Inventory Policy requires that Line of Business (LoB) maintain an accurate and comprehensive inventories of information systems, hardware and software. This policy applies to all information assets held on any Oracle system, including both enterprise systems and cloud services. The Oracle Information Systems Asset Inventory Policy requires an accurate inventory of all information systems and devices holding information assets throughout their lifecycle through a Corporate-approved inventory system.
Datacenter Security: Controlled Access Points	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	Oracle's third-party colocation data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), and geopolitical considerations among other criteria. Oracle's third-party colocation data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Datacenter Security: Equipment Identification	DCS-03.1	Do you have a capability to use system geographic location as an authentication factor?	Oracle NetSuite employs a security technology which validates against geographic restrictions in order to help ensure restricted locations cannot access the service and to prevent geographic attack events.
	DCS-03.2	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	Oracle NetSuite deploys automated equipment identification technology for the components of its service. The automated equipment identification technology also includes a location-aware identifier.
Datacenter Security: Offsite Authorization	DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	The relocation or transfer of hardware, software, or data to an offsite premises is not a standard practice and would only be on a case-by-case basis Oracle manages movement of assets in accordance with its Media Handling Standard, which is aligned with the ISO 27001 standard. The policy includes review and approval procedures to ensure that every transfer of asset is valid and authorized. For OCI assets, the Oracle Systems Decommissioning and Repurposing Policy governs the secure physical transfer process for information systems that involves a physical transfer or hardware assets.
Datacenter Security: Offsite Equipment	DCS-05.1	Can you provide tenants with your asset management policies and procedures?	Oracle has formal requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, internet access, and other company resources available to Oracle employees, contractors and visitors. The Oracle Information Systems Asset Inventory Policy requires that Line of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware and software. This policy applies to all information assets held on any Oracle system, including both enterprise systems and cloud services. The Oracle Information Systems Asset Inventory Policy requires an accurate inventory of all information systems and devices holding information assets throughout their lifecycle through a Corporate-approved inventory system. Oracle's Media Sanitation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. Electronic storage media include laptops, hard drives, storage devices, and removable media such as tape.
Datacenter Security: Policy	DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure	Oracle Global Physical Security policies and procedures use a risk-based approach to physical and environmental security. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained. Additionally, The Oracle NetSuite Service is annually audited by a third-party auditor against ISO 27001 requirements.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		working environment in offices, rooms, facilities, and secure areas?	
	DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	Oracle maintains high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business around the world. These apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Oracle requires its employees to receive training in ethics and business conduct every two years.
Datacenter Security: Secure Area Authorization	DCS-07.1	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	Oracle has implemented the following protocols: • Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors. • Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises. • Visitors are required to sign a visitor's register, be escorted and/or observed when they are on Oracle premises, and/or be bound by the terms of a confidentiality agreement with Oracle. • Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving Oracle's employment must return keys/cards and key/cards are deactivated upon termination. • Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations. • Oracle use a mixture of 24/7 onsite security officers or patrol officers, depending on the risk/protection level of the facility. In all cases officers are responsible for patrols, alarm response, and recording of security incidents. Oracle has implemented centrally managed electronic access control systems with integrated intruder alarm capability. The access logs are kept for a minimum of six months. Furthermore, the retention period for CCTV monitoring and recording ranges from 30-90 days minimum, depending on the facility's functions and risk level.
Datacenter Security: Unauthorized Persons Entry	DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	Oracle has implemented the following protocols: • Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors. • Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises. • Visitors are required to sign a visitor's register, be escorted and/or observed when they are on Oracle premises, and/or be bound by the terms of a confidentiality agreement with Oracle.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving Oracle's employment must return keys/cards and key/cards are deactivated upon termination. • Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations. • Oracle use a mixture of 24/7 onsite security officers or patrol officers, depending on the risk/protection level of the facility. In all cases officers are responsible for patrols, alarm response, and recording of security incidents. Oracle has implemented centrally managed electronic access control systems with integrated intruder alarm capability. The access logs are kept for a minimum of six months. Furthermore, the retention period for CCTV monitoring and recording ranges from 30-90 days minimum, depending on the facility's functions and risk level. Where Oracle contracts with a third party datacenter colocation provider, similar controls, including controlled ingress and egress, are implemented.
Datacenter Security: User Access	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	Access control refers to the policies, procedures, and tools that govern access to and use of resources. Examples of resources include a cloud service, physical server, file, application, data in a database, and network device. Least privilege is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties. Default-deny is a network-oriented approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination.
Encryption & Key Management: Entitlement	EKM-01.1	Do you have key management policies binding keys to identifiable owners?	Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption when data is at rest (in storage) on laptops, devices, and removable media. Solutions for managing encryption keys at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). Oracle defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include: • Locations and technologies for storing encryption keys • Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures • Changing default encryption keys

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• Replacement schedule for various types of encryption keys
Encryption & Key Management: Key Generation	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	Oracle NetSuite uses its own encryption keys to encrypt customer data in core functionality and records. For custom-built functionality and records, Oracle NetSuite provides application programing interface (API) to allow customers to use their own keys to encrypt their data. Oracle NetSuite encrypts customer keys using a securely stored key encryption key (KEK).
	EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	Oracle NetSuite uses its own encryption keys to encrypt customer data in core functionality and records. For custom-built functionality and records, Oracle NetSuite provides APIs to allow customers to use their own keys to encrypt their data. Oracle NetSuite encrypts customer keys using a securely stored key encryption key (KEK).
	EKM-02.3	Do you maintain key management procedures?	Oracle maintains Encryption Key Management Standard. Solutions for managing encryption keys at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). Specific requirements in this standard include: • Locations and technologies for storing encryption keys • Replacement schedule for various types of encryption keys
	EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to only use up-to-date versions of approved security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms.
	EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to only use up-to-date versions of approved security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms.
Encryption & Key Management: Encryption	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Oracle NetSuite customer data residing in OCI database tablespaces is encrypted at rest using Transparent Data Encryption technology.
	EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Encryption [Transport Layer Security (TLS) of at least v1.2] is used to transfer data and machine images across the network between components of the Oracle Cloud Infrastructure, except where legacy protocols are offered to customers that do not support encryption (e.g. NFS in File System Storage and iSCSI in Block Volumes), in

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			which case it is the responsibility of the customer to encrypt their data prior to sending it over the cloud network.
	EKM-03.3	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	Oracle has policies, procedures and mechanisms established for key management to support encryption of data in storage and in transmission for the key components of the Oracle NetSuite service. For internal corporate data and transmission encryption, Oracle has established procedures to manage cryptographic keys throughout their lifecycle (e.g., generation, distribution, and revocation).
Encryption & Key Management: Storage and Access	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	Oracle implements a wide variety of technical security controls designed to protect the confidentiality, integrity, and availability of corporate information assets. These controls are guided by industry standards and are deployed across the corporate infrastructure using a risk-based approach. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	Storage of encryption keys for application-level encryption is the customer's responsibility. Master encryption keys are stored either in physical hardware security modules (HSMs) or in a proprietary software management system built by Oracle for exclusive use within Oracle NetSuite.
	EKM-04.3	Do you store encryption keys in the cloud?	Storage of encryption keys for application-level encryption is the customer's responsibility. Master encryption keys are stored either in physical hardware security modules (HSMs) or in a proprietary software management system built by Oracle for exclusive use within Oracle NetSuite.
	EKM-04.4	Do you have separate key management and key usage duties?	For Oracle NetSuite-owned/-managed keys, there is segregation between personnel performing key management duties and key usage duties.
Governance and Risk Management: Baseline Requirements	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	Oracle's enterprise architecture organization defines and maintains guidance documentation and secured configurations for use within Oracle's corporate systems and in Oracle cloud. This guidance applies across layers of Oracle environments, including hardware, storage, operating systems, databases, middleware, and applications.
	GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Oracle NetSuite has 24x7 automated monitoring tool and 24x5 personnel monitoring in place for security infrastructure monitoring, which is being managed against the security baselines. In addition, the security information monitoring process is regularly reviewed for compliance to standards and baselines.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Governance and Risk Management: Risk Assessments	GRM-02.1	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	Oracle's risk assessment methodology and process are aligned with ISO 27001 and 27018 standards. Oracle's security and privacy risk assessment processes account for data residency, legal and statutory requirements for retention periods and data protection and classification and are modeled after information security and privacy frameworks, standards, and regulations, such as ISO 27001 and 27018 and General Data Protection Regulation (GDPR). Customers are responsible for their legal statutory and residency requirements for their data.
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	Oracle NetSuite conducts an annual security and privacy risk assessment that is aligned with ISO 27001 and 27018.
Governance and Risk Management: Management Oversight	GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	Oracle places a strong emphasis on personnel security. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions. Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. Each employee is required to complete the Oracle NetSuite information-protection awareness training and/or the security awareness training upon hiring and every year thereafter.
Governance and Risk Management: Management Program	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	Oracle's corporate security practices are documented at https://www.oracle.com/corporate/security-practices/corporate/ Global Information Security (GIS) defines policies for the management of information security across Oracle. Additionally, GIS sets direction and provides advice to help protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners and employees. GIS also coordinates the reporting of information security risk to senior leadership such as the Oracle Security Oversight Committee and Board of Directors. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle. Corporate governance teams and programs are described at https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html
	GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	The Chief Corporate Architect, who reports directly to the Executive Chairman and Chief Technology Officer (CTO), is one of the directors of the Oracle Security Oversight Committee (OSOC). The Chief Corporate Architect manages the Corporate Security departments which guide security controls at Oracle. Oracle annually reviews

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			its Information Security Management System (ISMS) and audits its management review in accordance with ISO 27001.
Governance and Risk Management: Management Support / Involvement	GRM-05.1	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	Global Information Security manages the Information Security Manager (ISM) Program. Information Security Managers serve as security advocates within their respective lines of business to increase awareness of and compliance with Oracle's security policies, processes, standards, and initiatives. Corporate Security architecture manages a variety of programs and leverages multiple methods of engaging with leadership and operational security teams responsible for Oracle operations, services, cloud, and all other lines of business.
Governance and Risk Management: Policy	GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy.
	GRM-06.2	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	The Chief Corporate Architect, who reports directly to the Executive Chairman and Chief Technology Officer (CTO), is one of the directors of the Oracle Security Oversight Committee (OSOC). The Chief Corporate Architect manages the Corporate Security departments which guide security at Oracle. These departments drive the corporate security programs, define corporate security policies, and provide global oversight for Oracle's security policies and requirements: • Global Information Security • Global Physical Security • Global Product Security • Corporate Security Architecture • Global Trade Compliance
	GRM-06.3	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	Oracle has formal requirements for its suppliers and partners to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when:

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle confidential information, and Oracle hardware assets placed in their custody For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
	GRM-06.4	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	Oracle NetSuite maintains an internal mapping of its controls and processes to SOC 1 / SOC 2, ISO 27001, ISO 27018, and PCI DSS. Oracle NetSuite's controls and processes are periodically validated and reviewed by third-party auditors, and customers may request audit reports through a self-service portal in their NetSuite Account Center.
	GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	Audit reports about Oracle cloud Services are periodically published by Oracle's third-party auditors. Customer may request access to available audit reports through a self-service portal in the customer's NetSuite Account Center.
Governance and Risk Management: Policy Enforcement	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Employees who fail to comply with these policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment.
	GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy.
Governance and Risk Management: Policy Reviews	GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	Oracle's Corporate Information Security Policy Review Process defines how Oracle Global Information Security (GIS) leads ongoing cross-departmental review of information security policies, so that these policies continue to be relevant and aligned with Oracle's technical, legal, governmental and business requirements.
Governance and Risk Management: Policy Reviews	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Customers can subscribe to updates on the Data Processing Agreement for Oracle Services at - https://www.oracle.com/corporate/contracts/cloud-services/contracts.html The Data Security Addendum is available at - https://www.oracle.com/corporate/contracts/cloud-services/netsuite/ The Oracle Privacy Policies are available at - https://www.oracle.com/legal/privacy/

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	Global Information Security (GIS) defines policies for the management of information security across Oracle. policies are reviewed at least annually. Oracle Privacy Policies are maintained by Oracle Privacy and Security Legal. The policies are available at - https://www.oracle.com/legal/privacy/
Governance and Risk Management: Assessments	GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	The Chief Corporate Architect, who reports directly to the Executive Chairman and Chief Technology Officer (CTO), is one of the directors of the Oracle Security Oversight Committee (OSOC). The Chief Corporate Architect manages the Corporate Security departments which guide security at Oracle. These departments drive the corporate security program, define corporate security policies, and provide global oversight for Oracle's security policies and requirements. For more information, see https://www.oracle.com/corporate/security-practices/corporate/objectives.html
	GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	Oracle assesses the likelihood and impact of risks based on a defined assessment scale that is applied to all risk categories. Oracle's security risk assessment and privacy risk assessment processes are aligned with ISO 27001 and ISO 27018, respectively.
Governance and Risk Management: Program	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	Oracle's Corporate Security Programs are designed to protect Oracle and customer information assets, such as: • The mission-critical systems that customers rely upon for Cloud, technical support and other services • Oracle source code and other sensitive data against theft and malicious alteration • Personal and other sensitive information that Oracle collects in the course of its business, including customer, partner, supplier and employee data residing in Oracle's internal IT systems
	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	Corporate governance teams and programs are described at https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html Global Information Security (GIS) defines policies for the management of information security across Oracle. Additionally, GIS sets direction and provides advice to help protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners and employees. GIS also coordinates the reporting of information security risk to senior leadership such as the Oracle Security Oversight Committee and Board of Directors. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Human Resources: Asset Returns	-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
	HRS-01.2	Do you have asset return procedures outlining how assets should be returned within an established period?	Oracle has formal requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, internet access, and other company resources available to Oracle employees, contractors and visitors.
Human Resources: Background Screening	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	In the United States, Oracle uses an external screening agency to perform pre-employment background investigations for newly hired U.S. personnel. Personnel screening in other countries varies according to local laws, employment regulations, and local Oracle policy.
Human Resources: Employment Agreements	HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. For more information, see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
	HRS-03.2	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. . For more information, see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
Human Resources: Employment Termination	HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy. For more information see

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
Human Resources: Portable / Mobile Devices	HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Oracle policy requires the use of antivirus, intrusion protection, and firewall software on endpoint devices such as laptops, desktops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption for their organization. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
Human Resources: Non-Disclosure Agreements	HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.
Human Resources: Roles / Responsibilities	HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	Not applicable. Oracle NetSuite customers can only access the application, not the underlying infrastructure. Refer to the application security page for more information: https://www.netsuite.com/portal/platform/infrastructure/application-security.shtml
Human Resources: Acceptable Use	HRS-08.1	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	Oracle policy requires the use of antivirus intrusion protection and firewall software on endpoint devices such as laptops, desktops, and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			provided to lines of business management to verify deployment of device encryption for their organization. Antivirus software must be scheduled to perform daily threat-definition updates and virus scans. The Oracle Information Technology (OIT) organization keeps anti-virus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. OIT is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. OIT provides automation to verify anti-virus configuration.
	HRS-08.2	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Human Resources: Training / Awareness	HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy.
	HRS-09.2	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy.
	HRS-09.3	Do you document employee acknowledgment of training they have completed?	Oracle keeps a record of employees' completion of mandatory trainings, as well as employee acknowledgment. Records of employees' completion of security awareness trainings are also reviewed during third-party audits and assessments.
	HRS-09.4	Is successful and timed completion of the training program(s) considered a prerequisite for	Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		acquiring and maintaining access to sensitive systems?	subcontractor before that subcontractor provides services. Management is notified of incomplete employee training plans.
	HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	Oracle places a strong emphasis on personnel security. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions. Each employee is required to complete the information-protection awareness training and/or the security awareness training upon hiring and every year thereafter.
	HRS-09.6	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.
Human Resources: User Responsibility	HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.
	HRS-10.2	Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	Oracle places a strong emphasis on personnel security. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.
	HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	Oracle places a strong emphasis on personnel security. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.
Human Resources: Workspace	HRS-11.1	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	Oracle personnel are required to utilize the Oracle's Information Technology (OIT) solutions for Windows Server Update Services (WSUS), virus definitions, security updates and tools which automatically lock the screen.
	HRS-11.2	Are there policies and procedures to ensure that unattended workspaces do not have openly	Oracle policy requires the use of antivirus, intrusion protection, and firewall software on endpoint devices such as laptops, desktops, and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		visible (e.g., on a desktop) sensitive documents?	and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption for their organization.
Identity & Access Management: Audit Tools Access	IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest? • Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?
	IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten.
Identity & Access Management: User Access Policy	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
	IAM-02.2	Do you have policies, procedures and technical measures inHRS place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
	IAM-02.3	Do you have procedures and technical measures in place for user account entitlement de-	Operations are organized into functional groups, where each function is performed by separate groups of employees. Examples of functional groups include developers, database administrators, system administrators, and network engineers.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		/provisioning based on the rule of least privilege?	Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html
	IAM-02.4	Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	Oracle has implemented and maintained strong network controls for the protection and control of both Oracle and customer data during its transmission Oracle's Network Security Policy establishes requirements for network management, network access and network device management, including authentication and authorization requirements for both physical devices and software-based systems.
	IAM-02.5	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest? • Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?
	IAM-02.6	Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	Oracle's Logical Access Policy requires a role-based access model, applying least-privilege principles for granting system access. Privileged access to Oracle NetSuite systems must be justified, approved, and employ multifactor authentication. Oracle NetSuite's security controls are periodically reviewed and validated by third-party auditors. Customers may request audit reports through a self-service portal in their NetSuite Account Center.
	IAM-02.7	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. Metrics are considered Oracle Confidential.
Identity & Access Management: Diagnostic / Configuration Ports Access	IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	Oracle's enterprise architecture organization defines and maintains guidance documentation and secured configurations for use within Oracle's corporate systems and in Oracle cloud. This guidance applies across layers of Oracle environments, including hardware, storage, operating systems, databases, middleware, and applications.
	IAM-04.1	Do you manage and store the identity of all personnel who have	Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Identity & Access Management: Policies and Procedures		access to the IT infrastructure, including their level of access?	programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security-incident management process. Access to security logs is provided on the basis of need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.
	IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. This policy does not apply to customer end user accounts for Oracle cloud services. Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval.
Identity & Access Management: Segregation of Duties	IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest? • Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose? For more information about logical access control, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
Identity & Access Management: Source Code Access Restriction	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	Oracle maintains strong security controls over its source code. Oracle's source-code protection policies provide limits on access to source code (enforcement of the need to know), requirements for independent code review, and periodic auditing of the company's source-code repositories. Oracle's objectives with protecting its source code are twofold: • Protect the company's intellectual property while fostering innovation • Protect Oracle and its customers against malicious attempts to alter Oracle's source code or exploit security vulnerabilities

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	Oracle Cloud largely relies on Oracle products that are subject to Oracle Security Assurance activities. Oracle-developed code used solely in the cloud, that is, code that is not used in on-premises product distributions, is also subject to Oracle Software Security Assurance.
Identity & Access Management: Third Party Access	IAM-07.1	Does your organization conduct third-party unauthorized access risk assessments?	Oracle performs annual risk assessments that include identification, assessment, and prioritization of unauthorized third-party access.
	IAM-07.2	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	Oracle's corporate security controls can be grouped into three categories: administrative, physical, and technical security controls. • Administrative controls, including logical access control and human resource processes • Physical controls designed to prevent unauthorized physical access to servers and data-processing environments • Technical controls, including secure configurations and encryption for data at rest and in transit.
Identity & Access Management: User Access Restriction / Authorization	IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	In alignment with ISO 27001, Oracle has a Logical Access Control Policy applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest? • Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose? Customers are responsible for implementing controls that ensure access rights granted for their own personnel within their Oracle NetSuite account.
	IAM-08.2	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	Oracle enforces strong password policies (including length and complexity requirements) for the Oracle network, operating system, email, database and other accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. System-generated and assigned passwords are required to be changed immediately on receipt.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			Identity management systems are required to comply with Corporate Security Architecture requirements. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
	IAM-08.3	Do you limit identities' replication only to users explicitly defined as business necessary?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
Identity & Access Management: User Access Authorization	IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest? • Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?
	IAM-09.2	Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Oracle has an established process in granting access to employees with legitimate business need to managed applications, infrastructure systems, and network components. The access request goes through a review and approval workflow, applying the principle of least privilege. Oracle's privacy policies are described at https://www.oracle.com/legal/privacy/ Customer controls access to their cloud services.
Identity & Access Management: User Access Reviews	IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	Oracle NetSuite conducts a periodic review of privileged (includes administrator) access to production. The periodic access review is reviewed and validated by third-party auditors at least annually. Results are documented in the audit reports, and customers may request the audit reports through a self-service portal in their NetSuite Account Center.
	IAM-10.3	Do you ensure that remediation actions for access violations follow user access policies?	Remediation actions for access violations follow user access policies and standards. In alignment with ISO 27001 standard, any unauthorized access identified during continuous monitoring or during periodic User Access Review (UAR) is modified or removed. Results of the review and remediation actions are documented and retained.
	IAM-10.4	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed customer data has been improperly handled or accessed. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs).
Identity & Access Management: User Access Revocation	IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
	IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
Identity & Access Management: User ID Credentials	IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Single Sign-on (SSO) is a session and user authentication service that allows users to use one set of login credentials to access multiple applications. To use SSO for the Oracle NetSuite Content and Experience, administrators must configure Oracle NetSuite in Oracle IDCS using a Security Assertion Markup Language (SAML)

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			application. Refer to the "Configuring SSO for NetSuite" section of the NetSuite Help Center - https://docs.oracle.com/en/cloud/paas/identity-cloud/idcsc/netsuite.html
	IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	Oracle NetSuite supports many types of authentications for authenticating in the Oracle NetSuite User Interface (UI), as well as various authentication methods for API access to Oracle NetSuite, including open standards such as Security Assertion Markup Language (SAML 2.0). https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/book_4299752196.html
	IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	Oracle NetSuite supports many types of authentications for authenticating in the Oracle NetSuite User Interface (UI), as well as various authentication methods for API access to Oracle NetSuite, including open standards such as Security Assertion Markup Language (SAML 2.0) https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/book_4299752196.html
	IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	NetSuite is implementing a zero trust-based policy enforcement point to enforce legal and policy constraints on employee user access.
	IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	Oracle NetSuite uses a role-based access permission model to define usage of record types, tasks, and pages within the Oracle NetSuite application.
	IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	Two-Factor Authentication, or 2FA, is a feature available to Oracle NetSuite customers. Authenticator applications, text messages (SMS), and voice calls are the supported delivery methods for 2FA verification codes.
	IAM-12.7	Do you allow tenants to use third-party identity assurance services?	Oracle NetSuite supports the following inbound single sign-on options that use third-party providers: • Authentication using third-party identity provider compliant with SAML v2.0 • Authentication using a third-party OpenID Connect (OIDC) provider For more information, see - https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/book_4299752196.html

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	IAM-12.8	Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	Oracle NetSuite supports password minimum length, age, history, complexity, account lockout, lockout threshold, and session timeout policy enforcement. For more information, see - https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/chapter_4713604654.html
	IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	Oracle NetSuite customers have the ability to define their own password policy/parameters. However, the account lockout policy is a core application feature which is not configurable at the customer account level. This is currently set to six (6) invalid attempts. For more information, see - https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/chapter_4713604654.html
	IAM-12.10	Do you support the ability to force password changes upon first logon?	Oracle NetSuite customers have the option to enable "Require Password Change on Next Logon" for newly provisioned accounts to enforce password change upon first logon. For more information, see - https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/chapter_4713604654.html
	IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	Oracle NetSuite provides its users with self-service actions for resetting passwords or unlocking accounts. For more information, see - https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/chapter_4713604654.html
Identity & Access Management: Utility Programs Access	IAM-13.1	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	All privileged access to production, which includes utility programs managing virtual partitions, are restricted to authorized personnel via Identify Access Management (IAM). Access must be justified and approved before being granted. These are further secured through a restricted VPN and multifactor authentication.
Infrastructure & Virtualization Security: Audit Logging / Intrusion Detection	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	Oracle has tools and processes in place to help detect, investigate, and respond to security events. 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 firewalls, IDS, routers, switches, real-time monitoring, audit logging and reporting.
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security-incident management process. Access to security logs is provided on the basis of need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible. System components that store and provide access to the audit logs are housed within Oracle's data center co-location provider facilities where appropriate physical access controls are in-place. Only authorized Oracle personnel are allowed to enter the Data Centers.
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	Oracle's Information Security Standard is modeled after International Organization for Standardization (ISO) 27001. Oracle also maintains a mapping of its security controls to ISO 27001, Payment Card Industry – Data Security Standard (PCI DSS), and SOC 1 / SOC 2 requirements. In addition, Oracle has established processes and controls to maintain a privacy posture within the organization. Oracle NetSuite's security controls are audited by third-party assessors against the ISO 27001, PCI DSS, and SOC 1 / SOC 2.
	IVS-01.4	Are audit logs centrally stored and retained?	Oracle NetSuite stores logs in a centralized log server. The logs are retained based on the Oracle retention requirements. The retention period is also compliant with PCI DSS requirements.
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Oracle NetSuite utilizes a Security Information and Event Management (SIEM) tool to ingest security and access-related events from production systems and alert security personnel of potential Security events. Alerts are reviewed regularly, and verified security events are classified according to severity, documented in a ticketing system, and tracked through resolution.
Infrastructure & Virtualization Security: Change Detection	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	NetSuite's infrastructure is hosted in the Oracle Cloud Infrastructure (OCI). Virtualization technologies used are managed by OCI. For details, please refer to OCI's CAIQ – https://www.oracle.com/corporate/security-practices/cloud/

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	IVS-02.2	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	Oracle NetSuite has a configuration management system that monitors and controls changes made to infrastructure systems, including virtual machines.
	IVS-02.3	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	Oracle NetSuite is a software as a service. As such, changes to infrastructure are not visible to customers.
Infrastructure & Virtualization Security: Capacity / Resource Planning	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Oracle NetSuite hosted in OCI uses OCI Network Time Protocol (NTP) to synchronize systems on the network.
Infrastructure & Virtualization Security: Capacity / Resource Planning	IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Not applicable. Oracle NetSuite does not allow its network, storage, memory, or I/O levels to oversubscribe. To prevent oversubscribing, Oracle NetSuite conducts a quarterly review of its capacity levels and predicts a growth trend analysis to forecast capacity requirements and plan future hardware purchases.
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	While there is no automated restriction in place, Oracle NetSuite prevents oversubscription by conducting a quarterly review of its capacity levels and predicts a growth trend analysis to forecast capacity requirements and plan future hardware purchases. For more information on OCI's capacity management process, refer to the OCI CAIQ, located here https://www.oracle.com/corporate/security-practices/cloud/
	IVS-04.3	Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	Oracle applies service scaling best practices for its Oracle NetSuite service in OCI to ensure required capacity to service our customer are met. For more information on OCI's capacity management process, refer to the OCI CAIQ, located here https://www.oracle.com/corporate/security-practices/cloud/

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	To verify that Oracle meets its regulatory, contractual, and business requirement for systems used to provide the Oracle NetSuite service, Oracle NetSuite uses various software tools to monitor the availability and performance of Oracle NetSuite's environment and the operation of Oracle NetSuite's infrastructure and network components. Additionally, all planned maintenance is internally tracked. Unplanned downtimes are monitored by Oracle using system monitoring tools. Oracle provides real-time system availability status of its Oracle NetSuite Service through its online dashboard: https://status.netsuite.com/
Infrastructure & Virtualization Security: Management - Vulnerability Management	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	Oracle NetSuite performs vulnerability scans of its environment, including virtual machines, using industry-accepted scanning tools and methodology.
Infrastructure & Virtualization Security: Network Security	IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	Not applicable. Oracle NetSuite is a Software as a Service (SaaS) offering.
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Oracle NetSuite's network diagrams and data flow diagrams are reviewed at least annually and updated as needed.
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	Oracle security personnel periodically review security access lists on the NetSuite network.
	IVS-06.4	Are all firewall access control lists documented with business justification?	Oracle requires a valid business justification for every addition, modification, or deletion of network security list, ports and protocols. Additionally, the network security list change activity reports are reviewed on a regular basis.
Infrastructure & Virtualization Security:	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using	Standardized build scripts and configuration management tools are in place for system requirements, installation, and configuration settings of production servers. System hardening includes limiting ports, protocols, and services to what the business needs. Oracle architecture hardening standards are established and updated annually.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
OS Hardening and Base Controls		technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	Oracle continuously scans its environment for new vulnerabilities and updates systems accordingly as part of its system hardening practice.
Infrastructure & Virtualization Security: Production / Non-Production Environments	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Oracle gives customers the option to purchase additional non-production (e.g., test/sandbox) environments to provide logical separation of their environments.
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	Not applicable. Oracle NetSuite is a Software as a Service (SaaS) offering.
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	Oracle NetSuite logically segregates production and non-production environments.
Infrastructure & Virtualization Security: Segmentation	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	Oracle NetSuite utilizes firewalls to protect its system and network environments, and accesses the environments through a segregated network connection, which is dedicated to environment access control and isolated from Oracle's internal corporate network traffic.
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	Oracle NetSuite's infrastructure is hosted in Oracle Cloud Infrastructure (OCI). Oracle is responsible for managing OCI firewall configurations and the access to and from these devices through security access lists. In addition to OCI-hosted firewalls, Oracle has implemented a variety of controls to provide network-based security measures to protect its enterprise network and meet its legal, regulatory, and contractual requirements.
	IVS-09.3	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	Not applicable. Oracle NetSuite customers do not have access to the infrastructure systems and network components.
	IVS-09.4	Do you have the ability to logically segment or encrypt customer data	Oracle NetSuite provide customers isolation to help ensure that there is data segregation either at the persistence layer or in the application layer. Customers'

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	access and views are restricted to their account instance and data related only to their account. This access restriction is tested before every major release. For information on Oracle Cloud Infrastructure's (OCI) multitenancy environment, please refer to the OCI CAIQ – https://www.oracle.com/corporate/security-practices/cloud/
	IVS-09.5	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	Oracle NetSuite's infrastructure is hosted in Oracle Cloud Infrastructure (OCI). Oracle NetSuite uses internal- and external-facing firewalls to limit traffic to and from its environments through defined rule sets that are reviewed periodically.
Infrastructure & Virtualization Security: VM Security - Data Protection	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	Oracle NetSuite's infrastructure is hosted in Oracle Cloud Infrastructure's (OCI). Please refer to OCI's CAIQ for more details on the process of migrating to virtual servers – https://www.oracle.com/corporate/security-practices/cloud/
	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	Oracle NetSuite's network design for OCI deployments provides isolation of unrelated resources and limits access to data. Oracle NetSuite uses staging networks in OCI when migrating production data to virtual servers.
Infrastructure & Virtualization Security: VMM Security - Hypervisor Hardening	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	Access to Virtual Cloud Network (VCN) are restricted to authorized personnel based on Identity Access Management (IAM) group policy. Access must be justified and approved before being granted. Access management is performed through a bastion server, and additional security is provided by using VPN, multifactor authentication, SSO web login, and API keys.
Infrastructure & Virtualization Security: Wireless Security	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network	Oracle's Network Security Policy establishes formal requirements for the provision and use of wireless networks and connectivity to access the Oracle corporate network, including network segmentation requirements. Oracle IT manages wireless networks and monitors for unauthorized wireless networks.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		environment perimeter and to restrict unauthorized wireless traffic?	Network devices must be registered in an Oracle-approved information systems inventory per Oracle Information Systems Inventory Policy. This policy requires the accurate inventory and documented ownership of all information systems processing information assets throughout their lifecycle. For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
	IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	For administration of network security and network-management devices, Oracle requires IT personnel to use secure protocols with authentication, authorization, and strong encryption. Network devices must be located in an environment protected with physical access controls and other physical security measure standards defined by Global Physical Security (GPS).
	IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Oracle's Network Security Policy establishes formal requirements for the provision and use of wireless networks and connectivity to access the Oracle corporate network, including network segmentation requirements. Oracle IT manages wireless networks and monitors for unauthorized wireless networks.
Infrastructure & Virtualization Security: Network Architecture	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	Oracle NetSuite's network architecture diagrams do not indicate which are high-risk environments with legal compliance impacts. Instead, high-risk environments are identified and documented during Oracle's annual risk assessment exercise.
	IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks)	Oracle employs intrusion-detection systems within the Oracle intranet to provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle utilizes a network-based monitoring approach to detect attacks on open firewall ports within Oracle's intranet. Events are analyzed using signature detection, which is a pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to Oracle's IT security for review and response to potential threats.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		and/or distributed denial-of-service (DDoS) attacks?	For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
Interoperability & Portability: APIs	IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Customers may refer to Oracle NetSuite's Help Center for information about APIs - https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/set_15021347.html
Interoperability & Portability: Data Request	IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	Oracle NetSuite provides users the capability via role-based access to view a particular record or export data from the record into industry-standards formats (e.g., CSV, XML, HTML, JPG, Excel, or PDF) using standard Oracle NetSuite export functionality. For more information, refer to the "Oracle NetSuite Privacy and Security Feature Guidance" on Oracle NetSuite's SuiteAnswers portal – https://netsuite.custhelp.com/app/answers/detail/a_id/74138
Interoperability & Portability: Policy & Legal	IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	Oracle NetSuite provides various APIs for interoperability between NetSuite and third-party applications. Customers may refer to Oracle NetSuite's Help Center for information about these APIs - https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/set_15021347.html Additionally, the Oracle Subscription Services Agreement provides guidance on the use of Third-Party Applications: https://www.oracle.com/corporate/contracts/cloud-services/netsuite/contracts.html#ssa
	IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	Oracle does not allow virtual machine images to be ported or transferred to a new cloud provider.
	IPY-03.3	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Oracle NetSuite's Data Security Addendum is available at - https://www.oracle.com/corporate/contracts/cloud-services/netsuite/contracts.html
Interoperability & Portability: Standardized Network Protocols	IPY-04.1	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	Oracle NetSuite uses HTTPS protocol with Transport Layer Security (TLS) version compliant with PCI DSS as an established method for ensuring private, trustworthy, and reliable communication between computer programs over a network. Additionally, only recommended and approved cipher suites are used across Oracle NetSuite's public-facing websites.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Oracle NetSuite provides customers with a Help Center within the application where the required network protocol standards are described. For more information, please refer to "Supported TLS Protocol and Cipher Suites" in the help guide - https://docs.oracle.com/en/cloud/saas/Oracle NetSuite/ns-online-help/chapter_1554220186.html
Interoperability & Portability: Virtualization	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	Oracle NetSuite is a software as a service (SaaS) provider that is hosted in Oracle Cloud Infrastructure (OCI). Please refer to OCI's CAIQ for more details on the virtualization process – https://www.oracle.com/corporate/security-practices/cloud/
	IPY-05.2	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	Not applicable. Customers do not have access to Oracle NetSuite's infrastructure systems.
	IPY-05.3	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	Oracle NetSuite is a software as a service (SaaS) provider that is hosted in Oracle Cloud Infrastructure (OCI). Please refer to OCI's CAIQ for more details on the virtualization process – https://www.oracle.com/corporate/security-practices/cloud/
Mobile Security: Anti-Malware	MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption for their organization.
Mobile Security: Application Stores	MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		company data and/or company systems?	organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Approved Applications	MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security Approved Software for BYOD	MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	The Oracle Information Technology (OIT) organization keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. OIT is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. OIT provides automation to verify antivirus configuration. Oracle employees are required to comply with email instructions from OIT and are responsible for promptly reporting to the Oracle employee helpdesk any virus or suspected virus infection that cannot be resolved by antivirus software. Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. Any Oracle employee who is discovered violating this standard may be subject to disciplinary action up to and including termination of employment.
	MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption for their organization.
Mobile Security: Cloud Based Services	MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	Corporate Security architecture manages a variety of programs and leverages multiple methods of engaging with leadership and operational security teams responsible for Oracle operations, services, cloud, and all other lines of business. An example program for managing the security of Oracle's architecture is the Corporate Security Solution Assurance Process (CSSAP). CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle, so that projects are aligned with:

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• Pre-review: the risk management teams in each line of business must perform a pre-assessment of each project using the approved template • CSSAP review: the security architecture team reviews the submitted plans and performs a technical security design review • Security assessment review: based on risk level, systems and applications undergo security verification testing before production use
Mobile Security: Compatibility	MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Device Eligibility	MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full disk encryption software on their laptops and desktops, except where approved for justifiable business purposes. Data on the disk can only be accessed through the use of a private key stored as a password-protected file on the disk. A preboot login manager allows authorized users to login to unlock the key, boot the operating system, and access the data.
Mobile Security: Device Inventory	MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Device Management	MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Encryption	MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full disk encryption software on their laptops and desktops, except where approved for justifiable business purposes. Data on the disk can only be accessed through the use of a private key stored as a password-protected file on the disk. A preboot login manager allows authorized users to login to unlock the key, boot the operating system, and access the data.
Mobile Security:	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile	Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. Any Oracle employee who is

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Jailbreaking and Rooting		devices (e.g., jailbreaking or rooting)?	discovered violating this standard may be subject to disciplinary action up to and including termination of employment.
	MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Legal	MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption for their organization.
	MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?	Oracle places a strong emphasis on personnel security. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.
Mobile Security: Lockout Screen	MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	The Oracle Information Technology (OIT) organization keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. OIT is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. OIT provides automation to verify antivirus configuration. Oracle employees are required to comply with email instructions from OIT and are responsible for promptly reporting to the Oracle employee helpdesk any virus or suspected virus infection that cannot be resolved by antivirus software.
Mobile Security: Operating Systems	MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Mobile Security: Passwords	MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	The use of passwords is addressed in the Oracle Password Policy. Oracle enforces strong password policies (including length and complexity requirements) for the Oracle network, operating system, email, database and other accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. System-generated and assigned passwords are required to be changed immediately on receipt. Oracle personnel are obligated to follow rules for password length complexity, as well as other password requirements. Employees must keep their passwords confidential and secured at all times, and are prohibited from sharing their individual account passwords with anyone, whether verbally, in writing, or by any other means. Employees are not permitted to use any Oracle system or applications passwords for non-Oracle applications or systems.
	MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?	The use of passwords is addressed in the Oracle Password Policy. Oracle personnel are obligated to follow rules for password length complexity, as well as other password requirements. Employees must keep their passwords confidential and secured at all times, and are prohibited from sharing their individual account passwords with anyone, whether verbally, in writing, or by any other means. Employees are not permitted to use any Oracle system or applications passwords for non-Oracle applications or systems.
	MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	Oracle enforces strong password policies (including length and complexity requirements) for the Oracle network, operating system, email, database and other accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords.
Mobile Security: Policy	MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	Oracle implements a variety of technical security controls designed to protect information assets at rest and in transit. These controls are guided by industry standards and are deployed across the corporate infrastructure: • Corporate systems such as applications and collaboration tools • Removable storage media • Laptops and mobile devices
	MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption for their organization.
Mobile Security: Remote Wipe	MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.
	MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Security Patches	MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.
	MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Users	MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.
	MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	Access control refers to the policies, procedures, and tools that govern access to and use of resources. Examples of resources include a cloud service, physical server, file, application, data in a database, and network device.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• Least privilege is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties. • Default—deny is a network-oriented configuration approach that denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source network address, and destination network address.
Security Incident Management, E-Discovery, & Cloud Forensics: Contact / Authority Maintenance	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed customer data has been improperly handled or accessed. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs).
Security Incident Management, E-Discovery, & Cloud Forensics: Incident Management	SEF-02.1	Do you have a documented security incident response plan?	Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	In the event that Oracle determines that a confirmed security incident involving Personal Information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared. Incident history is also Oracle Confidential and is not shared externally.
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	The Oracle Data Processing Agreement describes Oracle's obligations in the event of a personal information breach. Please refer to the section on Incident Management and Breach Notification within Oracle's Data Processing Agreement: https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	SEF-02.4	Have you tested your security incident response plans in the last year?	Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed customer data has been improperly handled or accessed. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). GIS defines roles and responsibilities for the incident response teams embedded within the Lines of Business (LoBs). All LoBs must comply with GIS incident response guidance about detecting events and timely corrective actions. Corporate requirements for LoB incident-response programs and operational teams are defined per incident type: • Validating that an incident has occurred • Communicating with relevant parties and notifications • Preserving evidence • Documenting an incident itself and related response activities • Containing an incident • Eradicating an incident • Escalating an incident
Security Incident Management, E-Discovery, & Cloud Forensics: Incident Reporting	SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
	SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	In the event that Oracle determines that a confirmed security incident involving Personal Information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services.
Security Incident Management, E-	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-	Reflecting the recommended practices in prevalent security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Discovery, & Cloud Forensics: Incident Response Legal Preparation		custody management processes and controls?	implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets.
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
	SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
Security Incident Management, E-Discovery, & Cloud Forensics: Incident Response Metrics	SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed customer data has been improperly handled or accessed. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs).
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	Incident history is Oracle Confidential and is not shared externally.
Supply Chain Management, Transparency, and Accountability: Data Quality and Integrity	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	Access control refers to the policies, procedures, and tools that govern access to and use of resources. Examples of resources include a cloud service, physical server, file, application, data in a database, and network device. Least privilege is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties. Default—deny is a network-oriented configuration approach that denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source network address, and destination network address.
Supply Chain Management, Transparency, and Accountability: Incident Reporting	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
Supply Chain Management, Transparency, and Accountability: Network / Infrastructure Services	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	Oracle NetSuite regularly monitors uptime performance to maintain its Service Level Commitment with customers. Customers can monitor the Oracle NetSuite Service uptime status through an online dashboard: https://status.netsuite.com/
	STA-03.2	Do you provide tenants with capacity planning and use reports?	Capacity planning information is Oracle Confidential and is not shared externally.
Supply Chain Management, Transparency, and Accountability: Provider Internal Assessments	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	The Chief Corporate Architect, who reports directly to the Executive Chairman and Chief Technology Officer (CTO), is one of the directors of the Oracle Security Oversight Committee (OSOC). The Chief Corporate Architect manages the functional departments directly responsible for identifying and implementing security controls at Oracle.
Supply Chain Management, Transparency, and Accountability: Third Party Agreements	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	Oracle also has formal requirements for its suppliers to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle confidential information, and Oracle hardware assets placed in their custody

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. For more information see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ and https://www.oracle.com/corporate/suppliers.html
	STA-05.2	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers. Oracle also has formal requirements for its suppliers to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers are required to adopt when: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle Confidential information, and Oracle hardware assets placed in their custody In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. (https://www.oracle.com/corporate/security-practices/corporate/supply-chain/)
	STA-05.3	Does legal counsel review all third-party agreements?	Oracle Legal reviews third-party supplier agreements. Oracle's Supply Chain Risk Management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services.
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. https://www.oracle.com/corporate/security-practices/corporate/supply-chain/

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Outside of disaster recovery purposes, restoring customer data from backups on an ad-hoc basis is outside the scope of Oracle NetSuite's services. Customers may submit a request for assistance with these activities, but additional fees may apply.
	STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	Geographical residency is set depending on the customer's location. Oracle has a process in place to ensure that transfer of Customer data to another geographical location is reviewed and approved based on Oracle-established criteria and any applicable legal requirements.
	STA-05.7	Can you provide the physical location/geography of storage of a tenant's data upon request?	Customers can request the city and country information where their cloud service instances are provisioned. Customer account administrators may view this information in their NetSuite Account Center under the company information section. Alternatively, customers can request this information from their NetSuite account manager.
	STA-05.8	Can you provide the physical location/geography of storage of a tenant's data in advance?	Customers should discuss available choices for locations of their cloud service instances with their account representative.
	STA-05.9	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	Customers do not define the specific geographical location for data routing or resource instantiation. Without prejudice to any applicable regional data center restrictions for hosted Services specified in Your Services Agreement, Oracle may Process Personal Information globally as necessary to perform the Services. For more information, see: https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing
	STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
	STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	Access and use of customer data require customer consent. Oracle employees do not have access to customer data by default.
	STA-05.12	Do you provide the client with a list and copies of all subprocessing	List of sub processors for Oracle NetSuite Services are available to customers via the Oracle NetSuite Account Center.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		agreements and keep this updated?	Agreements with sub processors are Oracle Confidential.
Supply Chain Management, Transparency, and Accountability: Supply Chain Governance Reviews	STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers. Oracle also has formal requirements for its suppliers to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers are required to adopt when: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle Confidential information, and Oracle hardware assets placed in their custody In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. (https://www.oracle.com/corporate/security-practices/corporate/supply-chain/)
Supply Chain Management, Transparency, and Accountability: Supply Chain Metrics	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	Oracle also has formal requirements for its suppliers and partners to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle Confidential information, and Oracle hardware assets placed in their custody
	STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			associated with the malicious alteration of these products before purchase and installation by customers. Oracle also has formal requirements for its suppliers to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers are required to adopt when: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle Confidential information, and Oracle hardware assets placed in their custody In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. (https://www.oracle.com/corporate/security-practices/corporate/supply-chain/)
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers. Oracle also has formal requirements for its suppliers to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers are required to adopt when: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle Confidential information, and Oracle hardware assets placed in their custody In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. (https://www.oracle.com/corporate/security-practices/corporate/supply-chain/)

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Supplier SLA reporting is Oracle Confidential.
	STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Oracle such as SOC 1 Type II, SOC 2 Type II, information security management system (ISMS) Statements of Applicability and associated ISO 27001 certification for controls. Oracle also makes Service Level Agreement (SLA) uptime metrics available to customers. For customers wanting to assess Oracle NetSuite's security capabilities, they may refer to its audit and certification reports. Individual internal control metrics are not shared.
	STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?	Oracle NetSuite provides status and information on the availability of its Oracle NetSuite Service at its online status dashboard. Please refer to this URL - https://status.netsuite.com/
	STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?	Customers are responsible for data management policies and service level conflicts of interest in their environment. Oracle NetSuite annually reviews its key suppliers to ensure ongoing adherence to Service Level Agreements (SLAs) in order to address any non-conformance and to eliminate any conflicts of interests with its suppliers and its customers.
	STA-07.8	Do you review all service level agreements at least annually?	Oracle NetSuite monthly reviews its Service Level Agreements (SLAs) and any SLA-impacting events and relationships. Additionally, Oracle NetSuite regularly monitors uptime performance against its Service Level Commitment (SLC). Customers may also monitor availability of the Oracle NetSuite Service through an online status dashboard: https://status.netsuite.com/
Supply Chain Management, Transparency, and Accountability: Third Party Assessment	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	Oracle suppliers are required to protect the data and assets Oracle entrusts to them. These Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers are required to adopt when accessing Oracle or Oracle customer facilities, networks and/or information systems, handling Oracle confidential information, or controlling custody of Oracle hardware assets. Suppliers are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards. These standards cover a wide range of requirements in the following critical areas: • Personnel/human resources security • Business continuity and disaster recovery • Information security organization, policy, and procedures • Compliance and assessments

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• Security incident management and reporting • IT security standards • Baseline physical and environmental security
	STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	Oracle's Supplier Security Management Policy requires all lines of business which utilize third party providers to maintain a program which manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each particular supplier's goods or services are leveraged.
Supply Chain Management, Transparency, and Accountability: Third Party Audits	STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	Oracle's Supplier Security Management Policy requires all lines of business which utilize third party providers to maintain a program which manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each particular supplier's goods or services are leveraged.
	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Audit reports about Oracle cloud Services are periodically published by Oracle's third-party auditors. Reports may not be available for all services or all audit types or at all times. Customer may request access to available audit reports through a self-service portal in the customer's NetSuite Account Center. Customer remains solely responsible for its regulatory compliance in its use of any Oracle cloud services. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
Threat and Vulnerability Management: Antivirus / Malicious Software	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	Oracle NetSuite is a software as a service (SaaS) provider that is hosted in Oracle Cloud Infrastructure (OCI). Please refer to OCI's CAIQ for information on anti-malware programs installed on the infrastructure layer - https://www.oracle.com/corporate/security-practices/cloud/
	TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	Oracle NetSuite's network-based threat detection system regularly checks for updates to stay current with the latest version.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Threat and Vulnerability Management: Vulnerability / Patch Management	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Oracle regularly performs penetration testing and security assessments against, platforms, and applications in order to validate and improve the overall security of Oracle cloud Services.
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Oracle regularly performs application-layer vulnerability scans using automated scanning tools.
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Oracle regularly performs vulnerability scans of its operating systems. Any vulnerabilities noted are addressed in accordance with Oracle's vulnerability management and patching process, which are periodically assessed by third-party auditors.
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	Oracle may provide information which summarizes that point-in-time penetration testing and environment vulnerability scans are performed regularly, with a summary of findings. Oracle does not provide the details of identified weaknesses because sharing that information would put all customers using that product or service at risk. Please see the Oracle cloud Security Testing Policy for information about customer testing of Oracle cloud services: https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm
	TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	Oracle NetSuite employs a centralized patch management process that utilizes a combination of commercial and proprietary software to manage all current patch levels of its infrastructure systems supporting the Oracle NetSuite Service. For Oracle NetSuite Application patching, minor updates or patches are applied as needed.
	TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	The Oracle NetSuite Data Security Addendum describes the customer's security obligations. See the Oracle NetSuite Data Security Addendum here: https://www.oracle.com/corporate/contracts/cloud-services/netsuite/contracts.html#data-security
Threat and Vulnerability Management:	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile	Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Oracle's goal is to ensure

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Mobile Code		code operates according to a clearly defined security policy?	that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience. Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at: **Fostering security innovations.** Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help organizations implement and manage consistent security controls across the technical environments in which they operate, on-premises and in the clouds. **Reducing the incidence of security weaknesses in all Oracle products.** Oracle Software Security Assurance key programs include Oracle's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups, and the use of automated analysis and testing tools. **Reducing the impact of security weaknesses in released products on customers.** Oracle has adopted transparent security vulnerability disclosure and remediation policies. The company is committed to treating all customers equally, and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs.
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. OIT and corporate security organizations regularly promote awareness of mobile device security and good practice.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle