ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) v4.0 for Oracle Retail Cloud Services

September 2024 | Version 1.0

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 4.0 are related to specific Oracle cloud offerings 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

Developed by the Cloud Security Alliance, the Cloud Assessment Initiative Questionnaire (CAIQ) 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

ORACLE RETAIL AI FOUNDATION CLOUD SERVICE
ORACLE RETAIL AI FOUNDATION PRIVATE END POINT CLOUD SERVICE
ORACLE RETAIL AI FOUNDATION STORAGE CLOUD SERVICE
ORACLE RETAIL INVENTORY PLANNING OPTIMIZATION CLOUD SERVICE ADVANCED EDITION
ORACLE RETAIL LIFECYCLE PLANNING OPTIMIZATION CLOUD SERVICE ADVANCED EDITION
ORACLE RETAIL ASSORTMENT AND SPACE OPTIMIZATION CLOUD SERVICE ADVANCED EDITION
ORACLE RETAIL INSIGHTS CLOUD SERVICE ADVANCED EDITION
ORACLE RETAIL DATA STORAGE CLOUD SERVICE
ORACLE RETAIL DATA COMPUTE CLOUD SERVICE
ORACLE RETAIL DATA COMPUTE PRIVATE ENDPOINT CLOUD SERVICE
ORACLE RETAIL MERCHANDISING FOUNDATION CLOUD SERVICE
ORACLE RETAIL ALLOCATION CLOUD SERVICE
ORACLE RETAIL INVOICE MATCHING CLOUD SERVICE
ORACLE RETAIL PRICING CLOUD SERVICE

ORACLE RETAIL FISCAL MANAGEMENT CLOUD SERVICE
ORACLE RETAIL MERCHANDISING CLOUD SERVICES SUITE HIGH PERFORMANCE EDITION
ORACLE RETAIL MERCHANDISING CLOUD SERVICES SUITE EXTREME PERFORMANCE EDITION
ORACLE RETAIL INTEGRATION CLOUD SERVICE
ORACLE RETAIL INTEGRATION CLOUD SERVICE HIGH PERFORMANCE EDITION
ORACLE RETAIL MERCHANDISE FINANCIAL PLANNING CLOUD SERVICE ADVANCED EDITION
ORACLE RETAIL ASSORTMENT PLANNING CLOUD SERVICE ADVANCED EDITION
ORACLE RETAIL XSTORE OFFICE CLOUD SERVICE
ORACLE RETAIL CUSTOMER AND SEGMENT MANAGEMENT CLOUD SERVICE
ORACLE RETAIL PROMOTION ENGINE CLOUD SERVICE
ORACLE RETAIL CAMPAIGN AND DEAL MANAGEMENT CLOUD SERVICE
ORACLE RETAIL LOYALTY AND AWARDS CLOUD SERVICE
ORACLE RETAIL GIFT CARDS CLOUD SERVICE
ORACLE RETAIL ORDER ORCHESTRATION CLOUD SERVICE
ORACLE RETAIL ORDER ADMINISTRATION CLOUD SERVICE
ORACLE RETAIL EFT CONNECT CLOUD SERVICE
ORACLE RETAIL BRAND COMPLIANCE CLOUD SERVICE
ORACLE RETAIL SUPPLIER EVALUATION CLOUD SERVICE
ORACLE RETAIL ENTERPRISE INVENTORY CLOUD SERVICE
ORACLE RETAIL STORE OPERATIONS CLOUD SERVICE

CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ) VERSION 4

Control Domain: Audit & Assurance

Question ID	Consensus Assessment Question	Oracle Response
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle's Business Assessment & Audit (BA&A) is an independent global audit organization which performs global processes and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards and select laws and regulations across Oracle's Lines of Business (LOB) and business units. Any key risks or control gaps identified by BA&A during these reviews are tracked through remediation. These reviews, identified risks, or control gaps are confidential and shared with executive leadership and Oracle's Board of Directors. The audit rights of customers for whom Oracle processes data are described in your agreement. For more information, see https://www.oracle.com/contracts/cloud-services/. The audit rights of customers of Oracle services are described in the Oracle Services Privacy Policy. For more information, see https://www.oracle.com/legal/privacy/services-privacy-policy.html

		Oracle Retail Cloud Service Applications implement audit and assurance policies, procedures, and standards documented and approved. Oracle Retail Cloud Service Applications publishes SOC 1 and SOC 2 reports annually. These are available for customer review upon request.
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Oracle Retail Cloud Services standards supporting Oracle Corporate Security policies are reviewed annually and updated as needed.
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	See A&A-01.1. Oracle's Business Assessment & Audit (BA&A) is independent. Its operational activities and procedures are conducted at least annually in alignment with the Institute of Internal Auditors (IIA) Standards. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/business-assessment-audit/
		Independent external audits and assessments of Oracle Retail Cloud Services are conducted at a minimum on an annual basis. Customers may request access to available audit reports for a particular Oracle SaaS Cloud Service through My Oracle Support (MOS) or via Sales.
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	See A&A-01.1. Oracle's Business Assessment & Audit (BA&A) is independent. Its operational activities and procedures are conducted in alignment with Institute of Internal Auditors (IIA).
		Independent external audits and assessments of Oracle Retail Cloud Services are approved based on risk plans reviewed under Oracle risk policies and standards. For more information, see; https://www.oracle.com/corporate/cloud-compliance/.
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Oracle Retail Cloud Services engages with external assessment entities and independent auditors to verify that Oracle Retail Cloud Services have a comprehensive control environment that includes policies, processes and security controls for the delivery of Oracle's applications, infrastructure and platform services. These efforts conform with ISO/IEC 27001 standards and Oracle Corporate Security Policies. For more information see: https://www.oracle.com/corporate/cloud-compliance/.

A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	An audit management process inclusive of risk analysis, security control assessments, remediation schedules and reporting are in place for Oracle Retail Cloud Services and followed for internal and external audits. Oracle Retail Cloud Services maintain PCI DSS validation for in-scope payment applications and issues SOC 1 and SOC 2 reports annually for all cloud services. These are available for customer review upon request.
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Any key risks or control gaps identified by Oracle's Business Assessment & Audit (BA&A) during these reviews are tracked through remediation. Risk-based action plans to address audit findings are established, documented, and communicated to BA&A for approval by Oracle's Lines of Business with evaluation by BA&A.
		Oracle Retail Cloud Services implement a risk-based, documented and approved corrective plan to remediate audit findings. Any key risks or control gaps identified during an internal or external compliance assessment for Oracle Retail Cloud Services follow a defined process following a risk-based approach to remediation.
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Risks identified by Oracle's Business Assessment & Audit (BA&A) and associated action item status are confidential and shared with executive leadership and Oracle's Board of Directors.
		Oracle Retail SaaS Application's remediation status of audit findings is reviewed and reported to appropriate stakeholders until findings are resolved.

Control Domain: Application & Interface Security

Question ID	Consensus Assessment Question	Oracle Response
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's	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. Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at: **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

	application security capabilities?	cultivation of security leaders within development groups, and the use of automated analysis and testing tools. **Reducing the impact of security weaknesses in Oracle products and services** Oracle has mature security vulnerability disclosure and remediation practices. The company is committed to treating all customers equally and delivering the best possible security maintenance experience through the Critical Patch Update and Security Alert programs. **Fostering security innovations.** Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help enable organizations to implement and manage consistent security policies across the hybrid cloud data center: database security and identity management, and security monitoring and analytics. For more information, see https://www.oracle.com/corporate/security-practices/assurance/
		Oracle Retail Cloud Services adhere to the OSSA Standards and are reviewed for compliance throughout the supported lifecycle. The OSSA (Oracle Software Security Assurance Practices) policies are reviewed annually and updated as needed.
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Oracle Retail Cloud Services adhere to the OSSA Standards and are reviewed for compliance throughout the supported lifecycle. The OSSA (Oracle Software Security Assurance Practices) policies are reviewed annually and updated as needed.
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/configuration.html
		Oracle Retail Cloud Service have baseline requirements to secure, document and to deliver the service to cloud operations teams in a secured configuration. The security of cloud configurations is planned from the design phase by the development team. Testing is performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment.
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Oracle Retail Cloud Services have technical and operational metrics are in place to help drive compliance to business objectives, security requirements and compliance obligations. Oracle Retail Cloud Services teams maintain a set of defined technical and operational metrics to monitor adherence to business objectives, security requirements and compliance obligations.

AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	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. Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. All Oracle developers are required to be familiar with these standards and apply them when designing and building products. The coding standards have been developed over several years and incorporate best practices as well as lessons learned from ongoing vulnerability testing by Oracle's internal product assessment teams. The Secure Coding Standards are a key component of Oracle Software Security Assurance and adherence to the Standards is assessed throughout the supported life of all Oracle products.
		Oracle Retail Cloud Services adhere to the SDLC process defined by OSSA Standards and implemented for application design, development, deployment, and operation per organizationally designed security requirements. OSSA Standards and are reviewed for compliance throughout the supported lifecycle. See: https://www.oracle.com/corporate/security-practices/assurance/
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Security assurance analysis and testing assess security qualities of Oracle products against various types of attacks. There are two broad categories of tests: static and dynamic analysis. **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 as a variety of internally developed tools, to catch problems while code is being written. Typically, analysis of these scan reports involves senior engineers from the product teams who are well-familiar with the product code sorting out false positives from real issues and reducing the number of false positives. **Dynamic analysis** activity takes place during latter phases of product development because it requires that the product or component be able to run. Dynamic analysis is aimed at externally visible product interfaces and APIs, and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing within Oracle. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
		Oracle Retail Cloud Services have defined testing strategies as part of our Development Security Operations (DevSecOps) development principles. We consistently validate all Cloud Service application upgrades through a defined vulnerability testing process. Oracle regularly performs penetration and vulnerability testing and security assessments against the Oracle Cloud infrastructure, platforms, and applications. These tests are intended to validate and improve the overall security of Oracle Retail Cloud Services.
AIS-05.2	Is testing automated when applicable and possible?	Oracle Retail Cloud Services Applications follow a development pipeline process which is automated where possible and includes application regression testing and security testing.

AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Cloud services are deployed in a specific configuration, or a small number of configurations. Testing must be performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment. Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/configuration.html
		Oracle Retail Cloud Services code deployments are undertaken over secured connections, code is scanned and mapped for potential threats with rigid access control and clear separation of duties throughout the development team.
AIS-06.2	Is the deployment and integration of application code automated where possible?	Oracle Retail Cloud Services are deployed using an automated provisioning tool and OCI IAM. See: https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/books.html

AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Oracle fixes significant security vulnerabilities based on the likely risk they pose to customers. The issues with the most severe risks are fixed first. Fixes for security vulnerabilities are produced in the following order:
		• Main code line first—that is the code line being developed for the next major release of the product
		• For each supported version that is vulnerable:
		  ○ Fix in the next patch set if another patch set is planned for that supported version
		  ○ Creation of Critical Patch Update patch
		For more information, see https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html

		Application security vulnerabilities are identified and remediated following defined processes. Oracle Retail Cloud Services follow a clearly defined process for regularly testing, assessing, evaluating, and maintaining the effectiveness of the technical and organizational security measures described. Regular scans are conducted, Oracle Retail Developers use static and dynamic analysis tools to detect security defects in Oracle code prior to deploying to production. Identified issues are evaluated and addressed in order of priority and severity. Oracle Retail 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-07.2	Is the remediation of application security vulnerabilities automated when possible?	Oracle Retail Cloud Services security vulnerabilities are remediated through the build and release pipeline. All application security updates are delivered through security patches and this process is automated whenever possible. Oracle Retail Cloud Service development teams are required to deliver the service to cloud operations teams in a secured configuration. Testing is

		performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment

Control Domain: Business Continuity Management & Operational Resilience

Question ID	Consensus Assessment Question	Oracle Response
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	The Risk Management Resiliency Program (RMRP) objective is to establish a business resiliency framework to enable efficient Line of Business (LOB) response to business interruption events affecting Oracle's operations. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/ The RMRP is comprised of several sub-programs: emergency response to unplanned and emergent events, crisis management of serious incidents, technology disaster recovery and business continuity management. The program goal is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored. The RMRP is implemented and managed locally, regionally, and globally. The RMRP program management office provides executive scorecard reporting on program activities, planning and plan testing status within the LOBs.
		Oracle Retail Cloud Services have a detailed SaaS Business Continuity / Disaster Recovery (BCDR) Program. The details of the SaaS Cloud Services BCDR program are covered under the Risk Management resiliency Program (RMRP). The program is driven by Policy documents like H&D Policy, DPA and SaaS Pillar Document. Risk Assessment, Business Impact Analysis and Business Continuity Plans are annually reviewed and updated. For operational purposes Crisis Communication Plan, DR Staffing Plan and Disaster Recovery Procedures are maintained. Periodic exercises are executed, results are documented, and findings are followed through to completion. Customer facing Disaster Recovery Test summary reports are published upon completion of each DR test cycle. See for additional information: https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	The RMRP policy mandates an annual operational cycle for (LoB) planning, evaluation, training, validation, and executive approvals for critical business operations. Oracle's Risk Management Resiliency Program defines requirements and standards for all Oracle LOBs regarding plans for and response to potential business disruption events. It also specifies the functional LOB roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across geographies. A centralized RMRP

		Program Management Office (PMO) has oversight responsibilities for the LoB compliance to the program. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
		Oracle Retail Cloud Applications policies (including business continuity management and operational resilience policies) are reviewed annually and updated as needed. Oracle Retail Cloud Services business continuity and operational resilience strategies published https://www.oracle.com/assets/retail-cloud-service-2613359.pdf:
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	The RMRP Program is generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance. For more information about the program and requirements for Oracle Lines of Business, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
		Oracle Retail Cloud Services have the criteria used for Services business continuity and operational resilience strategies that are based on industry requirements and published: https://www.oracle.com/assets/retail-cloud-service-2613359.pdf:
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	The RMRP PMO develops guidance as aids to LoB Risk Managers in managing their LoB's business continuity plans, testing and training procedures. The RMRP program requires all LoBs to: • Identify relevant business interruption scenarios, including essential people, resources, facilities and technology • Define business continuity plans and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Obtain approval of the plans from the LoB's executive For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	See BCR-03.1
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and	LOBs are required to annually review their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new technology or revised business processes. Critical LoBs must: • 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

	operational resilience plans?	• 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 For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
		Oracle Retail Cloud Services Risk Assessment, Business Impact Analysis and Business Continuity Plans are documented, developed, maintained, and updated to support business continuity and operational resilience plans.
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Business Continuity and operational resilience documentation is available to internal authorized stakeholders.
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations. See BCR-03.1
		Oracle Retail Cloud Services reviews its business continuity documentation at least annually in accordance with Oracle Corporate policy and updated as needed.
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	The critical LoBs (including Oracle Retail Cloud Services) 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resiliencemanagement/business-continuity.html
		Oracle Retail Cloud Services have a detailed SaaS Business Continuity / Disaster Recovery (BCDR) Program. The details of the SaaS Cloud Services BCDR program is covered under the Risk Management resiliency Program (RMRP) Oracle Retail Cloud Services conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability.
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Oracle Retail Cloud Services have a detailed SaaS Business Continuity / Disaster Recovery (BCDR) Program. The details of the SaaS Cloud Services BCDR program is covered under the Risk Management resiliency Program (RMRP). The procedures establish a communication plan for stakeholders and participants. See: https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
BCR-08.1	Is cloud data periodically backed up?	Oracle Retail Cloud Services maintains a periodic production backup of data which is undertaken in accordance with the Oracle hosting and delivery policy https://www.oracle.com/corporate/contracts/cloudservices/hosting-delivery-policies.html

BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Oracle Retail Cloud Services meet the confidentiality, integrity, and availability of backup data for applicable data plane backup requirements, as defined by the Cloud Compliance Standard for Resilience and Crisis Management. Backups are monitored, and issues relating to backup failure are tracked to resolution.
BCR-08.3	Can backups be restored appropriately for resiliency?	Oracle Retail Cloud Services undertakes backups in accordance with PCI DSS v4.0 Requirement 9.4 and as published in the "Oracle Hosting and Delivery Policy": https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html Oracle Retail Cloud Services do not undertake restoration of data on behalf of customers. Customer data should be exported directly via the Oracle Retail Cloud Services.
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Oracle's corporate Disaster Recovery (DR) plan focuses 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 a disaster, whether natural or man-made. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/disaster-recovery.html.
		Oracle Retail Cloud Services have a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters. Oracle Retail Cloud Services conducts annual reviews of business continuity plans with the objective of maintaining operational recovery capability.
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Oracle Retail Cloud Services DR and BCR plans are reviewed annually and updated as needed to maintain operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes.
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Oracle Retail Cloud Services DR and BCR plans are reviewed annually and exercised annually or as needed when significant changes occur.
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	Oracle generally does not involve external 3rd parties during DR exercise.
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable	Oracle maintains a redundant network infrastructure, including DNS servers to route between primary and secondary sites, network devices, and load balancers. Oracle cloud 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. For more information, see

	minimum distance in accordance with applicable industry standards?	https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
		Oracle deploys the Oracle Retail Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services. For more information, please refer to the following documents at https://www.oracle.com/contracts/cloud-services/: • Oracle Industries Cloud Services Pillar • Oracle Cloud Hosting and Delivery Policies

Control Domain: Change Control & Configuration Management

Question ID	Consensus Assessment Question	Oracle Response
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Oracle Retail Cloud Services follow formal change management procedures to provide review, testing, and approval of changes prior to deployment in the Oracle Cloud production environment. Changes made through change management procedures include system and service maintenance activities, management of application upgrades and updates, and coordination of customer specific changes where required. For changes to your services that are governed by Oracle's change control procedures please see: Oracle Cloud Hosting and Delivery Policies. https://www.oracle.com/contracts/cloud-services/
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Oracle Retail Cloud Services adhere to Oracle Corporate policies and reviews Retail SaaS Applications standards annually and updates as needed.
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Oracle Retail Cloud Services are deployed using a strict, baseline deployment which helps implement consistent deployment standards against each version release.

CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Oracle Corporate Security Solution Assurance Process (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 whether asset management occurs internally or externally. 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: • 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 Reviews ensure that projects are aligned with: • Oracle Corporate Security Architecture strategy and direction • Oracle Corporate security, privacy and legal policies, procedures and standards For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
		Oracle Retail Cloud Services review the risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced). All Oracle Retail Cloud Services are required to have these changes reviewed and approved by the Oracle Corporate Security Solution Assurance Process (CSSAP). All Oracle Retail Cloud Services are required to meet OSSA and be reviewed and approved by the Oracle Corporate Security Solution Assurance Process (CSSAP).
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted	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. For more information, https://www.oracle.com/corporate/security-practices/corporate/access-control.html Oracle's Information Systems Asset Inventory Policy requires that an accurate and current inventory be maintained for all information systems holding critical and highly critical information assets in Oracle Corporate and cloud infrastructures, including the physical location. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
		Oracle Retail Cloud Services follow the Oracle Corporate policies and standards that are in place outlining restrictions for adding, removing, and updating Oracle assets. Additionally, technical restrictions are in place where possible.

		For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	Oracle published change management process does include provision within the SLA for changes which may impact the application availability, end user authorization for such change is part of the approval chain prior to the change process implementation.
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Oracle Retail Cloud Services have change management baselines established for all relevant authorized changes on Oracle Retail Cloud Services assets.
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Oracle Retail Cloud Services detection measures are implemented with proactive notification for changes to a customer's environment that deviate from established baseline configurations. Oracle Retail Cloud Services use a centralized system for managing the access and integrity of device configurations. Change controls are in place to help ensure only approved changes are applied. Regular audits are performed to confirm compliance with security and operational procedures. Also, internal weekly scans are performed on the infrastructure.
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Oracle Retail Cloud Services have implemented standards and procedures to manage exceptions, including emergencies, in the change and configuration process.
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	Please see CCC-01.1 Oracle Retail Cloud Services exception process aligns with the GRC-04: Policy Exception Process.
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Changes to Oracle Retail Cloud Services environments include provisions to revert change if necessary. Processes are in place to proactively roll back changes to a previously known "good state". Standard operating procedures (SOP) define the steps to follow, including implementation, pre/peri/post validation, and rollback, as applicable.

Control Domain: Cryptography, Encryption & Key Management

Question ID	Consensus Assessment Question	Oracle Response
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle has formal cryptography, encryption, key management requirements, cryptographic algorithms and protocols. Compliance with these requirements is monitored by Oracle Global Product Security. Oracle products are required to use up-to-date versions of approved security-related implementations. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms. 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. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/
		Oracle Retail Cloud Services adhere to documented standards supporting Oracle corporate encryption and key management policies. These standards are documented, managed, communicated, applied, and evaluated. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address cryptography, encryption, and key management) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services review encryption and key management procedures at least annually and updates these as needed.
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services. The group is primarily responsible for making technical decisions and authoring internal standards to address government and industry requirements. Representatives from Corporate Security and development organizations define best practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence, and including roles and responsibilities. CRB's responsibilities include: • Creating and maintaining standards for cryptography algorithms, protocols, and their parameters • Providing approved standards in multiple formats, for readability and automation • Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle • Providing practical guidance on using cryptography

		• Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography
		Oracle Retail Cloud Services review cryptography roles and responsibilities in accordance with Oracle Corporate policy and must be approved by the Corporate Security Solution Assurance Process (CSSAP). For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Solutions for managing encryption keys and cryptographic libraries at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). Oracle Global IT 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 • Replacement schedule for various types of encryption keys For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
		Oracle Retail Cloud Services encrypts data at-rest and in transit in accordance both with Oracle corporate policy and PCI DSS v4.0.
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
		Appropriate data protection encryption algorithms are used based on data classification, associated risks, and encryption technology usability for Oracle Retail Cloud Services.
CEK-05.1	Are standard change management procedures established to review, approve, implement, and communicate cryptography, encryption, and key management	Change management is mandatory for all Oracle cryptography. Oracle Global IT 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

	technology changes that accommodate internal and external sources?	• Replacement schedule for various types of encryption keys For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
		Oracle Retail Cloud Services manage its change management processes in relation to cryptography in alignment with Oracle corporate policy
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Representatives from Corporate Security and development organizations define recommended practices related to using and implementing cryptography in Oracle products, derived from frequent reviews of existing industry practices and current threat intelligence. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html
		Changes to cryptography, encryption and key management-related systems, policies, and procedures, are managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis. Oracle Corporate Security defines the requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Oracle Retail Cloud Services adheres to these standards and must be approved per the Corporate Security Solution Assurance Process (CSSAP).
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Representatives from Corporate Security and development organizations define recommended practices related to using and implementing cryptography in Oracle products, derived from frequent reviews of existing industry practices and current threat intelligence. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html
		Oracle Retail Cloud Service cryptography, encryption, and key management risk programs are established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	No, Oracle Retail Cloud Services undertake all data encryption on behalf of the Customer.
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Encryption and key management systems, policies and processes are audited as part of our compliance function. Please see CEK-01.1

CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Encryption and key management systems, policies, and processes are audited, at a minimum, on an annual basis.
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Cryptographic keys are generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications. Oracle Retail Cloud Services use the up-to-date versions of the Oracle formal cryptography, encryption, and key management requirements and approved security-related implementations. Oracle modifies these standards as industry and technology evolve.
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes. Oracle Retail Cloud Services private keys are provisioned for a unique purpose and are managed, and the cryptography secrets adhere to the Oracle Corporate Key Management Standards for secure access. Oracle Retail Cloud Services keys are provisioned and stored in accordance with Oracle policy. Oracle policy and standards require all keys to be managed securely.
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Oracle has a formal Key Management Program supported by processes, procedures, and recommendations (aligned with NIST controls) that define specifics regarding key rotation. For Oracle Retail Cloud Services, cryptographic key rotation occurs based on regulation, certification, or for other security reasons.
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory	Oracle Retail Cloud Service cryptographic keys are revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions.

	requirement provisions?	
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Oracle Corporate has defined processes and technical measures in place that define the approved methods for key destruction, revocation of keys stored in hardware security modules and that address legal and regulatory requirements. These standards are part of the OSSA (Oracle Software Security Assurance Practices). Oracle Retail Cloud Services have established and implemented procedures to enforce segregation of key management and key usage duties. Key management encompasses the entire life cycle of cryptographic keys and has identified a method for establishing and managing keys in each management phase from generation, installation, storage, rotation, and destruction.
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Oracle Retail Cloud Services adhere to Oracle Software Security Assurance Practices for all key management practices. Processes, procedures, and technical measures are in place to create keys in a pre-activated state. Keys are not created prior to authorization to use.
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Oracle Retail Cloud Services adhere to Oracle Software Security Assurance Practices for all key management practices. Processes, procedures, and technical measures are in place to monitor, review and approve key transitions. Oracle Retail Cloud Services leverages key management software that allows for the approval and change of state for all key change of state transitions.
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at	Oracle Retail Cloud Services adhere to Oracle Software Security Assurance Practices for all key management practices. Processes, procedures, and technical measures are in place to deactivate keys as required. Oracle Retail

	the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Cloud Services leverages key management software that allows for the deactivation and key change of state.
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Oracle Retail Cloud Services adhere to Oracle Software Security Assurance Practices for all key management practices. Processes, procedures, and technical measures are in place to manage archived keys in a secure repository. Oracle Retail Cloud Services key management is secured and deployed in accordance with Oracle corporate policy for access control. https://www.oracle.com/corporate/security-practices/corporate/access-control.html
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Oracle Retail Cloud Services adhere to the OSSA Cryptography Standard which adheres to Oracle Corporate Security's formal policies and procedures governing the use of encryption. Oracle Retail Cloud Services have formal processes, procedures, and technical measures for encrypting customer data in transit (e.g., HTTPS TLS 1.2, SFTP) and at rest (e.g., currently AES-256).
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory	Processes, procedures and technical measures to assess operational continuity risks are defined, implemented and evaluated to include legal and regulatory requirement provisions.

	requirement provisions?	
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes. Oracle Retail Cloud Services have key management system processes, procedures, and technical measures defined and implemented. Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services, including legal and regulatory requirements. in accordance with Oracle Corporate policy, these must be approved by the Corporate Security Solution Assurance Process (CSSAP) For more information see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html See also: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html

Control Domain: Data Center Security

Question ID	Consensus Assessment Question	Oracle Response
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Oracle's Media Sanitization Policy specifies requirements including secure disposal of equipment and media used for data storage. This policy is established, documented, approved, communicated, and maintained.
		Oracle Retail Cloud Services have processes and procedures to comply with Oracle's Media Sanitization and Disposal Policy and Enterprise Engineering Media Sanitization and Disposal Standard. Development of this standard has been guided by Corporate Information Security Policies, guidance from NIST SP800-88 Rev. 1 and has been adapted to align with Oracle policies and standard practices.
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	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. For more information, https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
		Oracle Retail Cloud Services is aligned with Oracle's Media Sanitization and Disposal Policy and PCI DSS v4 Requirement 3.2.1 which requires that data is securely deleted.
DCS-01.3	Are policies and procedures for the secure disposal of	Oracle Corporate Security policies (including polices that address secure disposal of equipment outside the organization's premises) are reviewed annually and updated as needed.

	equipment used outside the organization's premises reviewed and updated at least annually?	Oracle Retail Cloud Services follow the Oracle Corporate Security policies, including polices that address secure disposal of equipment outside the organization's premises.
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Oracle's Information Systems Inventory Policy requires that Line of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware and software. This policy is established, documented, approved, communicated, and maintained. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
		Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services, including legal and regulatory requirements. Oracle Retail Cloud Service's use these key management system processes, procedures and technical measures as defined for its hardware lifecycle and data information policy. Accurate and comprehensive inventories of information systems, hardware and software are maintained and updated regularly.
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Oracle Retail Cloud Services require Manager approval for the relocation of all datacenter assets in accordance with published corporate policy. For more information, see the 'Oracle Cloud Change Management Policy' section of the Oracle Cloud Hosting and Delivery Policies document.: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address the relocation or transfer of hardware, software, or data/information to any location) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services follow the Oracle Corporate Security policies, including the polices that address secure disposal of equipment outside the organization's premises.
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html
		Oracle Retail Cloud Services relies on the Oracle Global Physical Security policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities). Oracle Global Physical Security manage all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets.

DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address safe and secure working environments) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services relies on Oracle Global Physical Security to manage all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. See https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Policies and procedures for the secure transportation of physical media are established, documented, approved, communicated, enforced, evaluated, and maintained. For more information see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address the secure transportation of assets) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services follows the "Secure Data Transfer using Encrypted Media" Standard Operating Procedure. This SOP defines hardware requirements, encryption levels and the procedural steps that must be taken to transport physical media. This SOP is reviewed annually and updated as needed.
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Oracle's formal Information Protection Policy sets forth the requirements for classifying and handling public and confidential information. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
		Per the Oracle Information Protection Policy, Oracle Retail Cloud Services information assets are classified according to the sensitivity and criticality of information they store, transmit, and receive.
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	The Oracle Information Systems Inventory Policy requires that Lines of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware, and software. Inventories must be managed within an approved inventory system. This policy defines required identifying attributes to be recorded for server hardware, software, data held on information systems, and information needed for disaster recovery and business continuity purposes.
		Oracle Retail Cloud Services catalogues and tracks assets in adherence with the Oracle Information Systems Inventory Policy. This policy requires accurate and comprehensive inventory of information systems, hardware, and software. Inventories must be managed within an approved inventory system. All system access is provisioned on a need-to-know basis. For more information see: https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html

DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Oracle Global Physical Security uses 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. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html Oracle Retail Cloud Services relies on Oracle Global Physical Security to manage all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets.
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	The goal is to balance prevention, detection, protection, and response, while maintaining a work environment that fosters collaboration among Oracle employees. Oracle Retail Cloud Services relies on Oracle Global Physical Security to manage all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets.
DCS-08.1	Is equipment identification used as a method for connection authentication?	Equipment identification is used as a method for connection authentication. The VPN that Oracle staff use to connect to Oracle Retail Cloud Services uses machine certificates and other identifiers to validate that the device is Oracle owned and provisioned before allowing access to resources. Oracle Retail Cloud Services manages equipment identification in alignment with the ISO 27001 standard.
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html

DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Oracle uses 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 and CCTV monitoring and recording. The access control system logs and CCTV recordings are retained for a period of 30-90 days as defined in Oracle's Record Retention Policy which are based on the facility's function, risk level and local laws. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Personnel are trained in incident response and escalation procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Data centers hosting Oracle cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate 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), standards compliance, and geopolitical considerations among other criteria. Oracle cloud service 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. Personnel are trained in procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Please see DCS-12.1
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned	Please see DCS-12.1

	intervals for continual effectiveness?	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Please see DCS-12.1

Control Domain: Data Security & Privacy Lifecycle

Question ID	Consensus Assessment Question	Oracle Response
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Oracle's information-asset classification determines corporate data-security requirements for Oracle-managed systems. Oracle policies provide global guidance for appropriate controls designed to protect corporate, cloud and customer data in accordance with the data classification. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/
		Oracle Retail Cloud Services follow Oracle's Information Asset Classification Policy. The policy provides GBU guidance and determines appropriate controls to protect data in accordance with the Oracle data classification and handling of data throughout its lifecycle. Oracle Retail Cloud Services follow Oracle's Information Asset Classification Policy according to all applicable laws and regulations.
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Oracle policies (including polices that address data security and privacy) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services security and privacy procedures are reviewed annually and updated as needed in accordance with Oracle Corporate policy.
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Industry accepted methods are applied for secure data disposal from storage media. 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/
		Oracle Retail Cloud Services follows Oracle's Media Sanitization and Disposal Policy and meets PCI DSS v4.0 Requirement 3.2.1.

DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Oracle Retail Cloud Services document and maintain data inventories and data flows. The Oracle Retail Reference Model is a collection of detailed implementation information for retailers and partners, including business process models, technical models, APIs and a retail glossary. See: https://www.oracle.com/retail/products/reference-model/ See: https://www.oracle.com/legal/privacy/services-privacy-policy.html
DSP-04.1	Is data classified according to type and sensitivity levels?	Oracle categorizes information into four classes- Public, Internal, Restricted, and Highly Restricted-with each classification requiring corresponding levels of security controls, such as encryption requirements for non-Public data. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Data flow documentation is created and maintained by Oracle Retail Cloud Services. This documentation is for internal use only. Oracle Retail Cloud Services diagrams are available during a client audit. Customer audits may be performed annually per the Oracle Data Processing agreement, section 7. Please see: https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Data Flow documentation is reviewed at least annually and updated as needed.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Oracle's Information Systems Asset Inventory Policy requires that an accurate and current inventory (including data owners and data stewards) be maintained for all information systems holding critical and highly critical information assets in Oracle Corporate and cloud infrastructures. Oracle Retail Cloud Services follow Oracle's Information Systems Asset Inventory Policy that requires Ownership and stewardship of all relevant personal and sensitive data is documented. The customer is the controller of their data.
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Oracle Retail Cloud Services follow Oracle's Information Systems Asset Inventory Policy that requires Ownership and stewardship of all relevant personal and sensitive data to be documented. The customer is the controller of their data. Oracle is not the controller of the data Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html https://www.oracle.com/ie/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Systems, products, and business practices are based on security principles by design and per international security standards and best practices. Oracle's security policies and practices cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27001:2022

		(formerly known as ISO/IEC 17799:2005) and ISO/IEC 27002:2022 standards. Oracle Retail Cloud Services are delivered in accordance with Oracle corporate policy and independent PCI DSS v4.0 validation.
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Systems, products, and business practices are based on privacy principles by design and per industry best practices. Oracle's privacy policies and practices cover the management of privacy for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with ISO 27018 and SSAE18 SOC1 / SOC2.
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html Privacy settings for Oracle Retail Cloud Services are controlled by the customer.
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations, and industry best practices?	Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html Oracle Legal teams perform DPIAs. Oracle Retail Cloud Services performs impact assessments for all new products and feature enhancements being brought to market.
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Oracle Retail Cloud Services has processes, procedures, and technical measures in place to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations). See the following links for additional information: https://www.oracle.com/ie/corporate/contracts/cloud-services/contracts.html https://www.oracle.com/ie/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and	Oracle Retail Cloud Services has processes, procedures, and technical measures that are defined and implemented to enable Data Subject Rights Requests to access, modify, or delete personal data. Note: Oracle is not the controller of the data. If Oracle directly receives any requests or inquiries from Individuals, it will promptly pass on such requests

	evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	to customers without responding to the Individual. Otherwise, Oracle will advise the Individual to identify and contact the relevant controller(s). Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html https://www.oracle.com/ie/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html Oracle Retail Cloud Services have processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject) For more detail, please refer to: https://www.oracle.com/legal/privacy/ https://www.oracle.com/legal/privacy/services-privacy-policy.html
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Please see the Oracle privacy policies at https://www.oracle.com/legal/privacy/ Oracle Retail Cloud Services have processes, procedures, and technical measures in place for the transfer and sub-processing of personal data within the service supply chain. Oracle and Oracle Affiliates employees, as well as any Third-Party sub-processors that Process Personal Information, are subject to appropriate written confidentiality arrangements, including regular training on information protection, and compliance with Oracle policies concerning protection of confidential information.
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Process, procedures, and technical measures are defined, implemented, and evaluated as part of Oracle Privacy policies. Please see the following for additional information. https://www.oracle.com/legal/privacy/ Oracle Retail Cloud Services have processes, procedures, and technical measures defined and implemented to disclose details to data owners of any personal or sensitive data access by subprocessors. To the extent Oracle engages Oracle affiliates and third-party sub processors to have access to Services Personal Information to assist in the provision of Services, such sub-processors shall be subject to the same level of data protection and security as Oracle under the terms of Your order for Services. Oracle is responsible for its sub-processors' compliance with the terms of Your order for Services. Oracle maintains lists of Oracle affiliates and sub processors that may process Services Personal Information. Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html
DSP-15.1	Is authorization from data owners obtained, and the associated	Replicating or using production data in non-production environments is not performed at Oracle. Oracle will not use customer data in non-production environments or for testing purposes. Production and non-production

	risk managed, before replicating or using production data in non-production environments?	environments are logically and physically segregated. Additionally, procedures are in place to ensure production data is not used in non-production environments.
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Oracle Retail Cloud Services have data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations. Oracle Retail Cloud Services data retention is 36 months unless otherwise determined by applicable fiscal law requirements. Note: Oracle is not the controller of the data. The customer remains solely responsible for data retention.
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Oracle Retail Cloud Services have processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle. Note: Oracle is not the controller of the data. The customer remains solely responsible for their data.
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Oracle customers are responsible for the proper handling of any data they choose to collect, store, or process, and to ensure that handling complies with all applicable law and regulation. Oracle makes available Data privacy and Data processing agreements for CSC review; these can be found at https://www.oracle.com/contracts/cloud-services/ Customers typically have direct access to their data stored in their services environments. Oracle therefore believes that customers are generally in a better position to identify and access their own data in response to a legal access request. However, in the event Oracle does receive a disclosure request directly from a law enforcement or government authority, the Oracle Data Processing Agreement (Section 10) and Oracle's BCR-p (Section 3.4) provide for the following safeguards: 1. Oracle will assess on a case-by-case basis whether a disclosure request would be binding on Oracle and valid under applicable law. 2. Oracle will challenge any access request that is not binding and valid under applicable law. Some statutes, such as the U.S. CLOUD Act, provide for multiple avenues for service providers to challenge access requests. 3. Oracle will promptly notify the customer, as well as the customer's and Oracle's data protection authorities, without otherwise responding to the access request (subject to 5. below). 4. Oracle will request the authority that made the request for an extension to enable the customer's and Oracle's data protection authorities to take a view on the validity of the request. 5. If Oracle would be expressly prohibited under applicable law to inform the customer, such as to preserve the confidentiality of a criminal investigation, Oracle will request the authority that made the request to waive this non-disclosure prohibition. Oracle will also document that it has asked for such a waiver.

		6. In addition to publicly available transparency reports (see below), Oracle will also provide annual transparency reports to its data protection authority about the number and types of requests it has received. Please also refer to: Oracle Cloud Service Agreement - https://www.oracle.com/corporate/contracts/cloudservices/contracts.html#ct07tabcontent1 Please review the Oracle Data Processing Agreement - https://www.oracle.com/corporate/contracts/cloudservices/contracts.html#ct07tabcontent1 SaaS Services are delivered in accordance with the oracle services privacy policy: https://www.oracle.com/au/legal/privacy/services-privacy-policy.html
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Oracle Retail Cloud Services will promptly inform the customer of requests to provide access to Personal Information unless otherwise required by law, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation? Please see: https://www.oracle.com/ie/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Oracle Retail Cloud Services has processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locations where data is processed or backed up.

Control Domain: Governance, Risk & Compliance

Question ID	Consensus Assessment Question	Oracle Response

GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Global Information Security (GIS) defines policies for the Line of Business 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html
		Oracle Retail Cloud Services have information governance program policies and procedures sponsored by Oracle Global Information Security (GIS) established, documented, approved, communicated, applied, evaluated, and maintained. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address governance, risk, and compliance) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services standards and procedures (including those that address governance, risk, and compliance) are reviewed annually and updated as needed.
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	The Chief Corporate Architect is one of the directors of the Oracle Security Oversight Committee (OSOC) and manages the Corporate Security departments which guide security controls at Oracle. These departments drive the corporate security programs, define corporate security policies, and provide security assurance oversight of Lines of Business. Corporate Security Architecture manages a cross-organization working group focused on security architecture of corporate and cloud systems. Participation includes members from cloud service development, operations, and governance teams. Each Line of Business is responsible implementing associated procedures. Oracle Privacy & Security Legal manages the cross-organization oversight of privacy risks. For more information, see https://www.oracle.com/legal/privacy/
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Oracle Corporate Security policies are reviewed annually and updated as needed.
		Oracle Retail Cloud Services standards and procedures (including those that address cloud security and privacy risks) are reviewed annually and updated as needed.

GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Global Information Security (GIS) manages a security exception program which oversees LoB exception and exception management activity. Oracle Retail Cloud Services follows Oracle Corporate Policies including an approved exception process when deviations from policy occur.
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Oracle's Information Security Program has been developed and implemented. Oracle's security policies cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, including employees and contractors. These policies are aligned with the ISO/IEC 27001:2013 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27002:2022 standards. Some Oracle products and services are certified per specific International, industry and government standards such as ISO/IEC 27001:2013 AICPA SSAE Number 18 (SOC), Payment Card Industry Data Security Standards (PCI DSS) and other standards. Oracle Retail Cloud Services maintains PCI DSS validation and issues SOC 1 and SOC 2 reports annually. These are available for customer review upon request.
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	See GRC-05.1
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Oracle Retail Cloud Service must comply with relevant standards, regulations, legal/contractual, and statutory requirements applicable to Oracle as identified and documented by Oracle Legal and Corporate Security. Oracle's Business Assessment & Audit (BA&A) is an independent global audit organization which performs global processes and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards and select laws and regulations. See A&A-01.1 The customer remains solely responsible for its regulatory compliance in its use of any Oracle Cloud services. The customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and	Oracle Retail has several Special Interest Groups (SIGs) that focus on different areas, including loss prevention and brand compliance.

	other relevant entities?	Oracle Retail Customer Community. See: https://community.oracle.com/industries/RGBU/

Control Domain: Human Resource Security

Question ID	Consensus Assessment Question	Oracle Response
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	In accordance with Oracle policy, background checks are required for individuals being considered for employment. For more information, see https://www.oracle.com/corporate/careers/background-check.html The Oracle Recruiting Privacy Policy describes the privacy and security practices of Oracle when collecting, using and handling (processing) personal information about job applicants in connection with our online and offline recruitment activities. It also explains the choices candidates have in relation to these processing activities.
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	In accordance with Oracle policy, background checks are required for individuals being considered for employment. For background check information organized by local law and regulation, see https://www.oracle.com/corporate/careers/background-check.html
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Oracle Human Resources policies (including polices that address candidate and employee background checks) are reviewed annually and updated as needed. Oracle Retail Cloud Services adhere to Oracle Recruiting Privacy and the privacy and security practices of Oracle Global Information Security (GIS) defined policies for the Line of Business management of information security across Oracle.
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of	Oracle's Acceptable Use Policy (AUP) guides the use of organizationally owned or managed assets. Employees must sign a confidentiality agreement 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

	organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
		Oracle Retail Cloud Services have policies and procedures for defining allowances and conditions for the acceptable use of organizationally owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained. Oracle Retail Cloud Services relies on Oracle Corporate Security and Corporate HR policies (including policies that address Acceptable Use). see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Oracle Corporate Security policies (including the Acceptable Use Policy) are reviewed annually and updated as needed. Oracle has formal "acceptable use of asset" policy 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Each employee is required to complete information-protection awareness training upon hiring and every two years. The course instructs employees on their obligations under Oracle policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs and are required by company policy. For more information see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Oracle Retail Cloud Services relies on Oracle Corporate Security and Corporate HR policies on policies and procedures requiring unattended workspaces to conceal confidential data reviewed. Please see: https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved,	Oracle Global Information Security (GIS) defines policies for the Line of Business management of information security across Oracle. For more information see https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html Data centers hosting cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats,

	communicated, applied, evaluated, and maintained?	power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
		Oracle Retail Cloud Services rely on Oracle Global Physical Security for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Oracle Corporate Security policies (including polices intended to protect information accessed, processed, or stored at remote sites and locations) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services rely on Oracle Global Physical Security for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. The policies and procedures are reviewed and updated at least annually.
HRS-05.1	Are return procedures of organizationally owned assets by terminated employees established and documented?	In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Oracle regularly reviews network and operating system accounts regarding 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Please see HRS-02.1
HRS-08.1	Are provisions and/or terms for adherence to established information	Please see HRS-02.1

	governance and security policies included within employment agreements?	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Oracle's information asset classification determines corporate data-security requirements for Oracle managed systems. Oracle policies and standards provide global guidance for appropriate controls designed to protect the confidentiality, integrity, and availability of corporate data in accordance with the data classification. Required mechanisms are designed to be commensurate with the nature of the corporate data being protected. For example, security requirements are greater for data that is sensitive or valuable, such as cloud systems, source code and employment records. 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 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/
		Oracle Retail Cloud Services documents the employee roles and responsibilities relating to information assets and security. Customers are responsible for the management of identity and access to their data in their use of Oracle Retail Cloud Services. Oracle Retail Cloud Services have processes, procedures, and technical measures in place for the secure management of users and roles. These are documented here: https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/books.html https://www.oracle.com/corporate/security-practices/corporate/access-control.html
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Please see HRS-02.1

HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated, and maintained?	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. Each employee is required to complete information-protection awareness training upon hiring and every two years. The course instructs employees on their obligations under Oracle policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs and are required by company policy. For more information, see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
HRS-11.2	Are regular security awareness training updates provided?	Please see HRS-11.1
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Please see HRS-11.1
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Please see HRS-11.1
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	See HRS-11.1
Control Domain: Identity & Access Management		

Question ID	Consensus Assessment Question	Oracle Response
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		Oracle Retail Cloud Services publish its identity and access procedures for customers at the following location: https://docs.oracle.com/en/industries/retail/index.html
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including policies applicable to identity and access management) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services align with the Oracle corporate standards for identity and access management policies applicable to identity and access management. They are reviewed annually and updated as needed.
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Oracle has 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. 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
		Oracle Retail Cloud Services follows Oracle Corporate strong password policies and procedures. These policies are documented and approved. see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including password complexity and protection requirements) are reviewed annually and updated as needed.
		Customers are responsible for the management of identity and access to their data in their use of Oracle Retail Cloud Services.
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	System identity information and levels of access is managed, stored, and reviewed. Logical access controls for applications and systems must provide identification, authentication, authorization, accountability, and auditing functionality. Oracle regularly reviews network and operating system accounts regarding the appropriate employee access levels. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		Oracle Retail Cloud Services procedures follows Oracle Corporate password policies.
	Is the separation of duties principle	Separation of duties principle is employed when implementing information system access. The Oracle Logical Access Controls Policy and standard

IAM-04.1	employed when implementing information system access?	describes logical access control requirements for Oracle systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined 'users' with access to Oracle systems, which are not Internet facing publicly accessible systems. Oracle SaaS security has developed its own standard that further extends/refines the one coming from Oracle corporate security, for the SaaS LoB. 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?
		Customers are responsible for ensuring the least privilege in their use of Oracle cloud services. Oracle Retail Cloud Services supports Role Based Access adhering to the principle of least privilege and segregation of duty with role management controlled and administered by the customer. This is documented. See https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/books.html
IAM-05.1	Is the least privilege principle employed when implementing information system access?	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 required to be 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, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		Customers are responsible for ensuring least privilege in their use of Oracle cloud services. Customers are responsible for user access provisioning and role assignment when connecting to Oracle Retail Cloud Services. Oracle Retail Cloud Services support Role Based Access in adherence to the principle of least privilege and segregation of duty within the integrated role management included with the product. Retail Cloud Service publishes user access and OIAM provisioning is documented here: https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/books.html
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates	A user access provisioning process is defined and implemented. 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

	data and assets access changes?	Customers are responsible for the user access provisioning in their use of Oracle Retail Cloud services. Oracle Retail Cloud Service publishes user access and OIAM provisioning is documented here: https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/books.html
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Oracle Lines of Business are required to regularly review 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html Customers are responsible for user access de-provisioning in their use of Oracle cloud services.
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Customers are responsible for review and revalidation of user access de-provisioning in their use of Oracle cloud services. Oracle reviews and revalidates Oracle administrative user access for least privilege and separation of duties on a quarterly cadence. Oracle Retail Cloud Services service employee access management covers on-boarding, internal/external transitions, and terminations. All terminations are processed automatically through the Oracle Human Resources Management System (HRMS). After a termination is processed, automated notifications are issued for terminations (regardless of type) based on the effective date of the termination.
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Oracle Retail Cloud Services adheres to the documented Oracle Network Security Standard that defines requirements and processes that include segregation of privileged access.
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and	Oracle Retail Cloud Services access processes are defined and implemented. Privileged Access roles and rights have processes to ensure they are reviewed on a quarterly basis. Privileged Account passwords expire on a shortened cycle. For more information see:

	rights are granted for a limited period?	Oracle Retail Cloud Services publishes user access and OIAM provisioning is documented here: https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/books.html
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged 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 publicly accessible, internet-facing Oracle systems or end users. 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. All network administration accounts, deployed in an Oracle managed network, must be provisioned, and managed by a corporate sanctioned access governance system.
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented, and evaluated?	Customers are responsible for review and revalidation of user access de-provisioning in their use of Oracle cloud services. Oracle Retail Cloud Services document their customer Identity and access for privileged administrative accounts. Oracle Retail Cloud Services publishes user access and OIAM provisioning is documented here: https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/books.html
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Oracle Retail Cloud Services have logging processes that are in place and are reviewed by external third-party auditors for our continued compliance with other compliance frameworks (i.e., SOC1, SOC2, PCI-DSS and ISO27001.) Logs are immutable where technically possible, otherwise compensating controls are in place to ensure a secure logging infrastructure.
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	See IAM-12.1
IAM-13.1	Are processes, procedures, and	Oracle Retail Cloud Services have the processes, procedures, and technical measures that ensure users are identifiable through unique identification (or

	technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	can associate individuals with user identification usage) are defined, implemented, and evaluated. Each user is assigned a unique identifier/account through Oracle Identity and Access management (OIAM). Note: Customers are responsible for the management of identity and access to their data in their use of Oracle Retail Cloud Services.
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Customers are responsible for the management of identity and access to their data in their use of Oracle Retail Cloud Services. Each user is assigned a unique identifier/account through Oracle Identity Manager (OIM) IAM. For Oracle Retail Cloud Services, the processes, procedures, and technical measures that ensure users are identifiable through OIM unique identification (or can associate individuals with user identification usage) are defined, implemented, and evaluated.
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Oracle Retail Cloud Services uses external and internal certificate authorities for certification generation. For customer facing URLs, Oracle uses external certificate authority vendors. For internal application communication, Oracle uses an external certificate authority.
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Customers are responsible for the management of identity and access to their data in their use of Oracle Retail Cloud Services. OIM Processes, procedures, and technical measures are in place for the secure management of passwords. These are documented here: https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/books.html https://www.oracle.com/corporate/security-practices/corporate/access-control.html
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Customers are responsible for the management of identity and access to their data in their use of Oracle Retail Cloud Services. OIM Processes, procedures, and technical measures are in place for the secure management of passwords. These are documented here: https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/books.html Oracle's Access Control security practices define these measures. For administration of network security and network-management devices, Oracle Retail Cloud Service requires Oracle personnel to use secure protocols with authentication, authorization, and strong encryption and are approved via the Corporate Security Solution Assurance Process (CSSAP).

		See: https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html

Control Domain: Interoperability & Portability

Question ID	Consensus Assessment Question	Oracle Response
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	The Oracle Retail Reference Model is a collection of detailed implementation information for retailers and partners, including business process models, technical models, APIs and a retail glossary. See: https://www.oracle.com/retail/products/reference-model/
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Oracle Retail Cloud Services have policies and procedures in place for information processing interoperability. The Oracle Retail Reference Model is a collection of detailed implementation information for retailers and partners, including business process models, technical models, APIs and a retail glossary. See: https://www.oracle.com/retail/products/reference-model/
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Oracle Retail Cloud Services are deployed only on Oracle Cloud Infrastructure. Oracle Retail Cloud Service customers wishing to import/export data must follow the published Oracle Retail Cloud Services specific documentation. See: https://docs.oracle.com/en/industries/retail/index.html
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for	Oracle Retail Cloud Services are deployed in accordance with Oracle Corporate Security policy, Oracle corporate policies are published online at: https://www.oracle.com/corporate/security-practices/ The Oracle Retail Reference Model is a collection of detailed implementation information for retailers and partners, including business process models, technical models, APIs and a retail glossary.

	information/data exchange, usage, portability, integrity, and persistence?	See: https://www.oracle.com/retail/products/reference-model/
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Oracle Retail Cloud Service customers wishing to import/export data must follow the published Oracle Retail Cloud Services specific documentation. See: https://docs.oracle.com/en/industries/retail/index.html Oracle Retail Cloud Services documentation (including interoperability and portability policies) is reviewed annually and updated as needed.
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Some Oracle Retail Cloud Services support programmatic interfaces (APIs). This is specific for each application. See the Applications Documentation available here: https://docs.oracle.com/en/industries/retail/index.html The Oracle Retail Reference Model contains detailed implementation information for retailers and partners, including business process models, technical models, APIs and a retail glossary. See: https://www.oracle.com/retail/products/reference-model/
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	All data in transit for Oracle Retail Cloud Services including data import or export is encrypted in accordance with the Oracle Hosting and Delivery Polices: https://www.oracle.com/contracts/cloud-services/
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Oracles Cloud Hosting and Delivery policies include provisions for CSC data access upon contract termination. For a period of 60 days upon termination of the Oracle Cloud Services, Oracle will make available, via secure protocols and in a structured, machine-readable format, Customer Content residing in the production Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by Customer. Any terms and conditions related to Oracle's performance of the applicable services shall be specified in the customer order for services documentation. Please refer to: https://www.oracle.com/contracts/cloud-services/

Control Domain: Infrastructure & Virtualization Services

Question ID	Consensus Assessment Question	Oracle Response

IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle Retail Cloud Services are deployed only on the Oracle Cloud infrastructure (OCI) which follows the Oracle Corporate Security Policies. Infrastructure and virtualization security policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained. See https://www.oracle.com/corporate/security-practices/corporate/
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Oracle Retail Cloud Services are deployed only on the Oracle Cloud infrastructure (OCI) which follows the Oracle Corporate Security Policies. Infrastructure and virtualization security policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained and reviewed and updated at least annually. See https://www.oracle.com/corporate/security-practices/corporate/
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Oracle Retail Cloud Services are deployed with Oracle managed capacity management and monitoring to help ensure service availability uptime and performance is in accordance with its published guidelines. Oracle Retail Cloud Services collects and monitors capacity and utilization data. This data is used to plan for adequate capacity to meet current, projected, and anticipated needs and customer service level agreements.
IVS-03.1	Are communications between environments monitored?	Oracle Retail Cloud Services communications between environments is monitored. Oracle Retail Cloud Services are deployed only on the Oracle Cloud infrastructure (OCI) that provides continuous surveillance for intercepting and responding to security events as they are identified. Alerts are forwarded to Oracle's security personnel for review and response to potential threats For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html.
IVS-03.2	Are communications between environments encrypted?	Oracle has corporate policies and standards that define the approved cryptographic algorithms and protocols. For all Retail Applications connections to the customer administration console, current APIs or host region must be made over an encrypted protocol using HTTPS and TLS 1.2 or above. Encryption is employed to protect data and virtual machine images during transport across public networks.
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as	Communications to and from the Oracle corporate network must pass through network-security devices at the network boundary. Access to the Oracle corporate network by third parties is subject to prior approval. Remote connections to the Oracle corporate network must exclusively use approved virtual private network (VPN) solutions. To learn more about Oracle's network management practices, please see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html

	justified by the business?	As defined the Oracle Network Security Policy, Oracle Retail Cloud Services restricts communication between environments to only authenticated and authorized connections.
IVS-03.4	Are network configurations reviewed at least annually?	Oracle Retail Cloud Services network configurations follow the defined review process required by Corporate Security Solution Assurance Process (CSSAP) developed by Oracle Corporate Security Architecture. This process ensures justification and approval of the new configuration has occurred. For more information see: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Oracle Retail Cloud Services network configurations follow the defined review process required by Corporate Security Solution Assurance Process (CSSAP) developed by Oracle Corporate Security Architecture. This process ensures justification and approval of the new configuration has occurred. For more information see: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Oracle Retail Cloud Services employs standardized system hardening practices across Oracle Retail Cloud Services instances. This includes alignment monitoring with base images and/or baselines, restricting protocol access, removing, or disabling unnecessary software and services, removing unnecessary user accounts patch management and logging.
IVS-05.1	Are production and non-production environments separated?	Oracle Retail Cloud Services production and non-production platforms are logically separated.
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Oracle Retail Cloud Services are designed, developed and deployed on the Oracle Cloud infrastructure (OCI). Oracle Retail Cloud Services deployments are logically separated and secured so that tenants have a restricted view of their data only. Customers are responsible for the management of identity and access to their data in their use of Oracle Retail Cloud Services. See: https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/books.html
IVS-07.1	Are secure and encrypted communication channels including	Your access to Oracle Retail Cloud Services is through a secure communication protocol provided by Oracle. Staging networks are segregated from production-level networks and utilized when migrating production data to virtual servers. Physical servers, applications, and virtual

	only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	machines are not moved. New environments are provisioned using a hardened master image with customer data migrated once the provisioning process is complete. Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Customer configuration information (e.g., connection strings, application settings) supplied through the management portal is protected while in transit and at rest.
IVS-08.1	Are high-risk environments identified and documented?	Oracle's 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. In addition, Oracle's Information Protection Policy requires all assets be classified based on their risk level.
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Processes, procedures, and defense-in-depth techniques are defined and implemented. Oracle Retail SaaS Application's defense-in-depth security framework helps detect and protect from network-based attacks. Specifically, our intrusion-detection systems within the Oracle Cloud Infrastructure 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 Cloud Infrastructure. Events are analyzed using signature detection, which involves 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 security personnel for review and response to potential threats. For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html.

Control Domain: Logging & Monitoring

Question ID	Consensus Assessment Question	Oracle Response
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Logging and monitoring policies are established, documented, approved, communicated, evaluated, and maintained by Oracle Corporate Security. Oracle Lines of Business (LoBs) are required to capture and store logs for 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html
		Oracle Retail Cloud Services are required to capture and store logs for certain security-related activities on operating systems, applications, databases, and network devices to support Oracle Logging and Monitoring polices.

		For more information, see the 'Monitoring' section of the Oracle Cloud Hosting and Delivery Policies document: https://www.oracle.com/assets/ocloud-hosting-delivery- policies-3089853.pdf
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address logging and monitoring) are reviewed annually and updated as needed. Oracle Retail Cloud Services has a defined GBU Security Logging Standard. This standard supports the Oracle Logging and Log Analysis Policy.
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Processes, procedures, and technical measures are in place to ensure audit log security and retention. Oracle centrally logs certain security-related activities, such as events and activities from 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. Log files are protected by strong cryptography, multi-factor authentication, and secure architecture. Oracle adheres to least privilege practices, and access to audit logs is monitored. The information management and records retention policy outline the required retention of audit logs, security events, and any protentional investigative reports. The retention of these records also adheres to any applicable government and compliance programs. Oracle Retail Cloud Services has a defined GBU Security Logging Standard. This standard supports the Oracle Logging and Log Analysis Policy. The following are defined in the standard: 1. Information included in the log collection record 2. Events to be logged 3. Log Storage 4. Retention period and classification 5. Frequency of Analysis of Logs
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	All Security related events (system events, firewall logs, network flows, etc.) from Oracle Retail Cloud Services and its underlying infrastructure are logged into a Security Information and Event Management (SIEM) solution to correlate information and alert on any potential security event. Oracle security personnel monitor these events 24x7x365 and have defined processes to enable the incident response process.
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their	All Security related events (system events, firewall logs, network flows, etc.) from Oracle Retail Cloud Services and its underlying infrastructure are logged into a Security Information and Event Management (SIEM) solution to correlate information and alert on any potential security event. A system is defined and implemented to generate alerts and notify responsible stakeholders.

	corresponding metrics?	
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	The GBU Logging and Log Analysis Standard defines security and parameters (including retention) for Retail SaaS Application logs. These logs are restricted and provided on a need-to-know basis. Record of audit log access are maintained to provide unique access accountability.
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Oracle Corporate security personnel have engineered SIEM detections to monitor anomalous activities. Oracle has dedicated detection and response teams that focus on designing and implementing solutions to help identify Tactics, Techniques, and Procedures (TTPs) of threat actors.
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Oracle Retail Cloud Services has defined procedures and processes to ensure appropriate and timely actions are taken on detected anomalies.
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Oracle Retail Cloud Services utilizes Network Time Protocol (NTP) to synchronize systems for a common time reference across the environment.
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Oracle Retail Cloud Services follows the Oracle Cloud Services Logging and Log Analysis Standard which defines the standards for log generation, storage, retention, analysis, and log archived retention periods.
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Retail SaaS Applications logging requirements and the threat landscape are continually reviewed. Logging requirement updates are made as necessary to include changing threats. The scope is reviewed annually and updated as needed. If necessary, the scope may be reviewed more frequently.
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Oracle Retail Cloud Services logs contain information on 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.
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Where possible, log files are protected by strong cryptography in addition to other security controls. Access to these logs is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.

LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Oracle Retail Cloud Services Applications monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. There are logs generated and mechanisms in place to review/respond to activity.
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Oracle Retail Cloud Services monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. Logs are generated and mechanisms have been put in place to review activity.
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	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 keys/cards are deactivated upon termination. Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations. Oracle uses 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. https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Oracle uses a variety of software tools to monitor the availability and performance of the Oracle Cloud Services and the operation of infrastructure and network components. Processes and measures for reporting and monitoring system anomalies and failures are in place.

LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Accountable parties are immediately notified about anomalies and failures. Oracle Retail Cloud Services leverages a Security Information and Event Management (SIEM) solution to correlate information such as system events, firewall logs, WAF logs, network flows from the environment and to alert on any potential security event. Oracle security personnel monitor the SIEM 24x7x365 and have defined processes to escalate events as needed. This process includes reporting and notification requirements to system owners and Oracle leadership.

Control Domain: Security Incident Management, E-Discovery & Cloud Forensics

Question ID	**Consensus Assessment Question**	**Oracle Response**
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Policies and procedures for security incident management, e-discovery, and cloud forensics are established, documented, approved, communicated, applied, evaluated, and maintained with the oversight of Oracle Global Information Security. Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed data has been unproperly handled or accessed. Note that cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available logs and other tooling. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to security events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for security event and 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. Upon discovery of an incident, Oracle defines an incident response plan for rapid and effective incident investigation, response, and recovery. 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
		All Security related events (system events, firewall logs, network flows, etc.) from Oracle Retail Cloud Services and its underlying infrastructure are logged into a Security Information and Event Management (SIEM) solution to correlate information and alert on any potential security event. A system is defined and implemented to generate alerts and notify responsible stakeholders.
SEF-01.2	Are policies and procedures reviewed	Oracle Corporate Security policies and procedures that address security incident management, e-discovery and forensics are reviewed annually and updated as needed.

	and updated annually?	Oracle Retail Cloud Services security procedures adhere to Oracle Corporate Security policies that address timely management of security incidents and are reviewed annually and updated as needed.
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Please see SEF-01.1
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Oracle Corporate Security policies and procedures that address timely management of security incidents are reviewed annually and updated as needed. Oracle Retail Cloud Services security procedures implement procedures and standards that support Oracle Corporate Security policies that address timely management of security incidents and are reviewed annually and updated as needed.
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	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). 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 • Addressing the root cause of an incident • Escalating an incident For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Oracle Retail Cloud Services security incident response plans are tested and updated as needed. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
SEF-05.1	Are information security incident	Information security incident metrics are established and monitored in each Line of Business (LoB) with oversight by Oracle Global Information Security.

	metrics established and monitored?	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	See SEF-01.1
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	In the event that Oracle determines that a confirmed security incident involving 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 and incident history are not shared externally.
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Please see SEF-01.1 For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Oracle maintains points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

Control Domain: Supply Chain Management, Transparency & Accountability

Question ID	Consensus Assessment Question	Oracle Response
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established,	Managing security and privacy in the cloud is a shared responsibility between the customer and the service provider. The distribution of responsibilities varies based on the nature of the cloud service (IaaS, PaaS, SaaS). Oracle strongly recommends that customers determine the suitability of using cloud services considering their own legal and regulatory compliance obligations. Making this determination is solely the customer's responsibility. For information, see https://www.oracle.com/cloud/compliance/

	documented, approved, communicated, applied, evaluated, and maintained?	Oracle has policies designed to protect the safety of its supply chain, guide how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as selects third-party technology used in corporate and cloud environments. Additionally, Oracle has policies to mitigate the risks associated with the malicious alteration of products before installation by customers. Oracle suppliers are required to comply with the Supplier Information and Physical Security Standards of mandatory security controls. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ Oracle's Supplier Management Security Policy defines requirements for Lines of Business supplier management programs, to guide selection and management of suppliers each LOB utilizes.
		As part of the GIU Supplier Management program, a central repository of GIU suppliers is maintained. The suppliers are assigned a Risk Category which is used to schedule security assessments. The suppliers are assessed regularly to ensure GIU suppliers are not only in compliance with corporate policy and standards (Corporate Security, Global Information Security (GIS) Supplier Security Program as led by GIS and Privacy and Security Legal, but understand their obligations to protect Oracle information assets, including customer data and intellectual property.
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Managing security and privacy in the cloud is a shared responsibility between the customer and the service provider. Oracle strongly recommends that customers determine the suitability of using cloud services considering their own legal and regulatory compliance obligations. Making this determination is solely the customer's responsibility. For information, see https://www.oracle.com/cloud/compliance/ Oracle Retail Cloud Services implement procedures and standards that support Oracle Corporate Security policies (including policies applicable to shared security responsibility model) are reviewed annually and updated as needed. See STA-01.1
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	The Security Shared Responsibility Model (SSRM) is applied, documented, implemented, and managed through the supply chain for the Oracle Retail Cloud Services. For more information see: https://www.oracle.com/corporate/suppliers.html
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	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. Quality and reliability for Oracle Retail's Applications' hardware systems are addressed through a variety of practices, including design, development, manufacturing, and materials management processes. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/

STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	The Oracle Cloud Hosting and Delivery Policies describe the customer (tenant) security obligations. Also, the Oracle Data Processing Agreement includes the responsibilities of the data controller (tenant/customer) versus data processor (Oracle). Please see the Oracle Hosting and Delivery Policies located at https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html and the Oracle Data Processing Agreement at https://www.oracle.com/contracts/cloud-services/
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Oracle Retail Cloud Services reviews and validates SSRM Documentation annually. Please see https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	All portions of the SSRM the organization is responsible for is implemented, operated, audited, and assessed. Oracle's security policies cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27001:2013 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27002:2022 standards. Corporate Security Architecture manages a cross-organization working group focused on security architecture, with the goal of collaboratively guiding security for Oracle cloud services. Participation includes members from Oracle cloud service development, operations, and governance teams.
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	For Oracle Retail Cloud Services Applications, an inventory of all supply chain relationships is developed and maintained. Oracle maintains master service agreements with vendors for services and products. These agreements define agreed upon security, privacy, and compliance controls prior to the onset of services. These controls meet the requirements of Oracle policy. Oracle Cloud Infrastructure (OCI) currently maintains contracts with third-party vendors for co-location facilities (for certain services), transportation and storage of encrypted customer backup tapes to off-site storage facilities (for certain services) and various data center functions such as physical security guards, systems maintenance and facility building operations/ maintenance. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	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. Supply availability, continuity and resiliency in Oracle's hardware supply chain are addressed through a variety of practices, including:

		• Multi-supplier and/or multi-location sourcing strategies where possible and reasonable. • Review of supplier financial and business conditions. • Requiring suppliers to meet minimum purchase periods and provide end-of-life (EOL)/end-of-support-life (EOSL) notice. • Requesting advance notification of product changes from suppliers so that Oracle can assess and address any potential impact. • Managing inventory availability due to changes in market conditions and due to natural disasters. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Service agreements between Oracle Retail Cloud Services and Customers incorporate these provisions and/or terms, see the following Oracle documents: Hosting and Delivery Policy, Services Pillar Document, Data Processing Agreement https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html https://www.oracle.com/be/corporate/contracts/cloud-services/contracts.html https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Oracle's Supplier Security Management Policy requires Oracle Retail Cloud Services, 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 each supplier's goods or services are leveraged. Oracle Retail supplier agreements are reviewed annually.
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Oracle Retail Cloud Services have processes for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities. 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 supplier's goods or services are leveraged.
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Oracle Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/suppliers.html
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Oracle's Supplier Security Management Policy requires all lines of business to maintain a program which manages risk for their suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual supplier review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each supplier's goods or services are leveraged. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
		Oracle Retail Cloud Services Security procedures adhere to Oracle Corporate Security policies that address Supply Chain Governance are reviewed and updated as needed. see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	See STA-13.1

Control Domain: Threat & Vulnerability Management

Question ID	Consensus Assessment Question	Oracle Response

TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Oracle has formal practices designed to identify, analyze, and remediate technical security vulnerabilities that may affect our enterprise systems and Oracle Cloud environments. The Oracle IT, security and development teams monitor relevant vendor and industry bulletins, including Oracle's own security advisories, to identify and assess relevant security patches. Additionally, Oracle requires that vulnerability scanning using automated scanning systems be frequently performed against the internal and externally facing systems it manages. Oracle also requires that penetration testing activities be performed periodically in production environments. Oracle's strategic priority for the handling of discovered vulnerabilities in Oracle Cloud is to remediate these issues according to their severity and the potential impact to the Oracle Cloud Services. The Common Vulnerability Scoring System (CVSS) Base Score is one of the criteria used in assessing the relative severity of vulnerabilities. Oracle requires that identified security vulnerabilities be identified and tracked in a defect tracking system. Oracle aims to complete all cloud service remediation activities, including testing, implementation, and reboot/reprovision (if required) within planned maintenance windows. However, emergency maintenance will be performed as required to address severe security vulnerabilities, as described in the Oracle Cloud Hosting and Delivery Policies and, as applicable, associated Pillar documentation. Oracle Software Security Assurance 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. Customers and security researchers can report suspected security vulnerabilities to Oracle: How to Report Security Vulnerabilities to Oracle or by submitting a Service Request in their support system. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html and https://www.oracle.com/corporate/security-practices/assurance/vulnerability/
		Oracle Retail Cloud Services procedures adhere to Oracle Software Security Assurance Methodology (including policies and procedures related to vulnerability management) and are reviewed annually and updated as needed.
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address threat and vulnerability management) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services procedures (including policies and procedures related to vulnerability management) are reviewed annually and updated as needed.
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved,	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

	communicated, applied, evaluated, and maintained?	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
		Oracle Retail Cloud Services Security Standards (including standards that address asset management and malware protection) are reviewed annually and updated as needed.
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address asset management and malware protection) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services Security Standards (including standards that address asset management and malware protection) are reviewed annually and updated as needed.
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Oracle Retail Cloud Services processes, procedures, and technical measures are defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications. Oracle Retail Cloud Services development and release cycles have vulnerability assessment tools to identify security threats and vulnerabilities in the Oracle Retail Cloud Services and Services environments. Formal procedures are in place to assess, validate, prioritize, and remediate identified issues. Oracle Retail Cloud Application Services act on the detection or notification of a threat or risk once it has been confirmed that, both, a valid risk exists and that the recommended changes are applicable to Services environments. The severity of vulnerabilities is determined using a Common Vulnerability Scoring System (CVSS) Base Score, and remediation timelines are based upon the assigned severity and possible business impact.
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Processes, procedures, and technical measures are defined, implemented, and evaluated to update detection tools, threat signature and compromise indicators on at least a weekly basis. Antivirus updates generally occur daily. Please see TVM-01.1
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use	Oracle Retail Cloud Services processes, procedures and technical measures are defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries. During the Development cycle, development teams are required to vet and get Corporate Security permission for any third-party software that may be embedded in Oracle products.

	third-party or open-source libraries (according to the organization's vulnerability management policy)?	Oracle Software Security Assurance (OSSA) policies require that any third-party components (e.g., open-source components used in the Oracle Retail Cloud Services) be approved and appropriately assessed for security purposes. The Oracle Retail Cloud Services development has patching and release cycles that require that third-party components be evaluated or re-evaluated for any vulnerabilities found in testing or through notifications of vulnerabilities. The severity of vulnerabilities is determined using a Common Vulnerability Scoring System (CVSS) Base Score, and remediation timelines are based upon the assigned severity and possible business impact
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Oracle Retail Cloud Services processes, procedures, testing and technical measures are defined, implemented and evaluated for, periodic, independent, penetration testing by the Oracle GIU SAR Penetration Test Team. Oracle's third-party auditors have confirmed that the pen testing team and Oracle Retail Cloud Services do not share reporting lines and are independent from one another. SOC 1 and SOC 2 auditing of, and reporting on Oracle Retail Cloud Services is performed at least annually. Oracle Retail Cloud Services must demonstrate that penetration testing has been performed and issues found remediated. Oracle Retail Cloud Services issues SOC 1 and SOC 2 reports annually for all cloud services. These are available for customer review upon request.
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Oracle Retail Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) for host-based and/or Network-based Intrusion Detection Systems (IDS) to protect the environment. IDS sensors are deployed in Intrusion Detection mode to monitor suspicious network traffic. IDS alerts are routed to a centralized monitoring system that is managed by the security operations teams 24x7x365. Oracle Corporate Security and Oracle Cloud infrastructure (OCI) processes, procedures, and technical measures are in place for all Oracle Retail Cloud Service deployments for continuous vulnerability detection on managed assets. Where CSSAP or SOC audits requires it penetration testing is scheduled and performed.
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Oracle uses the Common Vulnerability Scoring System (CVSS) to report the relative severity of security vulnerabilities when it discloses them. CVSS Base Score information is provided in the risk matrices published in Critical Patch Update and Security Alert Advisories. Oracle uses Common Vulnerabilities and Exposures (CVE) numbers to identify the vulnerabilities listed in the risk matrices in Critical Patch Update and Security Alert advisories. For more information, see https://www.oracle.com/corporate/security-practices/assurance/vulnerability/
		Oracle Retail Cloud Service Applications' vulnerability remediation is prioritized using a risk-based model from an industry recognized framework. The remediation process ensures all testing or reported vulnerabilities are evaluated and patches are deployed across all Oracle Retail Cloud products based on criticality. The severity of vulnerabilities is determined using the Common Vulnerability Scoring System (CVSS) Base Score.

TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	See TVM-01.1. Oracle Retail Cloud Services have a defined process for tracking and reporting vulnerabilities and remediation activities. This process includes the identification of vulnerabilities, assessment of their impact, and the implementation of remediation measures. Oracle also has a system for notifications to stakeholders about the discovered vulnerabilities, their impact and the remediation plan. This process is designed to help ensure the security and integrity of the cloud infrastructure and to maintain the confidence of customers in the security of the Oracle Cloud platform. Where CSSAP or SOC audits requires it penetration testing is scheduled and performed.
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	See TVM-01.1 Oracle Retail Cloud Services have a defined process for tracking and reporting vulnerabilities and remediation activities. This process includes the identification of vulnerabilities, assessment of their impact, and the implementation of remediation measures. Oracle also has a system for notifications to stakeholders about the discovered vulnerabilities, their impact and the remediation plan. This process is designed to help ensure the security and integrity of the cloud infrastructure and to maintain the confidence of customers in the security of the Oracle Cloud platform.

Control Domain: Universal Endpoint Management

Question ID	**Consensus Assessment Question**	**Oracle Response**
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops, and mobile devices. 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. Oracle employees are required to comply with email instructions from Oracle Information Technology teams 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
		Oracle Retail Cloud Services relies on Oracle Corporate Security and Oracle Cloud Infrastructure (OCI) provided processes, procedures and technical measures for all cloud endpoints. Oracle Retail Cloud Services endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP). Oracle Corporate Security policies require the use of antivirus, intrustion protection and firewall solutions on endpoint devices

		such as laptops, desktops and mobile devices. Where CSSAP or SOC audits require it, pentration testing is scheduled and performed. See: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address universal endpoint management) are reviewed annually and updated as needed.
		Oracle Retail Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Retail Cloud Services endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP). Oracle Corporate Security policies require the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops, and mobile devices
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	Please see UEM-01.1. This list is approved by Oracle Corporate Architecture and maintained by Oracle Information Technology.
		Oracle Retail Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Retail Cloud Services endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP). Oracle Corporate Security policies require the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops, and mobile devices
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Please see UEM-01.1. Endpoint validation is performed by automation approved by Oracle Corporate Architecture and maintained by Oracle Information Technology.
		Oracle Retail Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Retail Cloud Services endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP). Where CSSAP or SOC audits requires it penetration testing is scheduled and performed.
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Oracle's Information Systems Asset Inventory Policy requires that Line of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware and software.
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store,	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. 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

	transmit, or process organizational data?	access the data. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
		Oracle Retail Cloud Services endpoint management processes and procedures are aligned with Oracle Corporate policy detailed above.
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Interactive-used endpoints are configured to require an automatic lock screen. Oracle computers have secure desktop management software installed that lock screens automatically after a defined period of inactivity. This includes computers used to manage Oracle Retail Cloud Services. Oracle Retail Cloud Services enforces an automatic lock screen as a default setting that cannot be changed.
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	The Oracle Information Technology 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
		Oracle Retail Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Retail Cloud Service endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP). Where CSSAP or SOC audits requires it penetration testing is scheduled and performed.
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Please see UEM-05.1.
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Antivirus software must be scheduled to perform threat definition updates and virus scans. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
UEM-10.1	Are software firewalls configured on managed endpoints?	Oracle Retail Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Corporate Security policy requires the use of antivirus, intrusion protection and firewall software on laptops and mobile devices. See:

		https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Oracle Retail Cloud Service Application's DLP solutions typically include a combination of technologies, policies, and procedures to help prevent data loss and ensure compliance with regulatory requirements. How these are deployed and configured is informed by the GIU Information and Security Risk Management Program (GIU ISRMP).
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Unless required by regional or governmental regulations, geolocation capabilities are not in place for mobile endpoints.
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Oracle Retail Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints Processes, procedures, and technical measures are defined and implemented to enable remote company data deletion on managed endpoint devices. Oracle's secure desktop, and mobile device management software have remote wipe capabilities. Where CSSAP or SOC audits requires it, penetration testing of Oracle Retail Cloud Services is scheduled and performed.
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Oracle has formal requirements for its suppliers to confirm they protect 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 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/
		Third party endpoints are not allowed in Oracle Retail Cloud Services environments.

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

CAIQ for <Product ZZZZ>