ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) v4.1 for Oracle Cloud Infrastructure (OCI)

May 2026 | Version 4.1

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 4.1 are related to specific Oracle cloud offerings as listed in the "Oracle cloud services in Scope" section below.

The Oracle Trust Center 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/trust/

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.

ABOUT ORACLE CLOUD INFRASTRUCTURE

Oracle's mission is to help customers see data in new ways, discover insights, and unlock possibilities. Oracle provides several cloud solutions tailored to customers' needs. These solutions provide the benefits of the cloud, including global, secure, and high-performance environments in which to run all your workloads. The cloud offerings discussed in this document include Oracle Cloud Infrastructure (OCI). OCI is a set of complementary cloud services that enable customers to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance computing capabilities and storage capacity in a flexible overlay virtual network that is easily accessed from an on-premises network. OCI also delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI, see docs.oracle.com/iaas/Content/home.htm.

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?	OCI operates under security policies OCI operates under security policies that are generally aligned with ISO/IEC 27002 guidance for information security controls. OCI's control environment is subject to periodic assessment and testing by independent third-party audit organizations. Depending on the scope and service, these assessments may be performed in accordance with recognized assurance standards such as SSAE 18, ISAE 3402, ISAE 3000, or other applicable auditing standards. Oracle maintains documented audit and assurance policies that are approved, communicated, and reviewed under executive oversight. Oracle's independent Business Assessment & Audit (BA&A) organization conducts reviews to evaluate risk management practices and compliance with Oracle policies and standards across the business. Identified control gaps are tracked through remediation. Detailed audit results are treated as confidential and shared with appropriate stakeholders as needed.
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually, or upon significant changes?	OCI security and compliance policies and related compliance documentation are reviewed at least annually by designated control owners and relevant stakeholders (e.g., Security, Privacy, Legal/Compliance, IT). Policies and documentation are updated as needed to reflect changes in applicable requirements, business operations, systems, risk assessments, audit findings, or security incidents. All updates are formally approved, version-controlled, and communicated to relevant personnel in a timely manner. Review and approval activities are documented and retained.
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	OCI's security program is designed to align with widely recognized standards and frameworks, including policies generally aligned with ISO/IEC 27002 (Code of Practice for information security controls). OCI's internal controls are also periodically tested by independent third-party audit organizations. As a result of these independent audits, Oracle receives and periodically updates attestation and certification reports for OCI services, including (as applicable) ISO/IEC 27001, SOC 1, SOC 2, SOC 3, HIPAA, PCI DSS, and other standards. https://www.oracle.com/uk/corporate/cloud-compliance/#attestations
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies, and in response to significant changes or emerging risks?	Oracle maintains an independent Business Assessment & Audit (BA&A) function, aligned to Institute of Internal Auditors (IIA) standards, that performs risk-based assessments of security, compliance, and operational controls. OCI Assessments are conducted on a periodic basis and may also be initiated in response to significant changes or emerging risks. Results and thematic issues are reported to appropriate governance bodies and executive leadership. Key aspects of OCI

		independent audit & assurance include: Risk-based planning and execution: Audit and assurance activities are prioritized using risk assessment inputs, with emphasis on higher-risk areas. Independent third-party assessments: OCI leverages qualified external auditors/assessors for applicable assurance reports and certifications/attestations (e.g., SOC 1/2/3, HIPPA, ISO, PCI and other frameworks as in-scope).Change- and risk-responsive coverage: Audit/assurance scope is adjusted to address significant changes (new/modified services, systems, or material control/process changes) and evolving threats. Issue and remediation management: Identified control gaps are tracked, and corrective action plans (CAPs) are owned and implemented by the responsible line of business, with follow-up/validation as appropriate. Security assurance and testing: Security controls are evaluated through a combination of control testing and security validation activities (e.g., vulnerability management, static/dynamic testing where applicable) to identify and remediate weaknesses.
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Prior to submitting an audit activity for approval, the requesting Oracle line of business (LOB) or other responsible Oracle party must confirm the applicability of all relevant standards, regulations, and legal/contractual and statutory requirements. The audit activity must not be approved until this applicability review and compliance verification are completed. Oracle Legal continuously monitors the global regulatory landscape to identify legislation applicable to Oracle, supported by regional and local Legal teams tracking jurisdiction-specific changes. Oracle Legal partners with Corporate Security and other organizations to manage Oracle's compliance with regulatory obligations across all lines of business.
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 and aligned with relevant auditing standards?	Oracle maintains a comprehensive security program that protects both our internal operations and the services we provide to customers. These policies apply to all Oracle personnel, including employees and contractors, and are aligned with internationally recognized standards such as ISO/IEC 27001:2022 and ISO/IEC 27002:2022. Oracle also operates an audit management program that supports risk analysis and security assessments, documents findings and conclusions, tracks remediation plans and timelines, and produces audit reports. In addition, select Oracle products and services may be independently certified or assessed against specific industry and government standards, including ISO/IEC 27001:2022, SOC reports (SSAE 18), PCI DSS, and other applicable frameworks, depending on the service scope.
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) or independent assessments are tracked through remediation. OCI Risk-based corrective action plans to remediate audit findings are established, documented, and communicated to stakeholders and leadership for approval before being applied and maintained by Oracle's Lines of Business.

A&A-06.2	Is the remediation status of audit findings regularly reviewed and reported to relevant stakeholders?	Risks, control gaps, and remediation actions identified through Oracle Business Assessment & Audit (BA&A) activities and/or independent assessments are communicated to OCI leadership and relevant stakeholders and are tracked through remediation to closure. Status updates are provided until findings are remediated (or otherwise formally accepted in accordance with the Risk management process).

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?	Oracle Software Security Assurance (OSSA) is Oracle's end-to-end methodology for building security into product design, development, testing, and ongoing maintenance across both on-premises software and Oracle Cloud services. OSSA aims to (1) reduce security weaknesses through secure coding standards, mandatory training, security champions, and automated testing, and (2) minimize impact through mature vulnerability disclosure and remediation, including Critical Patch Updates and Security Alerts—helping customers meet their security requirements with a cost-effective ownership experience. OCI follows the OSSA methodology. For more information, see https://www.oracle.com/corporate/security-practices/assurance/ and https://www.oracle.com/security/what-is-zero-trust/
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually, or upon any significant changes?	OCI security standards and procedures follow the Oracle Security policies and Corporate Security Practices, and are reviewed annually and updated as needed, including in response to significant changes (e.g., new or changed regulations, material changes to business operations, major incidents, emerging threats, or significant technology/architecture changes). For more see https://www.oracle.com/corporate/security-practices/corporate/
AIS-02.1	Are baseline requirements to secure applications established, documented, and maintained?	Development organizations must provide an automated capability to continuously evaluate cloud service security configurations against an approved secure configuration baseline. The capability must operate efficiently, consistently, and reliably across all applicable instances (i.e., at fleet scale) and produce auditable results. OCI employs standardized system hardening practices across OCI devices. 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. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/configuration.html
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Oracle employees formal secure coding standards which are used as a roadmap and guide developers to produce secure code. OCI's Software Development Lifecyle (SDLC) program is developed at the project inception for any new service and is maintained for existing services. The SDLC program is aligned to corporate and business requirements and are reviewed as part of the third-party assessments. All OCI services producing software as part of an OCI offering or

		supporting an OCI offering must develop and maintain their SDLC which is reviewed and updated as needed at least annually.
AIS-04.1	Is a secure SDLC process defined and implemented for application requirements analysis, planning, design, development, testing, deployment, and operation per organizationally designed security requirements?	OCI follow Oracle's formal secure coding standards. These standards serve as a roadmap and guide for developers to produce secure code. OCI maintains a Software Development Lifecycle (SDLC) program that is established at project inception for any new service and maintained for existing services. The SDLC program must be aligned with applicable corporate and business requirements and is subject to review as part of third-party assessments, as applicable. All OCI services that produce software as part of an OCI offering, or that support an OCI offering, must develop, document, and maintain an SDLC program. The SDLC program must be reviewed and updated as needed, and at least annually.
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 meeting organizational delivery goals?	OCI must follow Oracle's formal secure coding standards. These standards serve as a roadmap and guidance for developers to produce secure code. OCI's Software Development Lifecycle (SDLC) program must be established at project inception for any new service and maintained throughout the service lifecycle for existing services, including upgrades and new versions. The SDLC program must align with corporate policies/controls and applicable business requirements to support application security, and it is subject to review as part of third-party assessments, as applicable. All OCI services that produce software as part of an OCI offering, or that support an OCI offering, must document, implement, and maintain an SDLC program. The SDLC program must be reviewed and updated as needed, and at least annually.
AIS-05.2	Is testing automated when applicable and possible?	After OCI code is checked in, unit tests run automatically. The build job also runs static code analysis and automatically creates high-priority defects, which must be resolved before promotion to production.
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Changes to infrastructure configurations and services supporting the System are documented and tracked in an electronic, access-controlled ticketing system. The ticketing system enforces a defined workflow and requires completion of mandatory fields to support compliance with change management requirements. At a minimum, required fields include: - Nature of the proposed change - Impacted systems (direct and indirect) - Impact of the change - Required updates to system documentation after the change - Test plan(s) - Internal and external notification plan (if necessary) - Rollback plan - Post-implementation verification process - The workflow prevents the ticket from being moved into the scheduled or implementation phase without the required review and approval of child tickets being in the closed state. Peer Review All changes to infrastructure configurations and services supporting the System require peer review prior to implementation. Reviews are performed by a qualified

		member of the same team (or equivalent) with sufficient knowledge of the impacted service to validate technical accuracy, identify potential issues, and assess risk. Testing and Environment Separation All changes are tested prior to implementation. The testing approach is commensurate with the change and may include unit, regression, manual, and/or integration testing. Development and testing environments are segregated from production to reduce the risk of unauthorized access or unintended changes to the operational environment. Emergency Changes Emergency changes require explicit approval by a Senior Manager (or above) prior to implementation, with associated documentation captured in the ticketing system. Implementation via CI/CD and Deployment Scope Code and infrastructure changes are implemented through CI/CD tooling. Except where cross-domain dependencies exist (e.g., DNS updates), changes are deployed independently per region and per availability domain to reduce blast radius and support-controlled rollout.
AIS-06.2	Is the deployment and integration of application code automated where possible?	OCI Code changes are implemented through Continuous Integration/Continuous Deployment (CI/CD) tools. Except where dependencies span multiple availability domains (e.g., domain name service updates), changes are deployed independently in each region and availability domain.
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Oracle Cloud Infrastructure performs internal vulnerability scans at least weekly, which include the discovery of end-of-support systems. Identified vulnerabilities are investigated and tracked to resolution.
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	OCI has a robust patch management solution to help ensure vulnerabilities are evaluated and patches are deployed across the environment based on criticality. Vulnerability severity is assessed using Common Vulnerability Scoring System (CVSS) scoring, and remediation SLAs are defined based on assigned severity and potential business impact. Patches and updates are implemented through Continuous Integration/Continuous Deployment (CI/CD) tools; except where dependencies exist across multiple availability domains (e.g., domain name service updates), changes are deployed separately in each region and availability domain.
AIS-08.1	Are processes, procedures, and technical measures defined and implemented to secure APIs?	OCI has documented and implemented processes, procedures, and technical controls to secure APIs throughout their lifecycle (design, build, deployment, and operations). APIs are protected through strong authentication and authorization, encryption in transit, secure configuration and change control, secure development practices, vulnerability management, and continuous logging/monitoring to detect and respond to unauthorized or anomalous activity.
AIS-08.2	Are reviews and updates for any improvements conducted at least annually, or upon significant changes?	OCI performs reviews of APIs and associated security controls at least annually, and additionally upon significant changes, to identify required updates and improvement opportunities. Any resulting updates are documented, prioritized, and implemented through the established change management process.

Control Domain: Business Continuity Management and 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) establishes a business resiliency framework that enables Lines of Business (LOBs) to respond efficiently to business interruption events impacting Oracle operations. It comprises coordinated sub-programs for emergency response to unplanned and emergent events, crisis management for serious incidents, technology disaster recovery, and business continuity management. The program's goal is to minimize negative impacts to Oracle and sustain critical business processes until normal operating conditions are restored. RMRP activities are implemented and managed across local, regional, and global levels, with the RMRP program management office providing executive scorecard reporting on program activities as well as LOB planning and plan testing status. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/resilience-management/
BCR-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	The Risk Management Resiliency Program (RMRP) policy mandates an annual operational cycle for Line of Business (LOB) planning, evaluation, training, validation, and executive approvals to support critical business operations. The program defines enterprise-wide requirements and standards for all Oracle LOBs to prepare for and respond to potential business disruption events, and it specifies the functional LOB roles and responsibilities needed to create, maintain, test, and evaluate business continuity capabilities across geographies. A centralized RMRP Program Management Office (PMO) provides oversight of LOB compliance with the program and supports consistent execution and reporting across the organization. For more information, seehttps://www.oracle.com/corporate/security-practices/corporate/resilience-management/
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	The Risk Management Resiliency Program (RMRP) is aligned with International Organization for Standardization (ISO) 22301 guidance for Business Continuity Management Systems. Oracle Cloud Infrastructure (OCI) holds ISO 22301 certification, reinforcing Oracle's commitment to maintaining and continually improving business continuity capabilities.
BCR-02.2	Are risk assessments and impact analysis reviewed and updated at least annually or upon significant changes?	OCI risk assessments and business impact analyses are reviewed and updated at least annually, and additionally upon significant changes.
BCR-03.1	Are strategies being established to reduce the impact of business disruptions, and are resiliency and recovery from business disruptions being improved?	The RMRP PMO develops guidance to help LOB Risk Managers manage their LOB business continuity plans, including testing and training procedures. Under the RMRP program, all LOBs are required to identify relevant business interruption scenarios (including essential people, resources, facilities, and technology), define business continuity plans and procedures to manage and respond to those

		scenarios (including emergency contact information), and obtain executive approval of the plans from the LOB's leadership.
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	The OCI Cloud Business Continuity Plan includes a routine Business Impact Assessment (BIA) and documented resilience strategies for OCI cloud services, leveraging cloud-provider high-availability infrastructure to support operational resiliency. The plan is reviewed and approved at least annually and is updated as needed.
BCR-05.1	Is relevant documentation developed, identified, and acquired both internally and from external parties, to support business continuity and operational resilience plans?	LOBs are required to review their business continuity plans at least annually to maintain operational recovery capability and to reflect changes in the risk environment, technology, and business processes. In addition, critical LOBs must (1) conduct a Business Impact Analysis (BIA) that defines the Recovery Time Objective (RTO) and, where appropriate, the Recovery Point Objective (RPO) and identifies the business continuity contingencies strategy; (2) define business continuity plans and procedures to manage and respond effectively to disruption scenarios, including current emergency contact information; and (3) revise plans as needed based on changes to operations, business requirements, and risk conditions. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resiliencemanagement/
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	OCI's Cloud Business Continuity and Disaster Recovery (BCDR) program documentation for Business Continuity (BC) and operational resilience is available to authorized personnel and OCI customers. The OCI BCDR program is certified to ISO 22301. Additional details—including internal OCI assessments and continuity plans—are available in the SOC 2 Type II reports.
BCR-05.3	Is business continuity and operational resilience documentation reviewed at least annually or upon significant changes?	During each exercise, OCI's resilience and disaster recovery (DR) framework is reviewed and updated. High-level documentation—including the Business Impact Analysis (BIA), Resilience Plan (RP), Disaster Recovery Plan, and Test/Exercise After Action Report (AAR)—is reviewed at least annually 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?	OCI's Business Continuity and Disaster Recovery (BCDR) program follows a regimented risk-scenario testing cadence, including quarterly operational resilience tabletop exercises and an annual end-to-end quality assurance testing exercise. Additional exercises include a Global RMRP tabletop, a service-specific annual tabletop for Tier 2 services, and— for Tier 1 services—one switchover/failover exercise plus three tabletop exercises spread across the year (across quarters).
BCR-07.1	Are communication channels with all relevant stakeholders established and maintained during business continuity and resilience procedures?	OCI's resilience and disaster recovery (DR) framework includes a communication plan for each OCI line of business (LoB) to be used during a crisis.
BCR-08.1	Are backups performed periodically?	Oracle periodically performs backups of the customer's OCI production data to reduce the risk of data loss in the event of an incident. These backups include the systems, configurations, and other data necessary to support recovery and maintain operational resilience.

BCR-08.2	Is the confidentiality, integrity, and availability of the backup ensured?	To protect integrity and confidentiality, backups are encrypted both in transit and at rest. Backups are stored in the Object Storage Service (OSS), which is designed for resilience, and access is governed by Oracle Identity and Access Management (IAM) policies to help ensure confidentiality and availability.
BCR-08.3	Can backups be restored appropriately for resiliency?	OCI Disaster Recovery (DR) restoration tests are performed regularly, and operational resilience is monitored for Oracle Cloud customers. Logs of restoration tests are maintained and reviewed by the audit team to support external accreditation.
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	OCI's Disaster Recovery Plan (DRP) covers defined disaster scenarios. A communication plan is maintained and regularly updated, informed by periodic disaster recovery exercises. OCI conducts an annual review of its plans to help ensure operational recovery capabilities remain effective and reflect changes in the risk environment (natural and man-made disasters) as well as new or updated business processes.
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	OCI's Disaster Recovery Plan (DRP) and related procedures are reviewed, updated, and formally approved at least annually, and are additionally updated as needed to reflect changes in the environment or operations.
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	OCI maintains a documented Disaster Recovery (DR) plan that includes annual testing to simulate disaster scenarios modeling catastrophic events that could disrupt OCI services. The DR plan and related procedures are reviewed and updated at least annually and updated as needed.
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	The Risk Management and Resiliency Program (RMRP) is implemented through a Local Crisis Management Team (LCMT), led by a Crisis Commander and composed of representatives from each line of business (LOB) at the impacted location. The LCMT gathers and shares information during a local crisis, executes the local Emergency Response Action Plan to help ensure personnel safety, and activates local business resiliency plans to sustain critical business functions. The Crisis Commander consolidates updates and escalates issues to the Regional Crisis Management Team as needed.
BCR-11.1	Are business-critical equipment supplemented with both locally redundant and geographically dispersed equipment located at a reasonable minimum distance, in accordance with applicable industry standards?	OCI's regional and availability architecture key concepts: Region: - A geographically localized area hosting OCI resources. - Can contain one or more Availability Domains (ADs). - Regions are independent of each other (for isolation and disaster recovery). Availability Domain (AD): - One or more data centers within a region. - All ADs inside a region are connected by a low-latency, high-bandwidth network. Fault Domain: - Subdivision within an AD, consisting of a group of physical hardware. - There are three Fault Domains per AD. - Designed for anti-affinity: spreading resources across fault domains reduces risk from hardware failures or maintenance. Power Supply Redundancy: - Each fault domain has independent, redundant power supplies for improved isolation.

		Network: - Inter-AD connectivity is high-speed and low-latency for high-availability and replication scenarios. Dedicated Region: - A dedicated version of a public region, assigned to a single customer for maximum isolation and control. Oracle maintains a redundant network infrastructure, including DNS servers to route between primary and secondary sites, network devices, and load balancers.

Control Domain: Change Control and Configuration Management

Question ID	Consensus Assessment Question	Oracle Response
CCC-01.1	Are policies and procedures for managing the risks associated with applying changes to assets owned, controlled, or used by the organization established, documented, approved, communicated, applied, evaluated, and maintained?	OCI maintains an Information Security Standard that supplements the Information Security Risk Management Policy and aligns with the Security Organization Policy. Approval and governance of OCI risk management practices and procedures are supported by the Cloud Change Management Standard and related guidelines, which define established Change Management (CM) processes. These processes incorporate change management controls and industry best practices for OCI services.
CCC-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	OCI reviews internal controls and applicable Cloud Compliance Standards—identified to meet the control framework requirements and relevant standards, as well as regulatory, legal, and statutory obligations—at least annually and whenever significant changes occur.
CCC-02.1	Is a defined quality change control, approval and testing process, incorporating baselines, testing, and release standards, established, maintained and implemented?	OCI makes changes to cloud hardware infrastructure, operating software, product software, and supporting application software provided as part of Oracle Cloud Services to maintain operational stability, availability, security, performance, and service currency. OCI follows formal change management procedures to review, test, and approve changes before implementing them in the service. These procedures cover system and service maintenance activities, upgrades and updates, and customer-specific changes, and are designed to minimize service interruption during change implementation
CCC-03.1	Is a change management procedure implemented to manage the risks associated with applying changes to assets, owned, controlled or used by the organization?	OCI Operations' change management process includes a documented risk assessment for internal and external assets, along with a risk plan managed by the change owner to address and mitigate risks throughout the change request lifecycle. Oracle makes changes to cloud hardware infrastructure, operating software, product software, and supporting application software provided as part of Oracle Cloud Services to maintain operational stability, availability, security, performance, and service currency. Oracle follows formal change management procedures to review, test, and approve changes prior to implementation, covering maintenance activities, upgrades and updates, and customer-specific changes, and is designed to minimize service interruption during change implementation.
CCC-04.1	Is a procedure to authorize the addition, removal, update, and management of assets owned, controlled, or	OCI security standards define restrictions for adding, removing, and updating OCI assets. All asset changes are recorded in the asset inventory, and only the relevant authorized team can update the inventory. Changes to cloud production asset

	used by the organization, implemented and enforced?	inventory require owner approval prior to execution and are logged through the change management process. Technical restrictions and safeguards are implemented where needed.
CCC-05.1	Are provisions to limit changes directly impacting service customer-owned environments (tenants) to explicitly authorized requests included within service level agreements?	OCI updates, upgrades, and planned maintenance windows are communicated clearly to customers and managed through the formal OCI Change Management (CM) process, in alignment with established service level agreements (SLAs) for availability and performance. Refer to the Oracle Cloud Hosting and Delivery Pillar document for Service Level Agreements located here: https://www.oracle.com/corporate/contracts/cloud-services/
CCC-06.1	Are change management and configuration baselines established, documented and implemented for all relevant authorized changes on organizational assets?	OCI Change Management (CM) aligns with industry best practices. Baselines are established, and OCI Security reviews all relevant authorized changes, including backup plans and customer notifications, prior to implementation. Changes to infrastructure configurations and supporting services are documented in an electronic, access-controlled ticketing system, with workflows and mandatory fields to help ensure compliance with change management requirements.
CCC-06.2	Are the baselines reviewed and updated at least annually or upon significant changes?	OCI's Secure Development Baseline is reviewed and updated at least annually and whenever significant changes occur.
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	All changes to OCI infrastructure configurations and services supporting the System must undergo a peer review and appropriate testing before implementation. A knowledgeable team member, familiar with the affected service, is required to review each change for accuracy and potential issues. Testing must be conducted in accordance with the nature of the change and may include unit, regression, manual, or integration testing as appropriate. Development and testing environments must remain separate from the production environment to minimize risks of unauthorized access or unintended changes to operational systems.
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	An emergency change control procedure is established for managing urgent change requests within Oracle Cloud Infrastructure (OCI). This procedure helps ensure that emergency changes are documented, assessed for risk, and implemented in a controlled manner to maintain the security, stability, and availability of the system, while minimizing disruption to operations.
CCC-08.2	Is the procedure aligned with the requirements of GRC-04: Policy Exception Process?	Oracle Cloud Infrastructure (OCI) change management processes align with the requirements of GRC-04: Policy Exception Process. All changes are governed by procedures that help ensure any exceptions to established policies are appropriately documented, justified, and approved in accordance with GRC-04 guidelines.
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?	Processes are established to proactively roll back changes to a previously known "good state" in order to safeguard Oracle Cloud Infrastructure (OCI). Standard Operating Procedures (SOPs) define the required steps for implementation, including pre-change, peri-change, and post-change validation, as well as rollback procedures when 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, and key management requirements. Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services 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.
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually, upon significant changes?	OCI follows Oracle Security policies security (including polices that address cryptography, encryption, and key management). OCI standards and procedures that address cryptography, encryption, and key management, are reviewed annually and updated 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 Board is responsible for making technical decisions and authoring internal standards that address both government and industry requirements. Representatives from Corporate Security and relevant development organizations collaborate to establish best practices for the use and implementation of cryptography in Oracle software products and cloud services. These practices are informed by regular reviews of industry standards, current threat intelligence, and clearly defined roles and responsibilities.
CEK-03.1	Are data protection at-rest and in-transit, and where applicable in use, provided using cryptographic libraries certified to approved standards?	OCI follows Oracle's established cryptography standards. These standards define approved cryptographic and key management implementations, utilizing authorized libraries to help ensure the protection of information assets both at rest and in transit.
CEK-04.1	Are encryption algorithms following industry standards utilized for protecting data, based on the data classification and associated risks?	OCI utilizes industry-standard, high-strength encryption algorithms for protecting data at rest and in transit, tailored to data sensitivity levels. The default standard for OCI data protection is AES-256 (Advanced Encryption Standard with a 256-bit key), which is considered one of the strongest encryption algorithms available.
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Change management is mandatory for all Oracle cryptography. Oracle Global IT defines the requirements for encryption, covering cipher strengths, key management, key generation, exchange/transmission, storage, use, and replacement. This standard includes detailed requirements for:- Specified locations and technologies for storing encryption keys- Controls to help ensure the confidentiality, availability, and integrity of transmitted encryption keys, including the use of digital signatures- Changing default encryption keys- Establishing replacement schedules for various types of encryption keys. OCI security follows the approved product security OSSA standards for all security related mandatory changes to OCI internal and external sources.
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems,	OCI's Security follows Oracle Secure Software Assurance (OSSA) standards and procedures for all OCI products and services employing approved encryption keys.

	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?	All cryptographic processes—including encryption algorithm selection, cipher strengths, key generation, management, storage, transmission, use, and replacement—must comply with these standards to help ensure protection against malicious activities throughout the product and service lifecycle. Any solutions or changes related to encryption key management must receive approval through 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?	Cryptographic practices for Oracle software products and cloud services are established collaboratively by representatives from security and development organizations. These practices are informed by ongoing reviews of industry standards and current threat intelligence to help ensure effectiveness and relevance. The Oracle Cloud Infrastructure (OCI) Global Enterprise Risk team is responsible for identifying, analyzing, measuring, mitigating/responding to, and monitoring risks—specifically those associated with OCI, including visibility and remediation for all key management operations. Product security teams, along with the security operations center, are tasked with continuously monitoring encryption algorithms and key lengths, ensuring that only secure and industry-appropriate cryptographic configurations are in use.
CEK-08.1	Are service providers providing service customers with the capacity to manage their own data encryption keys?	The OCI Vault enables customers to centrally manage the encryption keys that safeguard their data as well as the secret credentials used for secure resource access. Customers may leverage the Vault service to create and administer vaults, keys, and secrets. Vaults provide secure storage for master encryption keys and secrets. Depending on the designated protection mode, keys are either stored on OCI-managed secure servers or on highly available and durable Hardware Security Modules (HSMs) compliant with Federal Information Processing Standards (FIPS) 140-2 Security Level 3 certification.
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?	OCI operates a comprehensive internal and external audit program to review key management policies and processes. OCI follows OSSA-approved standards and implements established security technologies vulnerability handling processes to help ensure the protection of encryption and key management systems. Security vulnerabilities are addressed and remediated promptly based on risk prioritization. Key management systems are subject to regular reviews and assessments by accreditation auditors and the product security team, including vulnerability scans and configuration management, all in alignment with OCI Security and Privacy standards.
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	OCI follows the OSSA standards and procedures for encryption and key management system methods. Security reviews—including vulnerability scans, penetration testing, and configuration management—are performed by product security teams. These controls and processes are audited under multiple regulatory frameworks by both internal and external auditors. Audits are conducted on a monthly, ongoing basis as part of a comprehensive annual audit program, with updates implemented as necessary to maintain alignment with security best practices.
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic	Oracle Cloud Infrastructure services utilize industry-accepted technologies and processes for cryptographic key generation and key management, in accordance with the Cloud Compliance Standard for Encryption and the Oracle Cloud Infrastructure Standard Cryptography. Oracle Software Security Assurance (OSSA)

	libraries that specify algorithm strength and random number generator specifications?	standards define requirements for the creation, use, storage, and protection of encryption keys, ensuring adherence to robust security practices throughout their lifecycle.
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	OCI offers private keys provisioned for unique purposes and managed through its Key Management Service (KMS) and Vault services, which provide high-security, FIPS 140-2 Level 3-certified hardware security modules (HSMs). Additionally, OCI Vault provides a Secrets Management service to manage sensitive values like passwords, tokens, and certificates, which are encrypted by master keys in the vault.
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Cryptographic keys are managed throughout their lifecycle—including generation, storage, distribution, use, rotation, and destruction—with processes designed to maintain the integrity and confidentiality of data. Keys are revoked and removed prior to the end of their established crypto-period if they are compromised or when an entity is no longer authorized, following defined and implemented procedures and technical controls. These measures are regularly evaluated and include considerations for applicable legal and regulatory requirements.
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 requirement provisions?	Cryptographic key expiration and revocation processes are clearly defined, implemented, and regularly evaluated. Keys are immediately revoked and replaced if a symmetric key, asymmetric private key, or the password protecting an asymmetric private key is compromised or becomes invalid. Oracle Cloud Infrastructure (OCI) follows Oracle Software Security Assurance (OSSA) standards and procedures as outlined in the OSSA Key Management standards and guidance
CEK-14.1	Are processes, procedures and technical measures to securely destroy cryptographic keys when they are no longer needed, defined, implemented, and evaluated, and include provisions for legal and regulatory requirements?	OCI has defined and implemented processes, procedures, and technical measures for cryptographic key destruction and removal of unneeded keys through an automated process. Once a key is disabled or scheduled for deletion, it is rendered unusable for cryptographic operations. Keys scheduled for deletion are permanently deleted from the Hardware Security Module (HSM) within 30 days or less.
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?	OCI follows the OSSA key management lifecycle, including a key generation process that creates keys in a pre-activated state. All key management processes, implementations, and operations are clearly defined, implemented, and utilize approved security technologies.
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?	OCI follows OSSA key management lifecycle services and automates the processes of rotating, suspending, creating, and deleting cryptographic keys. This automation supports effective monitoring, review, and approval of key transitions. All key lifecycle management events are logged, enabling comprehensive auditing and reporting on changes to the status of cryptographic keys.
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the	See CEK-13.1

	time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	
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?	OCI's Compliance standards for cryptography—including procedures addressing cryptography, encryption, and key management—support the implementation of the key management lifecycle and secure management of archived keys. Virtual Private Vault customers can back up and recover cryptographic key materials protected by Hardware Security Modules (HSM) to and from a secure repository, access to which is restricted to authorized personnel only.
CEK-19.1	Are processes, procedures, and technical measures to use compromised keys to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) defined, implemented, and evaluated to include legal and regulatory requirement provisions?	The Oracle Software Security Assurance (OSSA) standards define requirements for the management of encryption keys, including security controls for key creation, use, storage, and protection. Oracle Cloud Infrastructure (OCI) provides key management capabilities to address potential cryptographic key compromises through structured processes, technical controls, and alignment with regulatory compliance frameworks. In the event of a suspected key compromise, OCI enables customers to designate affected keys as "decryption-only," ensuring ongoing encryption operations are performed exclusively with new keys.
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 requirement provisions?	Virtual Private Vault customers may back up and recover cryptographic key material protected by Hardware Security Modules (HSMs) to support business continuity and disaster recovery. Such backups must be stored only in an approved secure repository that is restricted to explicitly authorized personnel, protected by strong authentication, encryption, and auditing. Backup and recovery operations must follow least-privilege access, segregation of duties, and documented, approved procedures, and all access and actions must be logged and monitored in accordance with applicable security and compliance requirements.
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?	Cryptographic key lifecycle management events (including creation, activation, rotation, use, suspension, revocation, expiration, archival, deletion, import/export/backup/restore, and access/permission changes) must be logged and retained in accordance with applicable legal, regulatory, and contractual requirements. Logs must be tamper-resistant, time-synchronized, and protected by least-privilege access controls, and they must be available to authorized personnel to support auditing, compliance reporting, and investigation of changes to key status.

Control Domain: Datacenter Security

Question ID	Consensus Assessment Question	Oracle Response
DCS-01.1	Are policies and procedures for physical and environmental security established, documented, approved, communicated, applied, evaluated, and maintained?	OCI maintains physical and environmental security policies and procedures that are established, documented, approved by appropriate leadership, and communicated to relevant personnel and applicable third parties. These controls are implemented and consistently applied to protect OCI facilities and infrastructure, including measures such as 24/7 monitoring, strict physical access controls, environmental safeguards (e.g., fire detection/suppression and temperature/humidity controls), and resilient power and utility design.
DCS-01.2	Are policies and procedures for physical and environmental security reviewed and updated at least annually, or upon significant changes?	OCI physical and environmental security controls are periodically evaluated through risk-based testing, reviews, and independent assessments/audits as applicable, and are maintained and updated to help ensure ongoing effectiveness and alignment with applicable legal, regulatory, contractual, and compliance requirements.
DCS-02.1	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 Sanitation and Disposal Policy defines requirements for the secure removal of information from electronic storage media (sanitization) and for the disposal of information that is no longer required, to protect against unauthorized retrieval or reconstruction of confidential data. Electronic storage media includes, but is not limited to, laptops, hard drives, storage devices, and removable media such as tape. Oracle Global Information Security (GIS) establishes and maintains corporate information security policies. These policies are reviewed and updated by GIS at least annually, and as needed to address changes in risk, technology, or applicable legal and regulatory requirements
DCS-02.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Oracle Data Destruction to render information recovery impossible even if the equipment is not physically destroyed includes Cryptographic erasure, data wiping/over writing, degaussing
DCS-02.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually or upon significant changes?	Oracle's Media Sanitization and Systems Disposal Policy defines requirements for the secure sanitization and disposal of equipment and media, including the use of approved third-party destruction vendors. Detailed operational steps and control requirements are further documented in the Third-Party Destruction Process, which defines how Oracle Cloud Infrastructure (OCI) engages third-party vendors to degauss and/or physically destroy media devices using approved equipment, techniques, and procedures, and to maintain appropriate chain-of-custody and destruction evidence. These documents are version-controlled and are reviewed and updated at planned intervals (at least annually) and upon significant changes.
DCS-03.1	Are policies and procedures for the relocation or transfer of hardware, software,	Oracle's Information Systems Inventory Policy requires Lines of Business (LoBs) to maintain accurate and comprehensive inventories of information systems,

	or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	hardware, and software assets. The policy is formally established, documented, approved, communicated, and maintained. Third-party contracts, consistent with Oracle Supplier Information Security and Physical Security standards, include audit rights to validate compliance with relocation or transfer requirements. OCI customer data is deleted in accordance with contractual terms and is not recoverable.
DCS-03.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Oracle Corporate Security policies, including those addressing the relocation or transfer of hardware, software, or data/information to any location, are reviewed annually and updated as necessary based on changes in risk, business needs, or regulatory requirements.
DCS-03.3	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, or upon significant changes?	Oracle Corporate Security policies including those governing the relocation or transfer of hardware, software, and data/information to any location are reviewed at least annually and updated as needed,
DCS-04.1	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 to protect Oracle's employees, facilities, business enterprise, and assets. For more Information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification/ Procedure reviews are performed by the LOB. OCI Cloud Security maintains a Personnel Security Standard, supported by the Oracle Physical Security Policy, which describes requirements for maintaining a safe and secure work environment.
DCS-04.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually, or upon significant changes?	Oracle Corporate Security policies and OCI standards related to safe and secure working environments are reviewed at least annually and updated as needed.
DCS-05.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	OCI Security maintains Information Protection standards and procedures governing the secure handling, transmission, and physical transport of OCI confidential information. For more information, see https://www.oracle.com/uk/corporate/security-practices/corporate/data-protection/
DCS-05.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually, or upon significant changes?	Oracle Corporate Security policies, including requirements for secure transportation of assets, are reviewed at least annually and updated as required based on risk, regulatory, or business changes.
DCS-06.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Oracle maintains a formal Information Protection Policy that defines requirements for classifying and handling public and confidential information and provides guidance to Oracle personnel and business partners on classification schemes and the minimum handling requirements for each classification level.
DCS-06.2	Are assets' classifications reviewed and updated at least annually or upon significant changes?	Oracle's formal Information Protection Policy sets forth requirements for classifying and handling public and confidential information and is reviewed at least annually and upon significant changes.

DCS-07.1	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.
DCS-07.2	Is the catalogue reviewed and updated at least annually or upon significant changes?	Each Line of Business to keep an accurate inventory of all information systems and devices that store critical or highly critical information. LoBs must review and update this inventory at least once a year, and also whenever there is a significant change (for example, new systems/devices, retirements, major configuration changes, or ownership changes).
DCS-08.1	Are physical security perimeters designed and implemented to safeguard personnel, data, and information systems?	Oracle Global Physical Security applies a risk-based approach to physical and environmental security, regularly conducting risk assessments to confirm that appropriate, effective mitigation controls are implemented and maintained. In addition, the Oracle Cloud Infrastructure Data Center Services (DCS) Program Management, Audit, Security, and Safety (PASS) team assesses data center site control environments—including physical security controls and environmental safeguards—prior to a data center hosting production traffic (go-live) and thereafter according to the schedule defined in the Data Center Assessment Program.
DCS-09.1	Is equipment identification used as a method for connection authentication?	The Oracle Cloud Network Access (OCNA) VPN used by OCI employees to connect to OCI infrastructure requires both machine certificates and additional identifiers to validate that the device is Oracle-owned and provisioned before granting access to resources. OCI infrastructure manages equipment identification in alignment with the ISO 27001 standard.
DCS-10.1	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.
DCS-10.2	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.
DCS-11.1	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.
DCS-12.1	Are datacenter personnel trained to safely manage adverse events, including but not limited to unauthorized ingress and egress attempts?	Data center staff 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-13.1	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-14.1	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?	OCI data centers use environmental control systems (e.g., building/environmental monitoring and controls) designed to continuously monitor and maintain temperature and humidity within accepted industry standards for data center operations. These systems are supported by alerting and operational response procedures and are subject to routine preventative maintenance and periodic testing/verification to help ensure continued effectiveness.
DCS-15.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	OCI data center operations (e.g., electrical power, UPS/batteries, generators, fuel systems, and related distribution equipment) are secured and access-controlled, monitored, maintained, and tested on planned intervals to support continual effectiveness and availability. Monitoring and maintenance activities follow documented operational procedures, and testing/maintenance records are subject to audit as part of OCI's assurance program.
DCS-16.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	OCI business-critical equipment is located and designed within data center environments to be segregated from, and protected against, areas with higher likelihood of environmental risk events (e.g., flooding, water ingress, fire hazards), using a combination of site selection, facility design, and physical/environmental safeguards. These controls are implemented and operated under documented facility standards and are subject to independent assurance.
DCS-17.1	Are datacenter security metrics established, monitored, and reported to secure data center assets and services?	OCI data center security metrics are defined, monitored, and reported as part of ongoing security and operations management to help protect data center assets and the services they support. This typically includes tracking items such as physical access events and exceptions, monitoring/alarm status, incident trends,

		and compliance with operational procedures, with reporting to appropriate management functions.
DCS-18.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure continuous operations?	OCI processes, procedures, and technical measures are defined, implemented, and periodically evaluated to support continuous operations and service availability. This includes documented operational runbooks and change controls, resilient architecture (e.g., redundancy/failover), monitoring and incident response, capacity and performance management, and continuity/disaster recovery planning and testing appropriate to the service.

Control Domain: Data Security and Privacy Lifecycle Management

Question ID	Consensus Assessment Question	Oracle Response
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the preparation, classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	OCI maintains an information security and privacy governance program with policies, standards, and procedures that are documented, approved, communicated, and maintained to support the preparation, classification, protection, and handling of data across its lifecycle, aligned to applicable legal/regulatory requirements and risk-based controls. These expectations are reinforced through governance processes (e.g., risk management, training/awareness, compliance oversight) and are subject to periodic review and continual improvement.
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually, or upon significant changes?	For OCI's data security and privacy policies and procedures are reviewed and updated on a periodic basis (at least annually) and also upon significant business, technology, legal/regulatory, or risk changes, consistent with a formal governance and compliance program.
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	OCI applies industry-accepted secure media sanitization and disposal methods (e.g., logical sanitization/secure erase where appropriate and/or physical destruction) for storage media, designed to help ensure data is not recoverable when media is retired, replaced, or disposed of. These activities are performed under controlled procedures and are subject to audit/assurance.
DSP-03.1	Is a data inventory created and maintained for sensitive, regulated and personal information (at a minimum)?	OCI maintains inventories of information assets/systems within its governance and compliance programs, including tracking of sensitive and regulated information relevant to operating and securing OCI.
DSP-03.2	Is the inventory reviewed and updated at least annually or upon significant changes?	OCI's inventory of relevant information assets/systems is reviewed and updated at least annually and also upon significant changes, consistent with formal security governance and change management practices.
DSP-04.1	Is data classified according to type and sensitivity levels?	OCI's data/information is classified according to type and sensitivity as part of Oracle's information security governance program, and protections are applied commensurate with classification.
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	OCI maintains service architecture/design documentation and security documentation describing data handling and transmission paths for the service.

DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, or upon significant changes?	OCI's data-flow–related architecture and security documentation is reviewed at defined intervals (at least annually) and updated upon significant changes through Oracle's governance and change management practices.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	OCI documents ownership/stewardship roles and responsibilities for personal and sensitive data relevant to operating and securing OCI as part of its security and privacy governance (e.g., accountable owners, custodians, and privacy/security roles).
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	OCI's documentation defining data ownership and stewardship roles/responsibilities (for personal and sensitive data relevant to operating OCI) is reviewed at least annually and updated as needed as part of Oracle's governance and policy lifecycle processes.
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	OCI systems, services, and operational practices are developed and operated using security-by-design principles aligned with industry best practices. This typically includes secure architecture and engineering standards, risk assessment and threat considerations, secure development lifecycle practices, vulnerability management, change control, and continuous monitoring.
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	OCI incorporates privacy-by-design principles into its products and business practices, consistent with industry best practices and applicable privacy requirements. This typically includes governance over personal data handling, risk-based privacy controls, data minimization/need-to-know access, security measures such as encryption and logging, and processes to manage privacy obligations (e.g., incident response and regulatory requirements) appropriate to the service.
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	OCI provides privacy- and security-supporting defaults and controls, but compliance with applicable privacy laws for customer data processing is a shared responsibility. Oracle operates and secures the OCI platform under audited controls, while customers must configure their services and applications (and associated privacy settings) to align with applicable laws/regulations and their intended processing.
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?	OCI maintains a privacy governance program and performs DPIA or equivalent privacy risk assessments when required by applicable law for Oracle's processing activities.
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)?	OCI is operated under a security and privacy governance program with documented and periodically evaluated controls to protect data transfers from unauthorized access and to support processing in accordance with applicable laws and contractual scope. Technical measures include encryption in transit (e.g., TLS), strong identity and access management, network segmentation/private connectivity options, and logging/auditing, along with operational procedures (e.g., change management, incident response, and risk management).

DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	OCI has governance processes and technical/operational measures to support applicable privacy requirements for Oracle's own processing (as a cloud service provider).
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)?	OCI maintains policies, procedures, and technical measures reviewed and evaluated through governance and assurance processes to support lawful and purpose-limited processing for OCI.
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)?	OCI has defined, implemented, and periodically evaluated processes, procedures, and technical measures to govern transfers and sub-processing of personal data within the service supply chain, consistent with applicable laws/regulations and Oracle's contractual commitments.
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?	OCI has defined and implemented processes and contractual controls to disclose the identity of authorized subprocessors before they process personal data, typically via the Oracle Cloud DPA and an associated subprocessor list, and to provide advance notice of updates to that list (with an objection process, as applicable). Oracle also applies security controls and oversight for subprocessor access.
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	OCI operations maintains controls to limit and govern the use of production data in non-production environments for operating/supporting OCI. Where such use is necessary, it is subject to authorization, need-to-know access controls, and risk management measures consistent with Oracle's security/privacy governance and contractual commitments.
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	OCI supports retention and deletion requirements through service capabilities and platform controls. Oracle applies governed retention and deletion practices to OCI operational data. Customers determine and configure retention, archiving, and deletion for their data and workloads in OCI.
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	OCI is operated under a security governance program with documented controls and technical safeguards designed to protect sensitive data across its lifecycle. These include access controls (least privilege), encryption in transit and at rest, network security/segmentation, logging and monitoring, vulnerability and patch management, and secure media sanitization/disposal.
DSP-18.1	Does the service provider ensure that a procedure is in place and communicated to service customers for managing and responding to requests by law enforcement authorities for the disclosure of	OCI has a documented, established procedure for handling and responding to law enforcement/government requests for disclosure of personal data, and this procedure is communicated to customers through Oracle's published legal/privacy guidance and contractual framework. Oracle evaluates such requests for legal validity and scope and responds in accordance with applicable laws and regulations.

	personal data, in accordance with applicable laws and regulations?	
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?	For Oracle (platform/service): OCI provides region-based deployment and documentation describing regions/availability domains and service architecture so customers can determine where data is stored/processed (and where service backups/replication may occur, depending on the service and configuration). Oracle also maintains internal documentation for its operation and compliance needs.

Control Domain: Governance, Risk and 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?	OCI maintains an information governance / information security governance program that is sponsored by organizational leadership and supported by documented, approved, and communicated policies, standards, and procedures. These are applied in operations, periodically reviewed (including through audits/assessments), and maintained/updated as needed as part of continual improvement.
GRC-01.2	Are the policies and procedures reviewed and updated at least annually, or upon significant changes?	OCI policies and procedures are formally reviewed and, where necessary, updated at least annually, and additionally upon significant changes (e.g., major regulatory changes, material changes to services/architecture, significant incidents, new risks, mergers/acquisitions, etc.).
GRC-02.1	Is there an established and maintained formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of risks?	OCI maintains a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for risk identification, evaluation, ownership assignment, treatment (mitigation/transfer/avoidance), and formal risk acceptance with defined approval processes. Supporting documentation is available upon request, subject to confidentiality and applicable contractual terms.
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	OCI maintains a formal governance process under which relevant OCI organizational policies and associated procedures are reviewed on a defined cadence (at least annually) and updated as needed when substantial changes occur (e.g., material service/process changes, regulatory changes, significant incidents, or organizational changes). Evidence is typically maintained via document control/versioning and governance approvals (shared under NDA/audit as applicable).

GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	OCI's governance program includes a formal, documented exception/waiver process that is used when a deviation from an established policy is required. Exceptions are expected to be reviewed and approved by appropriate authorities, documented with scope/justification, risk assessment, compensating controls, and an expiration/review date, and tracked according to established governance and audit requirements (details/evidence typically shared under NDA/audit as applicable).
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	OCI has developed and implemented an information security program that is designed to cover the control areas reflected across the CSA CCM domains (e.g., governance /risk/compliance, IAM, data security & privacy, logging/monitoring, vulnerability management, incident response, BCP/DR, physical/environmental security, and third-party/supply chain considerations). Applicable controls are implemented for the OCI cloud services, with supporting policies/standards and operational processes; detailed evidence is typically available under NDA and through audits/assessments as applicable.
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Roles and responsibilities for planning, implementing, operating, assessing, and continuously improving governance programs are defined and documented through OCI's governance and assurance processes (e.g., documented policies/standards, control ownership models, and oversight functions). Supporting evidence is typically available through internal compliance documentation and, where appropriate, under NDA/audit.
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Oracle/OCI maintains processes to identify, track, and document applicable standards, regulatory requirements, and legal/contractual/statutory obligations relevant to the organization and the cloud services, and to translate those obligations into internal policies, standards, and control requirements. Evidence is generally available through compliance/governance documentation and applicable audit reports, subject to confidentiality and contractual terms.
GRC-07.2	Are the identified requirements reviewed at least annually or upon significant changes?	OCI maintains governance processes to help ensure identified compliance obligations (standards, regulatory, legal/contractual, and statutory requirements) are reviewed at least annually and additionally when significant changes occur (e.g., new/updated laws or regulations, material service changes, major incidents, or organizational changes). Updates are tracked through established compliance and document/control management practices (details/evidence shared as appropriate under NDA/audit).
GRC-08.1	Is contact established and maintained with related special interest groups and other relevant entities?	OCI establishes and maintains contact with relevant external and internal entities (as appropriate) such as industry groups, standards bodies, security and cloud communities, and coordination/response organizations, to stay informed on emerging threats, best practices, and compliance developments.

Control Domain: Human Resources

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?	Oracle has established, documented, and maintained background verification (pre-employment screening) policies and procedures that apply to new hires and, as applicable, contingent workers (e.g., contractors) and certain third parties. These processes are approved, communicated, and operationalized through HR and third-party onboarding processes, and they are periodically evaluated/updated. The scope and checks performed vary based on role, location, legal requirements, and level of access, and are supported by controls for recordkeeping and compliance. Detailed specifics and evidence are typically provided under NDA/audit as appropriate.
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?	Oracle's background verification policies and procedures are designed to align with applicable local laws and regulations, ethical considerations, and relevant contractual constraints. Screening requirements are generally risk-based and role-based, so the level/type of verification is proportional to job responsibilities, the sensitivity/data classification and systems to be accessed, business requirements, and acceptable risk. (Specific checks vary by country/role and are typically shared only as appropriate under NDA/audit.) OCI follows Oracle's human resource policies.
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually, or upon significant changes?	Oracle's background verification policies and procedures are reviewed on a defined cadence (at least annually) and updated as needed upon significant changes (e.g., changes in applicable employment/screening laws, regulatory requirements, business scope, or risk posture). Updates are managed through established policy
HRS-02.1	Are 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 maintains acceptable use policies and supporting procedures that define allowances and conditions for the acceptable use of organization-owned or organization-managed assets (e.g., endpoints, networks, systems, and information resources). These are documented, approved, communicated to the workforce, enforced through technical/administrative controls, periodically evaluated, and maintained. Detailed artifacts are typically available under NDA/audit as appropriate. OCI employees maintain the confidentiality of customer data. All employees are responsible for understanding and following Oracle policies.
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, or upon significant changes?	Oracle maintains documented policies and procedures governing acceptable use of Oracle-owned or Oracle-managed assets supporting OCI services. These policies are reviewed at least annually and updated upon significant changes through Oracle's controlled policy governance and change management processes. Customers may reference Oracle compliance reports/attestations for independent verification where applicable
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved,	OCI follow Oracle established and documented policies and procedures that require personnel to secure unattended workspaces and protect confidential

	communicated, applied, evaluated, and maintained?	information (e.g., locking screens, securing documents/media, and preventing unauthorized viewing).
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually, or upon significant changes?	OCI maintains security policies and procedures that require unattended workspaces to prevent unauthorized viewing of confidential information (e.g., clear screen/lock workstation and secure physical documents). These policies and procedures are reviewed at least annually and updated as needed, including following significant changes (e.g., material process/technology changes, regulatory changes, or security events).
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	OCI maintains documented, management-approved information security policies and supporting procedures addressing the protection of information when accessed, processed, or stored from remote sites (e.g., remote work locations, non-Oracle facilities, or offsite environments). These requirements are communicated to personnel and implemented through administrative and technical controls (such as access controls, encryption/secure connectivity where applicable, endpoint security, and user responsibilities). The policies and procedures are periodically reviewed/evaluated and maintained to reflect changes in risk, technology, and compliance obligations.
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, or upon significant changes?	OCI maintains documented, approved policies and procedures for protecting information in remote/offsite contexts. These policies and procedures are reviewed at least annually and updated upon significant changes to help ensure continued effectiveness and alignment with security and compliance requirements."
HRS-05.1	Are return procedures of organizationally owned assets by terminated employees established and documented?	Oracle/OCI maintains documented offboarding/separation procedures that include the return of organization-owned assets by terminated employees and the coordination of asset recovery and access revocation through HR, IT, and security processes.
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all relevant personnel?	Oracle/OCI maintains documented procedures for employment status changes that define and communicate roles and responsibilities across HR, management, IT, and Security to help ensure appropriate changes to access, assets, and required approvals are completed in a timely manner.
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Employees are required to complete required employment onboarding documentation (including the applicable employment agreement and/or acknowledgment of corporate policies such as acceptable use and confidentiality obligations) before being granted access to organizational information systems, resources, and assets.
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Employees are contractually obligated—through employment agreements and/or related onboarding acknowledgments (e.g., confidentiality and acceptable use)—to comply with established information governance and security policies, as applicable.
HRS-09.1	Are employee roles and responsibilities relating to information assets' security and privacy, established, documented and communicated?	Employee roles and responsibilities related to the security and privacy of information assets are established, documented, and communicated through organizational policies/standards and role-based requirements (e.g., acceptable use, data handling/classification, privacy requirements, and security awareness

		training), with additional responsibilities defined for privileged or control-owner roles as applicable.
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?	Requirements for non-disclosure/confidentiality agreements (NDAs) that reflect the organization's data protection needs and relevant operational details are identified and documented, and they are reviewed at planned intervals and updated as needed (including when there are significant changes to legal/regulatory requirements, business operations, or risk posture).
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	A security awareness training program for all employees is established and documented, approved through organizational governance , communicated to personnel, and implemented as part of onboarding and periodic refresher training. The program is maintained and periodically evaluated (e.g., through completion tracking, assessments, and updates to reflect emerging threats and policy changes).
HRS-11.2	Are regular security awareness training updates provided?	Regular security awareness training updates are provided to employees (e.g., periodic refresher training and ongoing awareness communications) to address evolving threats, policy changes, and lessons learned.
HRS-12.1	Are employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Personnel with access to sensitive organizational information and/or personal data receive appropriate security awareness training, including mandatory baseline training and supplemental role-based training (e.g., data handling/classification and privacy requirements) commensurate with their access and job duties.
HRS-12.2	Are employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Personnel with access to sensitive organizational and/or personal data are provided with regular updates to the procedures, processes, and policies relevant to their professional function through policy communications, periodic refresher training/awareness, and role-based guidance as changes are introduced.
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?	Employees are notified of their roles and responsibilities to maintain awareness of, and comply with, established policies and procedures and applicable legal/statutory/regulatory obligations. This is typically communicated through onboarding requirements, policy acknowledgments (e.g., code of conduct/acceptable use), mandatory training and periodic refreshers, and role-based communications for employees with specific compliance obligations.

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?	OCI maintains a documented, management-approved IAM policy framework and supporting procedures that are communicated and implemented to govern identity lifecycle management and access control. These controls are operationalized, periodically evaluated (e.g., through monitoring, audits, and reviews), and maintained/updated to remain effective and aligned with security and compliance requirements.

IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually, or upon significant changes?	OCI maintains approved IAM policies and procedures. They are communicated and implemented through administrative and technical controls (e.g., account provisioning/deprovisioning, authentication requirements, authorization/least privilege, logging/monitoring, and periodic access reviews where applicable). The IAM control framework is evaluated periodically and maintained/updated to address changes in risk, technology, and compliance requirements.
IAM-02.1	Are policies and procedures for the management of authentication credentials, including passwords, established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	OCI maintains approved policies and procedures for authentication credential management (including passwords). These requirements are communicated to personnel and implemented through administrative and technical controls (e.g., credential issuance and storage requirements, password/secret standards, MFA where applicable, rotation/revocation processes, and monitoring). The credential management controls are periodically evaluated and updated to address changes in threats, technology, and compliance requirements."
IAM-02.2	Are policies and procedures reviewed and updated at least annually, or upon significant changes?	OCI Policies and procedures are reviewed at least annually and updated as needed when significant changes occur (e.g., regulatory/contractual changes, material business or technology changes, risk assessment results, audit findings, or security incidents). Reviews and updates are documented with defined ownership, version control, and required approvals.
IAM-03.1	Is the inventory of identities managed, stored, and regularly reviewed, and is their level of access monitored?	OCI maintains and reviews inventories of Oracle workforce/service identities used to operate OCI, and monitors access as part of OCI's security operations and control program. Provides tenancy capabilities (OCI IAM, federation, Audit logging) to support customers.
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	OCI implements separation of duties within OCI operations and administrative access to OCI production systems using role definition, privileged access controls, approvals, and monitoring, with periodic reviews.
IAM-05.1	Is the least privilege principle employed when implementing information system access?	OCI's least privilege is employed when implementing information system access. Access is granted based on defined roles/responsibilities and business need, limited to the minimum permissions required, and is approved, logged, and periodically reviewed. Privileged access is restricted, time-bound or tightly controlled where feasible, and monitored; access is adjusted or revoked upon role changes or termination.
IAM-06.1	Is an identity access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	OCI has a formal identity and access provisioning process is defined and implemented to authorize, record, and communicate access to data and assets. Access requests require documented business justification and appropriate approvals; provisioning and deprovisioning actions are performed by authorized personnel or approved automation; changes are recorded (e.g., tickets/workflows and audit logs) and communicated to relevant stakeholders. Access is updated promptly for role changes and revoked upon termination, with periodic reviews to validate continued need.
IAM-07.1	Is a process in place to de-provision or modify identity access in a timely manner?	OCI uses established identity lifecycle processes to promptly disable/remove or adjust Oracle workforce/service identity access to OCI production systems when roles change or employment ends, with logging and oversight.
IAM-08.1	Are reviews and revalidation of identity access for least privilege and separation of duties completed with a frequency commensurate with	Oracle performs periodic reviews of Oracle workforce/service identity access used to operate and support OCI services to validate least privilege and Separation of duties, and adjusts access based on changes and review outcomes.

	organizational risk tolerance, and at least annually or upon significant changes?	
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated?	OCI processes, procedures, and technical measures are defined and implemented to segregate privileged access roles. Privileged roles are formally identified and role-based controls are used to separate administration, security, and audit functions where feasible. Privileged access is granted only with appropriate authorization, is logged and monitored, and is periodically reviewed. The effectiveness of privileged role segregation is evaluated through governance activities such as access reviews, control testing, and internal/external audits; exceptions are documented and handled via compensating controls (e.g., enhanced monitoring and independent review).
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	OCI uses privileged access controls and operational procedures to limit duration of elevated access for Oracle personnel supporting/operating OCI, with approvals, logging, and review.
IAM-10.2	Are procedures implemented to prevent the accumulation of segregated privileged access?	See IAM-06.1
IAM-11.1	Are processes and procedures for service 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?	See IAM-06.1
IAM-12.1	Are processes, procedures, and technical measures that ensure identities' activities are identifiable through uniquely associated IDs defined, implemented, and evaluated?	OCI's processes, procedures, and technical measures are defined and implemented to help ensure individuals and system identities are uniquely identified and that their activities are attributable through uniquely associated IDs. Unique identifiers are used for user and service identities; shared/generic accounts are restricted and controlled where necessary. Authentication and authorization events and administrative actions are logged to support traceability. The effectiveness of these measures is periodically evaluated through access reviews, monitoring, and control testing/audits, with remediation tracked to closure.
IAM-13.1	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?	OCI Oracle Cloud Security Logical Access Controls Standard defines processes, procedures, and technical measures for authenticating access to Oracle Cloud systems, applications and data assets, including multi-factor authentication (MFA) for a least-privileged user and sensitive data access. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html
IAM-13.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	OCI uses certificates and/or equivalent strong cryptographic mechanisms to authenticate and secure communications for OCI service components and operation system identities, supported by lifecycle management and monitoring as part of OCI's control environment.

IAM-14.1	Are processes, procedures, and technical measures for the secure management of authentication credentials, including passwords, defined, implemented, and evaluated?	OCI processes, procedures, and technical measures are defined and implemented for the secure management of authentication credentials (including passwords). Controls include credential complexity and length requirements, secure storage, protection of secrets/keys, secure transmission, and controlled reset/recovery procedures. Credential issuance, changes, and privileged credential use are logged/monitored, and the effectiveness of credential management controls is periodically evaluated through reviews, monitoring, and audit/control testing. Credentials are rotated or revoked based on policy and upon suspected compromise.
IAM-15.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Oracle Corporate Single Sign-On (SSO) standards and technical controls define and govern the processes, procedures, and technical measures used to help ensure appropriate authentication is in place to verify users prior to granting access to OCI information assets. These controls are designed to support risk-based authentication (including MFA where applicable), least privilege, and traceable access, and are subject to periodic review/evaluation as part of Oracle's control program.

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 interfaces (e.g., APIs)?	Oracle policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained to govern communications between application interfaces (e.g., APIs). These requirements typically include secure interface design and configuration, authentication and authorization, encryption in transit (e.g., TLS), logging/monitoring, change management, and periodic review/control testing to validate effectiveness.
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Oracle policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained to govern information processing interoperability. These typically cover the use of approved standards/protocols and interfaces, secure data exchange (e.g., encryption in transit and integrity protections where applicable), authentication/authorization, configuration and change management (including interface versioning/deprecation), and logging/monitoring. Control effectiveness is periodically evaluated through reviews and assurance activities, and updates are made as needed based on risk, audits, and significant changes.
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	OCI establishes, documents, approves, communicates, applies, evaluates, and maintains policies/standards and technical controls intended to support application development portability. These controls typically include: use of industry-standard technologies and interfaces; containerization and orchestration support; Infrastructure-as-Code (IaC) and automation practices; documentation, interface versioning and deprecation practices; secure SDLC and change management; and periodic evaluation/assurance (e.g., reviews, testing, and

		audit/control assessments) to validate effectiveness and drive updates based on significant changes or identified risks.
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Oracle applies these controls to OCI service design and operations within Oracle's control environment and provides security features (e.g., IAM, encryption, logging, backup/replication options) to support customers. OCI maintains documented standards and procedures for secure information transfer, which are communicated through applicable cloud service documentation and contractual commitments (e.g., service descriptions/SLA where applicable).
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually, or upon significant changes?	OCI interoperability and portability procedures are reviewed at least annually and updated as needed upon significant changes (e.g., material technology/architecture changes, new or changed legal/regulatory/contractual requirements, risk assessment outcomes, audit findings, or security incidents). Reviews and updates are documented with defined ownership, version control, and required approvals.
IPY-02.1	Are service customers able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	OCI provides application interfaces (APIs/SDKs/CLIs) that enable customers to programmatically access and retrieve their data and service resources to support interoperability and portability, subject to service-specific capabilities and the customer's authorization/configuration. Access is controlled through OCI IAM policies and is auditable via OCI logging (e.g., Audit logs), where applicable.
IPY-03.1	Are cryptographically secure network protocols implemented for the management, import, and export of data in accordance with industry standards?	OCI cryptographically secure network protocols are implemented for management operations and for the import/export of data in accordance with industry standards. Where applicable, communications are protected using strong, standards-based cryptography (e.g., TLS/HTTPS/SSH) to provide confidentiality and integrity in transit. Protocols and cipher configurations are governed through documented standards, monitored, and periodically reviewed/updated to address emerging threats and industry guidance.
IPY-04.1	Do agreements include provisions specifying service customers' 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 service customers d. Data deletion policy	Oracle Cloud Hosting and Delivery Policies and the Oracle PaaS and IaaS Public Cloud Services Pillar document describe Oracle Cloud service objectives (including target service availability and uptime) and include provisions addressing customer access to data upon contract termination. At the end of the service period, the customer's content remains available for retrieval for the period specified in the applicable Service Specifications (or as required by law). After the retrieval period expires, remaining content is deleted or otherwise rendered unrecoverable in accordance with the Service Specifications. For information https://www.oracle.com/contracts/cloud-services/

Control Domain: Infrastructure Security

Question ID	Consensus Assessment Question	Oracle Response
I&S-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	OCI network security standards and procedures are reviewed and approved through Oracle's security governance processes and follow Oracle Security policies.
I&S-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually, or upon significant changes?	OCI Network Security Standards are established and approved through Oracle's Global Information Security governance processes, aligned with Oracle information security policies, and are reviewed at least annually and updated as needed based on significant changes (e.g., risk, technology, regulatory, or audit/incident-driven updates).
I&S-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	OCI resource availability, quality, and capacity are planned and monitored to meet required system performance and availability objectives. OCI uses capacity management and performance monitoring processes to forecast demand, track utilization, and mage scaling and resilience of the infrastructure and services. Service health and performance are monitored, and capacity-related risks are managed through operational processes (e.g., alerting, incident/problem management, and change management) to help ensure business requirements are met.
I&S-03.1	Are communications between environments, services, and applications monitored?	OCI monitors communications between environments, services, and applications at the cloud infrastructure and managed-service layers. Network/security telemetry (e.g., platform and service logs and security events) is centrally collected and monitored, and intrusion detection/monitoring is applied to relevant traffic (scope depends on the service.
I&S-03.2	Are communications between environments, services, and applications encrypted?	OCI provides capabilities and secure service endpoints that support encryption in transit (e.g., TLS/HTTPS) for OCI services and platform communications, and offers networking/security services (e.g., VPN/IPSec, FastConnect with MACsec where applicable, load balancers/TLS termination) to enable encrypted connections.
I&S-03.3	Are communications between environments, services, and applications restricted to only authenticated and authorized connections, as justified by the business?	OCI provides the mechanisms to enforce authenticated/authorized connectivity and least-privilege access (e.g., IAM, security policies, network isolation primitives, and managed service endpoints with authentication).
I&S-03.4	Are network configurations reviewed at least annually?	OCI provides network security and configuration mechanisms (e.g., VCNs, subnets, route tables, security lists/NSGs, gateways) and logging/audit capabilities that help enable review and governance .
I&S-03.5	Are network configurations supported by the documented justification of all	OCI follows the Oracle Cloud Network Security Standard and provides the network security constructs and governance tooling (e.g., VCNs, security lists/NSGs, route tables, gateways, IAM, logging/audit) that enable customers to implement least-privilege network access and support documentation and review.

	allowed services, protocols, ports, and compensating controls?	
I&S-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?	OCI hardens and maintains security baselines for the underlying OCI infrastructure, including hypervisors and the OCI control plane, in accordance with Oracle security standards and industry best practices. For Oracle-managed PaaS components, Oracle applies hardening/baselines within the managed service scope.
I&S-05.1	Are the environments separated into production and non-production environments to reduce the risk of sensitive production data being used in non-production environments?	OCI supports separation of production and non-production environments to reduce the risk of sensitive production data being used in non-production. OCI provides the isolation and segmentation capabilities needed to separate environments.
I&S-05.2	Is production data sanitized or protected before being used for any authorized non-production purpose?	OCI provides capabilities that support protecting data when moving or copying it into non-production (e.g., encryption services, access controls/IAM, logging/audit, and tooling that can be used to enforce segregation and monitor data access).
I&S-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that service customer (tenant) access is appropriately segmented, segregated, monitored, and restricted?	OCI services and supporting infrastructure are designed and operated to help ensure tenant access is appropriately segmented and segregated, and access is restricted and monitored through identity and security controls. Oracle is responsible for tenant isolation at the cloud infrastructure and control plane layers, and for providing capabilities to segment, restrict, and monitor access.
I&S-07.1	Are secure and encrypted communication channels including only up to date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	OCI uses encrypted communication channels and supports the use of up-to-date, approved protocols when migrating servers, services, applications, or data. OCI uses encrypted communication channels and supports the use of up-to-date, approved protocols when migrating servers, services, applications, or data.
I&S-08.1	Are high-risk environments identified and documented based on data sensitivity, threat exposure, and business impact?	OCI identifies and documents high-risk environments through formal risk assessments and security reviews that evaluate data sensitivity, threat exposure, and business impact, with periodic and change-driven revalidation.
I&S-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	OCI defines, implements, and evaluates processes/procedures and defense-in-depth techniques to protect against, detect, and respond in a timely manner to network-based attacks. This includes layered network security controls (e.g., segmentation, firewalling/DDoS protections, monitoring/logging, and incident response processes) that are reviewed and improved as part of ongoing security operations and risk management.

Control Domain: Logging and 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?	OCI follows Oracle Security policies (that include Logging and monitoring). 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.
LOG-01.2	Are policies and procedures reviewed and updated at least annually, or upon significant changes?	OCI logging and monitoring standards and procedures are reviewed annually and updated as needed. Reviews and updates are tracked through OCI's governance and compliance processes.
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	OCI and Oracle Cloud Security have a defined OCI logging and log analysis standard and follow Oracle logging and log analysis policy. Logs are automatically collected, and retention of customer data follows applicable government and compliance requirements. OCI implements technical and procedural controls to protect logs and periodically evaluates the effectiveness of these controls through security governance and compliance activities.
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	OCI identifies and monitors security-relevant events across the cloud platform and underlying infrastructure through centralized logging, monitoring, and security operations processes. OCI services generate and make available security-related events (e.g., API activity via OCI Audit, service/resource logs where supported, and platform monitoring/alerting capabilities) and these signals are monitored and evaluated as part of Oracle's operational security and incident response practices.
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	OCI has a defined and implemented event management capability to identify security events and generate alerts to responsible stakeholders. OCI uses a proprietary event management system and additional alarms to alert when specific events occur across OCI environments and components. Alert/alarm configuration is informed by regulatory requirements, industry standards, results of internal penetration testing, and security operations reviews/round-table discussions. Events ingested into the SIEM are prioritized to enable rapid triage based on severity and criticality, including impacted systems, applications, users, and regulatory context.
LOG-04.1	Is audit log access restricted to authorized identities, and are records of that access maintained?	OCI restricts access to audit logs and underlying logging systems to authorized personnel/identities using role-based access controls and least privilege. OCI also maintains records of administrative/user access and activity through logging and monitoring controls, and reviews access in accordance with internal security policies.
LOG-05.1	Are capabilities implemented and maintained to correlate and monitor security audit logs for the detection of suspicious or anomalous activity that deviates from typical or expected patterns?	OCI implements and maintains centralized logging and monitoring capabilities to collect, correlate, and monitor relevant security audit logs for OCI services/platform operations. OCI uses automated detection and alerting to identify suspicious or anomalous activity that deviates from expected patterns and supports investigation/response through defined operational security processes.

LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	OCI has documented processes to monitor logging/telemetry and review detected anomalies, including defined triage, escalation, investigation, and remediation workflows. Anomalies are handled in accordance with OCI's incident management and security operations procedures, with timely response expectations driven by severity and risk.
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	OCI clocks for servers supporting services, including bastion servers, are synchronized using Network Time Protocol (NTP). OCI NTP servers use Global Positioning System (GPS) as the authoritative time source to provide consistent, reliable time synchronization across relevant OCI-managed information processing systems.
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	OCI 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 and as per relevant regulatory requirements?	OCI Cloud Security logging processes and the threat landscape are continually monitored and reviewed. The logging scope is reviewed at least annually and updated as necessary to address changes in threats and applicable regulatory requirements. Where warranted, the scope may be reviewed and updated more frequently.
LOG-08.1	Are technical measures defined, implemented, and evaluated to enable service customers to detect and scrub or tokenize sensitive data from logs, in order to prevent unauthorized exposure as per applicable laws and regulations?	OCI provides logging services and analytics capabilities that help enable customers to collect, search, analyze, alert on, and operationalize log data to help detect the presence of sensitive information. However, scrubbing/redaction/tokenization of sensitive data in logs is primarily the customer's responsibility, typically implemented at the application/workload layer and/or in customer-managed log processing pipelines prior to ingestion.
LOG-09.1	Are audit records generated, and do they contain relevant security information?	OCI cloud components are configured to generate and retain security-relevant audit/log records in alignment with the Oracle Cloud Security Logging and Log Analysis Standard. The scope of audited events is reviewed at least annually and updated as needed based on changes in the threat environment and risk.
LOG-10.1	Are audit records protected from unauthorized access, modification, and deletion?	OCI generates audit records for customer API calls, including actions performed through the Console, via the OCI Audit service. Audit records contain security-relevant information (e.g., who performed the action, source IP, target resource, timestamp, request/response details). Audit events are retained for 90 days and cannot be deleted by customers. Access to audit information and logging tooling is restricted based on least privilege/need-to-know, and security operations personnel are alerted on detected unauthorized or suspicious access attempts.
LOG-11.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	OCI monitors operational activities as they relate to key lifecycles and other cryptographic operational efforts. There are logs generated and mechanisms in place to review and respond to activity.
LOG-12.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	OCI monitors operational activities related to cryptographic keys, including key lifecycle management and other cryptographic operations. Logs are generated for relevant events and controls are in place to review activity for auditing and reporting purposes. Customers can access and retain these logs and configure

		monitoring/alerting in accordance with their security and compliance requirements.
LOG-13.1	Is physical access logged and monitored using an auditable access control system?	OCI monitors physical access using an auditable access control system. Physical access mechanisms generate access control logs that are forwarded to a Central Logging System (CLS) for centralized monitoring. Logging controls are configured to help prevent unauthorized or inadvertent alteration of log records by restricting access and applying appropriate protections. The standard log retention period is 90 days.
LOG-14.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	OCI has documented and implemented processes and technical measures to monitor for anomalies/failures, generate alerts, mage incidents, and evaluate effectiveness through post-incident review and continuous improvement.
LOG-14.2	Are accountable parties immediately notified about anomalies and failures?	OCI leverages Security Information and Event Management (SIEM) capability to correlate telemetry from multiple sources, including system events, firewall logs, Web Application Firewall (WAF) logs, and network flow data. Alerts are generated for potential security events and anomalies. Oracle Security personnel monitor the SIEM 24x7x365 and follow defined incident handling and escalation procedures. These procedures include reporting and notification requirements to appropriate accountable parties, including system owners and Oracle leadership, as required.

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, 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. 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 organization to provide overall direction for security events and incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). There are defined roles and responsibilities for the incident response teams embedded within the Lines of Business (LoBs). All LoBs must comply with 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.
SEF-01.2	Are policies and procedures reviewed and updated annually, or upon significant changes?	Oracle Corporate Security policies and procedures that address security incident management, e-discovery and forensics 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, or upon significant changes?	Oracle Corporate Security policies and procedures that address timely management of security incidents are reviewed annually and updated as needed.
SEF-03.1	Is a security incident response plan that includes a communication strategy for notifying relevant internal departments, impacted service customers, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle's Security Incident Management Policy defines requirements for reporting and responding to information security events and incidents. This policy authorizes the Oracle Chief Security Officer organization to provide overall direction for security event and incident preparation, detection, investigation, resolution, and forensic evidence handling across Oracle's Lines of Business (LoBs). The Integrated Cyber Center (ICC) is responsible for centralized coordination of security incident response and customer trust and security communications matters. LoB incident response programs must: Investigate and validate that a security event has occurred Communicate with relevant parties and provide appropriate notifications Preserve evidence and forensic artifacts Document the security event or incident and related response activities Contain security events or incidents Address root cause and implement corrective actions Escalate security events and incidents in accordance with defined procedures
SEF-04.1	Is a structured approach followed to evaluate the effectiveness of incident response plans at planned intervals or upon significant changes?	The Oracle Chief Security Officer organization conducts specialized training and exercises to test the effectiveness of the Incident Response Plan (IRP) and validate alignment with Incident Management and Response policies. The IRP is reviewed at least annually and updated as needed.
SEF-05.1	Are information security incident metrics established, monitored and reported?	Information security incident metrics are established and monitored within each Line of Business (LoB) under the oversight of the Oracle Chief Security Officer organization.
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	OCI has defined, implemented, and regularly evaluated processes, procedures, and technical controls to support business processes for triaging security-related events. These measures include documented incident/event triage and escalation procedures, centralized security monitoring and alerting, case management workflows, and coordinated response by security and operations teams. OCI validates effectiveness through periodic reviews, testing/exercises, and post-incident lessons learned as part of continuous improvement.
SEF-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for timely and effective response to security incidents	OCI has documented, implemented, and periodically tested incident response processes and technical controls to detect, triage, escalate, contain, and remediate security incidents in a timely manner based on defined incident categories and severity levels.

	in accordance with incident categories and severity levels?	
SEF-07.2	Are these processes and procedures reviewed, updated, and tested at least annually?	OCI has documented, implemented, and periodically tested incident response processes.
SEF-08.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	In the event Oracle determines that a confirmed security incident involving information processed by Oracle has occurred, Oracle will promptly notify impacted customers (or other relevant third parties) in accordance with its contractual and regulatory obligations, as set forth in the applicable Data Processing Agreement for Oracle Services. Oracle does not share information externally regarding malicious attempts, suspected incidents, or incident history.
SEF-08.2	Are material security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	OCI maintains incident response and notification processes to report material security breaches, including relevant supply chain incidents, in accordance with applicable contractual commitments (including SLAs/contract terms), laws, and regulations.
SEF-09.1	Is a secure repository of security incident records established and maintained?	Oracle maintains security incident management processes and retains relevant records for OCI-managed infrastructure and services in accordance with Oracle's internal security policies and compliance requirements. These records are protected with appropriate access controls and monitoring.
SEF-09.2	Are incident records regularly reviewed to identify patterns, root causes, and systemic vulnerabilities, and are relevant corrective measures implemented?	OCI regularly reviews security/incident records to identify patterns, root causes, and systemic vulnerabilities, and implements corrective actions as appropriate. This is handled through established operational security and incident management processes (e.g., centralized logging/monitoring, incident tracking, post-incident reviews/lessons learned, and remediation via configuration changes, patching, control enhancements, and preventive detections). Where relevant, OCI also coordinates corrective actions across services/teams and validates remediation effectiveness.
SEF-10.1	Are points of contact maintained for applicable regulation authorities, local law enforcement, and other legal jurisdictional authorities?	OCI maintains appropriate points of contact (POCs) for engagement with applicable regulatory authorities, local law enforcement and other legal jurisdictional authorities, as needed, and these POCs are managed through Oracle's established security, privacy, and legal/compliance functions.
SEF-10.2	Are points of contact reviewed and updated at least annually?	OCI maintains designated points of contact for OCI security and operations (including incident response and escalation). These contact details are reviewed and updated at least annually and upon personnel/role changes to help ensure availability and accuracy.

Control Domain: Supply Chain Management, Transparency, and Accountability

Question ID	Consensus Assessment Question	Oracle Response
STA-01.1	Are policies and procedures for supply chain risk management established, documented, approved, communicated, applied, evaluated, and maintained?	OCI maintains an established Supply Chain Risk Management (SCRM) program with documented, management-approved policies and procedures that are communicated internally and to relevant suppliers, implemented through supplier onboarding/contracting and ongoing vendor risk management activities, and periodically reviewed and updated.
STA-01.2	Are policies and procedures for supply chain risk management reviewed and updated at least annually, or upon significant changes?	OCI maintains documented supply chain risk management (SCRM) policies and procedures that are reviewed and updated at least annually and also on an ad hoc basis when significant changes occur
STA-02.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle implements a Shared Security Responsibility Model (SSRM) through established, documented, approved, and maintained security policies and procedures. These are communicated and applied across the organization and are evaluated through Oracle's governance and assurance activities. Oracle also maintains supply chain security policies and supplier management requirements including mandatory Supplier Information and Physical Security Standards and a Supplier Management Security Policy to guide the selection, oversight, and risk mitigation of third-party hardware/software and to reduce risks of malicious product alteration prior to customer use.
STA-02.2	Are the policies and procedures that apply the SSRM reviewed and updated annually, or upon significant changes?	OCI Cloud Security follows the Supplier Security Policy and the Supply Chain Security Standard to implement the Shared Security Responsibility Model (SSRM) process. These policies/standards and associated procedures are reviewed at least annually and are updated as needed upon significant changes. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html.
STA-03.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain?	OCI's Security Shared Responsibility Model (SSRM) is applied, documented, implemented, and managed in a way that supports OCI's supply chain through Oracle's governance and third-party/supplier security processes. Oracle documents and enforces security requirements for relevant suppliers/third parties supporting OCI, conducts risk-based due diligence and contracting (including security obligations), and performs ongoing oversight commensurate with supplier criticality and risk.
STA-04.1	Is the service customer given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	OCI provides customers with Security Shared Responsibility Model (SSRM) guidance that explains the division of security responsibilities between Oracle ("security of the cloud") and the customer ("security in the cloud"). Oracle remains responsible for the OCI cloud services and underlying infrastructure as described in the SSRM and related documentation.
STA-05.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM?	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). For more information see the Oracle Hosting and Delivery Policies and

		the Oracle Data Processing Agreement at https://www.oracle.com/contracts/cloud-services/
STA-06.1	Is the SSRM documentation reviewed and validated?	OCI Cloud Security SSRM documentation is reviewed annually and updated as needed. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/hosting-deliverypolicies.html
STA-07.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	OCI Cloud Security conducts third-party security assessments in scope with audit standards, including Supplier activities that are aligned with external regulations.
STA-08.1	Is an inventory of all supply chain relationships developed and maintained?	OCI maintains an inventory of all supply chain relationships. These agreements define the security, privacy, and compliance controls prior to the onset of services. Oracle follows the Oracle Supply Chain program to develop and maintain supply chain relationships. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain
STA-09.1	Is a process defined, implemented, and enforced for establishing a Bill of Material for the service supply chain?	OCI has a defined, implemented, and operational enforced process for establishing and maintaining a “bill of materials style” record for the service supply chain.
STA-09.2	Is the Bill of Material reviewed and updated at least annually or upon significant changes?	OCI has a defined, implemented, and operationally enforced process for establishing and maintaining a “bill of materials style” record for the service supply chain. Annual reviews are conducted on an annual basis.
STA-10.1	Are risk factors associated with supply chain relationships periodically reviewed?	OCI has established and maintains a supply chain risk management program to assess supplier risk factors and determine appropriate risk-based security measures for protecting Oracle and customer confidential information within the supply chain. The program and associated requirements are periodically reviewed at least annually and updated as needed to reflect changes in risk, supplier relationships, business requirements, or the threat landscape.
STA-11.1	Do service agreements between service providers and service customers (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 • Operational Resilience	See STA 04.1

STA-12.1	Are supply chain agreements reviewed at least annually or upon significant changes?	OCI maintains formal service agreements between Cloud Service Providers (CSPs) and Cloud Service Consumers (CSCs) that define service scope, responsibilities, and applicable security and compliance requirements. These service agreements are reviewed at least annually and are updated as needed to reflect material changes.
STA-13.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	OCI conducts risk assessments at least annually in alignment with OCI Risk Treatment SLAs to evaluate conformance with applicable security and compliance requirements and to identify, prioritize, and track risk treatment actions. Assessment results are used to update risk treatment plans and associated remediation activities, including timelines and accountable owners, and to help ensure plans remain effective as risks or control requirements change.
STA-14.1	Are policies that require all supply chain service providers to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Oracle has established Supplier Information Security and Physical Security Standards that define required security controls for suppliers and partners when accessing Oracle or Oracle customer facilities, networks, and/or information systems; handling Oracle confidential information; or maintaining custody of Oracle hardware assets. Suppliers are contractually responsible for complying with these standards and ensuring their personnel and subcontractors are bound by contractual terms consistent with Oracle's requirements. For more information https://www.oracle.com/corporate/security-practices/corporate/supply-chain/suppliers.html
STA-15.1	Are the organization's service providers' IT governance policies and procedures reviewed at least annually or upon significant changes?	Oracle's Third-Party Risk Management Policy requires each line of business to maintain a supplier risk management program. These programs must include assurance and oversight activities commensurate with supplier risk, including conducting supplier reviews at least annually where appropriate based on the risk to the confidentiality, integrity, or availability of data introduced by the supplier's goods or services.
STA-16.1	Is a process defined and implemented for conducting risk-based security assessments of the supply chain?	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 and threats to protect systems against vulnerability exploitation?	Oracle maintains a formal vulnerability management program for its enterprise systems and Oracle Cloud environments to identify, assess, track, and remediate technical security vulnerabilities. Oracle IT, security, and development teams monitor vendor and industry security bulletins (including Oracle security advisories) to evaluate and apply relevant patches. Oracle requires frequent automated vulnerability scanning of internal and external facing systems and periodic penetration testing in production environments. Vulnerabilities are prioritized for remediation based on severity and potential impact (including use of CVSS Base Score as a key input), tracked in a defect tracking system, and addressed through planned maintenance windows or emergency maintenance for severe issues in accordance with Oracle Cloud Hosting and Delivery Policies and applicable pillar documentation. Oracle also provides mechanisms for customers and security researchers to report vulnerabilities via Oracle's vulnerability reporting process or by submitting a support Service Request.
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually, or upon significant changes?	Oracle Corporate Security policies (including policies that address threat and vulnerability management) are reviewed annually and updated as needed.
TVM-02.1	Are policies and procedures to protect against malware and malicious instructions established, documented, approved, communicated, applied, evaluated, and maintained?	OCI has established, documented, approved, and communicated security policies and procedures to protect against malware and malicious activity, implements these controls across its environment, and periodically evaluates and updates them as part of ongoing security operations and compliance assurance, consistent with the shared responsibility model. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually, or upon significant changes?	Oracle Corporate Security policies (including policies addressing asset management and malware protection) are reviewed at least annually and updated as needed.
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	OCI defines, implements, and evaluates processes, procedures, and technical controls for vulnerability detection on organizational assets, with automated scans performed at least monthly and supported by continuous monitoring and remediation workflows.
TVM-04.1	Are a threat analysis process and procedures defined, implemented, and evaluated to identify, assess, and review the threat landscape for cloud systems?	OCI has defined and implemented threat analysis processes and procedures to identify, assess, and review the cloud threat landscape. These include threat intelligence integration, structured risk assessment, and continuous monitoring. The processes are regularly evaluated and updated, with outputs feeding into

		security operations and vulnerability management programs to help ensure timely risk mitigation.
TVM-04.2	Are threat models built according to industry best practices to inform the risk mitigation strategy?	OCI performs threat modeling using industry best practices as part of the Secure Software Development Lifecycle. Threat models are created during design and updated for significant changes, with identified risks documented, prioritized, and mitigated through defined security controls and architectural improvements, aligned with standards such as NIST and ISO 27005.
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	OCI implements processes and technical controls to update detection tools, threat signatures, and indicators of compromise on at least a weekly basis, and more frequently as needed. Updates are driven by automated threat intelligence feeds, internal analysis, and incident response insights, and are validated through ongoing monitoring, threat hunting, and security testing to help ensure effectiveness.
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open source libraries (according to the organization's vulnerability management policy)?	OCI implements processes and automated tools (including vulnerability scanning) to identify and remediate risks in third-party and open-source libraries. Vulnerabilities are prioritized based on severity, with defined remediation timelines. Controls are integrated into the Software Development Lifecycle and regularly reviewed per Oracle's vulnerability management policy.
TVM-07.1	Are processes, procedures and technical measures defined, implemented and evaluated for the periodic performance of penetration testing by independent third parties?	OCI maintains formal processes and procedures for periodic penetration testing conducted by independent third parties, aligned with industry standards (e.g., ISO 27001, SOC). Testing follows a risk-based approach, and identified vulnerabilities are tracked and remediated through a defined vulnerability management program with continuous evaluation and improvement.
TVM-08.1	Are processes, procedures and technical measures defined, implemented and evaluated based on identified risks to support scheduled and emergency responses to vulnerability identification?	OCI defines and implements risk-based processes, procedures, and technical controls for vulnerability management. Vulnerabilities are assessed based on severity and impact, with scheduled patching for standard issues and expedited response for critical vulnerabilities. Automated scanning, patching tools, and continuous monitoring support remediation. Controls are regularly evaluated through audits, testing, and ongoing review.
TVM-09.1	Is vulnerability remediation prioritized using a risk-based method from an industry-recognized framework?	OCI prioritizes vulnerability remediation using a risk-based methodology aligned with industry frameworks such as CVSS, NIST, and OWASP. Vulnerabilities are ranked based on severity, exploitability, asset criticality, and business impact to help ensure timely remediation of highest-risk issues.
TVM-10.1	Is a risk-based method used for the prioritization and mitigation of threats, leveraging an industry-recognized framework to guide threat decision-making and protection measures?	OCI uses a risk-based approach to prioritize and mitigate threats, aligned with industry-recognized frameworks (e.g., ISO, NIST), to guide threat management and control implementation.
TVM-11.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	OCI formal vulnerability management process is implemented to track, prioritize, and remediate vulnerabilities. Activities are recorded in a centralized system, with defined SLAs and regular reporting. Relevant stakeholders are notified of identified vulnerabilities and remediation status.

TVM-12.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	OCI establishes and tracks metrics for vulnerability identification and remediation (e.g. severity levels, SLA compliance). These are continuously monitored and reported at defined intervals to support risk management and remediation efforts.

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?	OCI maintains formally established, documented, approved, and communicated endpoint security policies and procedures. These are consistently applied across endpoints, regularly evaluated through audits and monitoring, and continuously maintained to address evolving risks and requirements.
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually, or upon significant changes?	OCI maintains formal Universal Endpoint Management (UEM) policies and procedures that are reviewed and updated at least annually, and additionally upon significant changes to the environment, technology, regulatory requirements, or risk posture. The review process is governed by OCI's information security and risk management framework, which helps ensure that policies remain aligned with industry standards, evolving threats, and organizational requirements. Updates are tracked through formal change management procedures, and relevant stakeholders are notified of material changes.
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?	OCI maintains and enforces a documented allowlist of approved applications, services, and trusted application sources for endpoints accessing or storing organizational data. Applications are subject to security review and approval, with controls enforced via endpoint management tools. The list is regularly reviewed, and unauthorized software is restricted or removed.
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	OCI processes are in place to validate endpoint compatibility with supported operating systems and applications through standardized configurations, testing, and monitoring.
UEM-04.1	Is an inventory of all endpoints used and maintained to store, access and process company data?	OCI maintains a comprehensive and continuously updated inventory of all endpoints (including compute instances, storage systems, databases, APIs, and managed services) that are used to store, access, or process company and customer data.
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, transmit, or process organizational data?	OCI enforces endpoint security through defined policies, procedures, and technical controls. Only authorized, compliant endpoints may access systems. Controls include IAM with MFA, encryption, endpoint protection, and network restrictions. Effectiveness is monitored via logging, audits, and continuous compliance checks.

UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	OCI helps ensure that all relevant interactive use endpoints are configured to require an automatic lock screen after a defined period of activity. This control is enforced through centralized endpoint management solutions and applies to corporate workstations, administrative systems, and remote access environments. Automatic session locking is implemented in accordance with Oracle's information security policies and standards, requiring re-authentication to regain access. These controls are aligned with industry recognized frameworks and are regularly reviewed and monitored for compliance.
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Changes to endpoint operating systems, patch levels, and applications are managed through OCI's formal organizational change management process. This process includes documented change requests, risk and impact assessments, testing and validation, approval workflows, and controlled deployment. All changes are tracked and auditable to help ensure compliance with security and operational requirements.
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	OCI uses encryption of data at rest on all managed endpoint devices using full disk encryption. Encryption is centrally managed, mandatory, and cannot be disabled by users. Non-compliant devices are restricted from accessing corporate resources, and encryption keys are securely managed. These controls help ensure data remains protected from unauthorized disclosure in the event of device loss or compromise.
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	OCI deploys and mages anti-malware detection and prevention technologies on Oracle-controlled endpoints. These solutions provide real-time threat detection, prevention, and remediation, and are centrally managed, monitored, and regularly updated.
UEM-10.1	Are software firewalls configured on managed endpoints?	OCI helps ensure that managed endpoints are protected by software-based firewalls where applicable. Host-based firewalls are configured according to security best practices and organizational policies, helping to restrict unauthorized inbound and outbound traffic. These controls are enforced through standardized configurations, regular monitoring, and compliance checks.
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	OCI provides services such as Data Safe, Cloud Guard, and active logging/monitoring capabilities that support data discovery, classification, and protection aligned to risk assessments. Customers can implement and enforce DLP controls on managed endpoints using OCI-active tools and/or third-party solutions in accordance with their security and compliance requirements under the shared responsibility model.
UEM-12.1	Are remote geo-location capabilities enabled for all managed mobile endpoints, in accordance with applicable laws and regulations?	Oracle Cloud Infrastructure implements remote geo-location capabilities for managed mobile endpoints where technically feasible and legally permissible. Such capabilities are enabled in a controlled and risk-based manner, taking into account applicable laws, regulations, and privacy requirements, including user consent where required.
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	OCI implements policies, procedures, and technical controls to enable remote deletion of company data on managed endpoint devices, including remote wipe capabilities, access revocation, monitoring, and periodic control reviews.

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?	OCI processes, procedures, and contractual requirements are established to help ensure third-party endpoints meet defined security standards. Technical controls (e.g., device compliance checks, access restrictions, and monitoring) are implemented, and compliance is regularly evaluated through audits and ongoing monitoring.