ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) v4.0 for Oracle Cloud Infrastructure (OCI)

September 2023 | Version 1.0

Purpose Statement

Developed by the Cloud Security Alliance, the Cloud Assessment Initiative Questionnaire (CAIQ) provides a standard template for cloud services providers 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 allows 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 at cloudsecurityalliance.org/research/artifacts/.

The answers contained in this CAIQ version 4.0 are related to Oracle cloud services.

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

If you have specific questions about this document, contact your Oracle account representative.

Disclaimer

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

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

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?	Oracle's Business Assessment & Audit (BA&A) is an independent global audit organization that performs global process and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards, and select laws and regulations across Oracle's Lines of Business and business units. Any key risks or control gaps identified by BA&A during these reviews are tracked through remediation. These reviews, identified risks, or control gaps are confidential and shared with executive leadership and Oracle's Board of Directors. The audit rights of customers for whom Oracle processes data are described in the Oracle Data Protection agreement. For more information, see oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing. The audit rights of customers of Oracle services are described in the Oracle Services Privacy Policy. For more information, see oracle.com/legal/privacy/services-privacy-policy.html.
		OCI reviews the internal standards and controls identified to meet global, regional, and industry compliance frameworks requirements, relevant policies, and regulatory, legal, and statutory requirements at least annually.
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as needed.
		OCI Compliance Standards are reviewed for completeness and accuracy at 6-month or 12-month intervals. All reviews are documented, approved, and communicated to OCI personnel.
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	See A&A-01.1. Oracle's Business Assessment & Audit (BA&A) is independent. Its operational activities and procedures are conducted at least annually in alignment with Institute of Internal Auditors (IIA) Standards. For more information, see oracle.com/corporate/security-practices/corporate/governance/business-assessment-audit/.
		Independent third-party audits of OCI's internal controls are conducted on a semiannual basis. For information about OCI's current compliance attestations, see oracle.com/corporate/cloud-compliance/. OCI customers can download audit reports and certifications directly from the Cloud Console.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	See A&A-01.1. Oracle's Business Assessment & Audit (BA&A) is independent. Its operational activities and procedures are conducted in alignment with Institute of Internal Auditors (IIA).
		OCI operates under policies that are generally aligned with the ISO/IEC 27002 Code of Practice for information security controls. OCI's internal controls are subject to periodic testing by independent third-party audit organizations including SOC 1, SOC 2, SOC 3, HIPAA, PCI, and many other standards. Attestation reports for OCI services are periodically issued by Oracle's third party auditors.
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	The relevance of standards, regulations, and legal/contractual and statutory requirements applicable to the audit are verified before the audit activity is approved. Compliance with those standards is to be verified by the Oracle LOB or other relevant Oracle party before requesting the audit activity be approved. Oracle Legal monitors the global regulatory landscape to identify legislation applicable to Oracle, including regional and local teams monitoring changes in relevant jurisdictions. Oracle Legal partners with Corporate Security and other organizations to manage Oracle's compliance to regulatory obligations across all lines of business.
		OCI engages with external assessment entities and independent auditors to verify that OCI has a comprehensive control environment that includes policies, processes, and security controls for the delivery of OCI infrastructure and platform services. These efforts conform with ISO/IEC 27001 standards and Corporate Security Policies. For more information, see oracle.com/corporate/cloud-compliance/.
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Audits of OCI's internal controls are planned, approved, and communicated across the business. The scope of the audits includes reviewing the effectiveness of the implementation of security operations. An internal and external audit of OCI is conducted by an independent party on an annual basis. OCI evaluates and communicates internal control findings in a timely manner to those parties responsible for taking corrective action. Findings are reviewed and tracked through resolution.
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Any key risks or control gaps identified by Oracle's Business Assessment & Audit (BA&A) during these reviews are tracked through remediation. Risk-based corrective action plans to remediate audit findings are established, documented, and communicated to BA&A for approval before being applied and maintained by Oracle's Lines of Business with evaluation by BA&A and executive leadership.
		OCI evaluates and communicates audit control findings in a timely manner to those parties responsible for taking corrective action.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Risks and control gaps identified by Oracle's Business Assessment & Audit (BA&A) and remediation status are confidential and shared with executive leadership and Oracle's Board of Directors.
		Findings are reviewed and tracked through resolution. Risks rated as critical and high are reviewed, assigned an owner, and remediated in line with the OCI risk management assessment program. Corrective action and audit finding remediation plans are Oracle Confidential and not shared externally.

Control Domain: Application & Interface Security

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience. Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices with the following goals: **Reducing the incidence of security weaknesses in all Oracle products** Oracle Software Security Assurance key programs include Oracle's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups, and the use of automated analysis and testing tools. **Reducing the impact of security weaknesses in Oracle products and services** Oracle has adopted transparent security vulnerability disclosure and remediation practices. The company is committed to treating all customers equally and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs. **Fostering security innovations** Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help organizations implement and manage consistent security controls across the technical environments in which they operate, on-premises and in the cloud. For more information, see oracle.com/corporate/security-practices/assurance/.
		OCI reviews the internal standards and controls identified to meet global, regional, and industry compliance frameworks requirements, relevant policies, and regulatory, legal, and statutory requirements at least annually.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address application security) are reviewed annually and updated as needed.
		The OCI Compliance Standard for Application Security is reviewed for completeness and accuracy no less than annually.
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. For more information, see oracle.com/corporate/security-practices/assurance/development/configuration.html.
		OCI employs standardized system hardening practices across OCI devices, which include alignment monitoring with base images or baselines, restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, and logging.
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	OCI's technical and operational metrics are defined, implemented, and reviewed by leadership at least annually as a part of the ISO program to meet relevant business objectives, security requirements, and compliance obligations.
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	To ensure that Oracle products are developed with consistently high security assurance, and to help developers avoid common coding mistakes, Oracle employs formal Secure Coding Standards. Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. They discuss general security knowledge areas such as design principles, cryptography and communications security, and common vulnerabilities, and provide specific guidance on topics such as data validation, CGI, and user management. All Oracle developers must be familiar with these standards and apply them when designing and building products. The coding standards have been developed over a number of years and incorporate best practices as well as lessons learned from continued vulnerability testing by Oracle's internal product assessment team. Oracle ensures that developers are familiar with its coding standards. The Secure Coding Standards are a key component of Oracle Software Security Assurance (OSSA) and adherence to the standards is assessed and validated throughout the supported life of all Oracle products.
		OCI's SDLC practices are intended to align with OSSA corporate standards.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Security assurance analysis and testing verify security qualities of Oracle products against various types of attacks. Two broad categories of tests are employed for testing Oracle products: static analysis and dynamic analysis. **Static analysis** Static security analysis of source code is the initial line of defense used during the product development cycle. Oracle uses a commercial static code analyzer and a variety of internally developed tools to catch problems while code is being written. **Dynamic analysis** Dynamic analysis activity always occurs during latter phases of product development: at the very least, the product or component should be able to run. Although this may vary among Oracle organizations, typically this activity is handled by a security QA team (or a similar dedicated group) and may be shared by multiple product teams. Dynamic analysis is aimed at externally visible product interfaces and APIs, and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing within Oracle. For more information, see oracle.com/corporate/security-practices/assurance/development/analysis-testing.html. The Oracle Corporate Security Solution Assurance Process (CSSAP) and the Oracle Release Management (ORM) process are implemented for new OCI service offerings, and new versions and new features for existing services by validating that new services meet Oracle Software Security Assurance (OSSA) standards and Compliance Onboarding requirements. This process is ongoing throughout the development lifecycle with regular monitoring and scanning and an established Change Management program to test and validate all production deployments. As part of the ORM process, teams are required to complete static, dynamic, and malware testing. Any findings from the automated scans, and high and critical findings from manual scans, must be addressed prior to release approval.
AIS-05.2	Is testing automated when applicable and possible?	After code is checked in, unit tests are automatically run. The completed build job automatically triggers static code analysis on supported languages. Findings from these scans are opened automatically and must be tracked to resolution.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Cloud services are deployed in a specific configuration or in a small number of configurations. Testing must be performed on the product in this configuration, with predeployment tests performed in an environment identical to the production environment. Development organizations are required to provide a capability in which the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. For more information, see oracle.com/corporate/security-practices/assurance/development/configuration.html. Changes to infrastructure configurations and services supporting OCI are documented in an electronic, access-controlled ticketing system. A workflow and mandatory fields are implemented in the ticketing system to help ensure compliance with the change management requirements. The mandatory fields require a description of the following items: • The nature of the proposed change • The impacted systems (direct and indirect) • The impact of the change • Required updates to system documentation after the change • The test plans • The internal and external notification plan (if necessary) • The rollback plan • The 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. Changes to infrastructure configurations and services supporting OCI must be peer-reviewed prior to implementation. A member of the same team with knowledge of the impacted service, who can technically review the change for accuracy and potential issues, typically acts as the reviewer. Changes to infrastructure configurations and services supporting OCI must be tested prior to implementation. The type of test depends on the nature of the change but may include unit, regression, manual, or integration tests. The development and testing environment is separated from the production environment to reduce the risks of unauthorized access or changes to the operational environment. Emergency changes to infrastructure configurations and services supporting the OCI require approval of a Senior Manager or above. Code changes are implemented through continuous integration/continuous deployment (CI/CD) tools. Except where dependencies exist across multiple availability domains (for example, updates to domain name services), changes are implemented separately in each region and availability domain.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
AIS-06.2	Is the deployment and integration of application code automated where possible?	Code changes are implemented through continuous integration/continuous deployment (CI/CD) tools. Except where dependencies exist across multiple availability domains (for example, updates to domain name services), changes are implemented separately in each region and availability domain.

AIS-07.1	Are application security vulnerabilities remediated following defined processes?	To provide the best security posture to all Oracle customers, Oracle fixes significant security vulnerabilities based on the likely risk that they pose to customers. As a result, the issues with the most severe risks are fixed first. Fixes for security vulnerabilities are produced in the following order:
		• Main code line first—that is the code line being developed for the next major release of the product
		• For each supported version that is vulnerable:
		  ○ Fix in the next patch set if another patch set is planned for that supported version
		  ○ Creation of a Critical Patch Update patch
		For more information, see oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html.
		
		A commercial vulnerability scanning tool scans external IP addresses and internal OCI nodes at least weekly. Identified threats and vulnerabilities are investigated and tracked to resolution in accordance with the Cloud Compliance Standard for Vulnerability Management.
		
		OCI performs internal vulnerability scans weekly, which includes 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 that ensures vulnerabilities are evaluated, and patches are deployed across the environment based on criticality. OCI vulnerability severity is assessed based on Common Vulnerability Scoring System (CVSS) scoring, and remediation timelines are based on the assigned severity and possible business impact. Patches and updates are implemented through continuous integration/continuous deployment (CI/CD) tools. Except where dependencies exist across multiple availability domains (for example, updates to domain name services), changes are implemented separately in each region and availability domain.

Control Domain: Business Continuity Management & Operational Resilience

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	The Risk Management Resiliency Program (RMRP) objective is to establish a business-resiliency framework to help provide an efficient response to business interruption events affecting Oracle's operations. For more information, see oracle.com/corporate/security-practices/corporate/resilience-management/. The RMRP approach is comprised of several subprograms: emergency response to unplanned and emergent events, crisis management of serious incidents, technology disaster recovery, and business-continuity management. The goal of the program is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored. Each of these subprograms is a uniquely diverse discipline. However, by consolidating emergency response, crisis management, business continuity, and disaster recovery, they can become a robust collaborative and communicative system. Oracle's RMRP is designed to engage multiple aspects of emergency management and business continuity from the onset of an event and to leverage them based on the needs of the situation. The RMRP is implemented and managed locally, regionally, and globally. The RMRP program management office provides executive scorecard reporting on program activities and status within the lines of business.
		The OCI Cloud Compliance Standard for Resilience and Crisis Management establishes procedures for OCI personnel and services. Each OCI service team must create, maintain, and test their Resilience Plan annually. Updates and modifications are communicated to employees following the review. OCI standards are available to all employees on the company's intranet and enhanced through required training.
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations. Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. For more information, see oracle.com/corporate/security-practices/corporate/resilience-management/.
		The OCI Cloud Standard for Resilience and Crisis Management is reviewed for completeness and accuracy no less than annually.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Corporate business continuity policy, standards, and practices are governed by the RMRP Program Management Office (PMO) and are generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance. For more information, see oracle.com/corporate/security-practices/corporate/resilience-management/.
		OCI maintains a Business Impact Analysis (BIA) and Service Resiliency Plan (SRP) for each service. The plans are reviewed annually and have the following characteristics: • Include a defined purpose and scope, aligned with relevant dependencies • Are accessible to and understood by those who use them • Have an assigned owner and include documented roles and responsibilities • Include detailed recovery procedures and reference information and the method for plan invocation
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	The RMRP PMO develops planning materials and tools as aids to LOB Risk Managers in managing their business continuity plans, testing, and training procedures. The RMRP program requires all LOBs to perform the following actions: • Identify relevant business interruption scenarios, including essential people, resources, facilities, and technology • Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Obtain approval from the LOB's executive For more information, see oracle.com/corporate/security-practices/corporate/resilience-management/.
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	See BCR-03.1
		OCI services are required to conduct an annual review of their business continuity plans with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. Each service, new or established, must annually review and update their Business Impact Analysis and Recovery Plan as well as complete an After Action Report designed to remediate any risks or problems that arise from the annual review.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	The critical LOBs are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. They must perform the following actions: • Conduct a Business Impact Analysis that specifies a Recovery Time Objective and Recovery Point Objective (if appropriate to the function) and identifies the organization's business continuity contingencies strategy • Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Revise business continuity plans based on changes to operations, business requirements, and risks For more information, see oracle.com/corporate/security-practices/corporate/resilience-management/.
		OCI services are required to conduct an annual review of their business continuity plans with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. Each service, new or established must annually review and update their Business Impact Analysis and Recovery Plan as well as complete an After Action Report designed to remediate any risks or problems that arise from the annual review.
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	See BCR-03.1
		OCI services must create, maintain, and continuously evaluate their Resilience Plan for operations. All resilience documentation, including the Resilience Plan, must be maintained in a central repository that is accessible to authorized stakeholders.
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations. See BCR-03.1
		OCI services must create, maintain, and continuously evaluate their Resilience Plan for operations. Resilience Plans are reviewed and tested annually.
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	The critical LOBs are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. For more information, see oracle.com/corporate/security-practices/corporate/resilience-management/business-continuity.html.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	OCI services test their Resilience Plan annually against a preplanned, designed disruption scenario, including testing all appropriate security provisions, to assess the Resilience Plan effectiveness in minimizing impacts to systems or processes from the effects of a major incident or disruption.
BCR-08.1	Is cloud data periodically backed up?	The Cloud Compliance Standard for Resilience and Crisis Management establishes requirements for OCI service backups, including testing backups monthly for reliability and integrity. Customers are responsible for implementing a backup process, replication process, or both in line with their requirements and policies.
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	OCI services must meet applicable control plane and data plane backup requirements, as defined by the Cloud Compliance Standard for Resilience and Crisis Management. OCI backups are monitored, and issues relating to backup failure are tracked to resolution.
BCR-08.3	Can backups be restored appropriately for resiliency?	OCI services document and maintain resiliency plans to ensure that damage or disruption to critical assets can be quickly minimized and that these assets can be restored to normal operations as quickly as possible. Oracle provides restore capabilities as part of the service offerings where backup is offered. Customers are responsible for implementing a backup process, replication process, or both in line with their requirements and policies. For more information about Oracle Services Backup Strategy, see the Oracle Cloud Hosting and Delivery Policies and Oracle Service Descriptions at oracle.com/contracts/cloud-services/.
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Oracle's corporate Disaster Recovery (DR) plan focuses on the resiliency of computing infrastructure supporting Oracle's internal operations and cloud services. Oracle's production data centers are geographically separated and have component and power redundancy, with backup generators in place for availability of data center resources in case of an impacting event. For more information, see oracle.com/corporate/security-practices/corporate/resilience-management/disaster-recovery.html.
		OCI maintains a Business Impact Analysis (BIA) and Service Resiliency Plan (SRP) for each service. The plans are reviewed annually and have the following characteristics: • Include a defined purpose and scope, aligned with relevant dependencies • Are accessible to and understood by those who use them • Have an assigned owner and include documented roles and responsibilities • Include detailed recovery procedures and reference information and the method for plan invocation

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	See BCR-05.1.
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	See BCR-05.1.
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	No.
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Oracle maintains a redundant network infrastructure, including DNS servers to route between primary and secondary sites, network devices, and load balancers. Oracle cloud data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html. OCI is physically hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centers within a region. A region is composed of one or more availability domains. Each availability domain contains three fault domains. A fault domain is a grouping of hardware and infrastructure within an availability domain. Fault domains provide anti-affinity: they let customers distribute their instances so that the instances are not on the same physical hardware within a single availability domain. A hardware failure or Compute hardware maintenance event that affects one fault domain does not affect instances in other fault domains. In addition, the physical hardware in a fault domain has independent and redundant power supplies, which prevents a failure in the power supply hardware within one fault domain from affecting other fault domains. The availability domains within the same region are connected to each other by a low-latency, high-bandwidth network, which makes it possible for customers to provide high-availability connectivity to the internet and on-premises, and to build replicated systems in multiple availability domains for both high-availability and disaster recovery. Regions are independent of each other and can be separated by vast geographical distances. Dedicated regions are public regions assigned to a single organization. Generally, customers deploy an application in the region where it is most heavily used, because using nearby resources is faster than using distant resources. However, customers can also deploy applications in different regions for the following reasons: • To mitigate the risk of region-wide events such as large weather systems or earthquakes • To meet varying requirements for legal jurisdictions, tax domains, and other business or social criteria

Control Domain: Change Control & Configuration Management

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	OCI does not use external business partners for development, change management, or release management. All development is performed by OCI employees. Changes to infrastructure configurations and services supporting the System are documented in an electronic, access-controlled ticketing system. A workflow and mandatory fields are implemented in the ticketing system to help ensure compliance with the change management requirements. The mandatory fields require a description of the following items: • The nature of the proposed change • The impacted systems (direct and indirect) • The impact of the change • Required updates to system documentation after the change • The test plans • The internal and external notification plan (if necessary) • The rollback plan • The 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. Changes to infrastructure configurations and services supporting the System must be peer-reviewed prior to implementation. A member of the same team with knowledge of the impacted service, who can technically review the change for accuracy and potential issues, typically acts as the reviewer. Changes to infrastructure configurations and services supporting the System must be tested prior to implementation. The type of test depends on the nature of the change but may include unit, regression, manual, or integration tests. The development and testing environment is separated from the production environment to reduce the risks of unauthorized access or changes to the operational environment. Emergency changes to infrastructure configurations and services supporting the System require approval of a Senior Manager or above. Code changes are implemented through continuous integration/continuous deployment (CI/CD) tools. Except where dependencies exist across multiple availability domains (for example, updates to domain name services), changes are implemented separately in each region and availability domain.
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	OCI reviews internal controls and OCI Cloud Compliance Standards identified to meet the requirements of the control framework, relevant standards, and regulatory, legal, and statutory requirements at least annually.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	See CCC-01.1.
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Oracle Corporate Security Solution Assurance Process (CSSAP) is a security review process developed by Corporate Security Architecture, Global Information Security, Global Product Security, Oracle Global IT, and Oracle's IT organizations to provide comprehensive information-security management review. CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle: • **Pre-review**: The risk management teams in each LOB must perform a preassessment of each project by using the approved template. • **CSSAP review**: The security architecture team reviews the submitted plans and performs a technical security design review. • **Security assessment review**: Based on risk level, systems and applications undergo security verification testing before production use. Reviews ensure that projects are aligned with Oracle Corporate Security Architecture strategy and direction, and Oracle Corporate security, privacy, and legal policies, procedures and standards. For more information, see oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.
		OCI does not use external business partners for development, change management, or release management. All development is performed by OCI employees. Changes to infrastructure configurations and services supporting the System must be tested prior to implementation. The type of test depends on the nature of the change but may include unit, regression, manual, or integration tests. The development and testing environment is separated from the production environment to reduce the risks of unauthorized access or changes to the operational environment. Code changes are implemented through continuous integration/continuous deployment (CI/CD) tools. Except where dependencies exist across multiple availability domains (for example, updates to domain name services), changes are implemented separately in each region and availability domain.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted	Oracle's Network Security Policy establishes requirements for network management, network access, and network device management, including authentication and authorization requirements for both physical devices and software-based systems. Unused network ports must be deactivated. For more information, see oracle.com/corporate/security-practices/corporate/access-control.html. Oracle's Information Systems Asset Inventory Policy requires that Lines of Business (LOBs) maintain accurate and comprehensive inventories of information systems, hardware, and software. This policy applies to all information assets held on any Oracle system, including enterprise systems and cloud services. For more information, see oracle.com/corporate/security-practices/corporate/information-assets-classification.html.
		The OCI Cloud Compliance Standard for Asset Management outlines the proper procedures for handling of OCI assets, including but not limited to, logging any changes to the registered components and location of assets in the inventory register during asset acquisition, development, utilization, maintenance, and disposal or renewal.
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	Refer to the Hosting and Delivery Pillar document for Service Level Agreements located at oracle.com/corporate/contracts/cloud-services/.
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Changes to infrastructure configurations and services supporting the System are documented in an electronic, access-controlled ticketing system. A workflow and mandatory fields are implemented in the ticketing system to help ensure compliance with the change management requirements. The mandatory fields require a description of the following items: • The nature of the proposed change • The impacted systems (direct and indirect) • The impact of the change • Required updates to system documentation after the change • The test plans • The internal and external notification plan (if necessary) OCI Change Management follows the OCI Cloud Compliance Standard for Change Management, which is shared with all employees.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	The OCI Cloud Compliance Standard for Change Management outlines the procedures for Oracle personnel and programs that develop, administer, or support OCI, which includes unauthorized change prevention. OCI services monitor for unexpected and unauthorized changes and log deviations on the affected host, and alert the Detection and Response Team (DART) as necessary.
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Changes to infrastructure configurations and services supporting the System are documented in an electronic, access-controlled ticketing system. A workflow and mandatory fields are implemented in the ticketing system to help ensure compliance with the change management requirements. The mandatory fields require a description of the following items: • The nature of the proposed change • The impacted systems (direct and indirect) • The impact of the change • Required updates to system documentation after the change • The test plans • The internal and external notification plan (if necessary) • The rollback plan • The 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. Changes to infrastructure configurations and services supporting the System must be peer-reviewed prior to implementation. A member of the same team with knowledge of the impacted service, who can technically review the change for accuracy and potential issues, typically acts as the reviewer. Changes to infrastructure configurations and services supporting the System must be tested prior to implementation. The type of test depends on the nature of the change but may include unit, regression, manual, or integration tests. The development and testing environment are separated from the production environment to reduce the risks of unauthorized access or changes to the operational environment. Emergency changes to infrastructure configurations and services supporting the System require approval of a Senior Manager or above. Code changes are implemented through continuous integration/continuous deployment (CI/CD) tools. Except where dependencies exist across multiple availability domains (for example, updates to domain name services), changes are implemented separately in each region and availability domain.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	OCI Change Management aligns with the requirements of the GRC-04: Policy Exception Process.
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	See CCC-08.1.

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. Compliance with these requirements is monitored by Oracle Global Product Security. 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. For more information, see oracle.com/corporate/security-practices/corporate/data-protection/.
		The Cloud Compliance Standard for Encryption establishes encryption methods and procedures to protect the confidentiality, integrity, and availability of data. The standard specifies appropriate encryption technologies and acceptable levels of encryption for Oracle Cloud. The Cloud Compliance Standard for Encryption is based on standards from the National Institute of Standards and Technology (NIST), the Federal Government Standards on encryption (FIPS 140 and FIPS 180), and Oracle's Cryptographic Review Board. Customers are responsible for appropriately safeguarding encryption keys that they own, manage, and maintain. Vault allows customers to centrally manage the encryption keys that protect their data and the secret credentials that they use to securely access resources. Customers can use the OCI Vaultiv service to create and manage vaults, keys, and secrets. Vaults securely store master encryption keys and secrets. Specifically, depending on the protection mode, keys are stored either on the server or on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 2 security certification.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address cryptography, encryption, and key management) are reviewed annually and updated as needed.
		The OCI Cloud Compliance Standard for Encryption is reviewed for completeness and accuracy no less than annually.
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Oracle's Cryptography Review Board (CRB) defines and promotes cryptography-related technical standards for Oracle products and services. The group is primarily responsible for making technical decisions and authoring internal standards to address government and industry requirements. Representatives from Corporate Security and development organizations define best practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence. CRB's responsibilities include: • Creating and maintaining standards for cryptography algorithms, protocols, and their parameters • Providing approved standards in multiple formats, for readability and automation • Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle • Providing practical guidance on using cryptography • Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography For more information, see oracle.com/corporate/security-practices/corporate/governance/global-product-security.html.
		The OCI Cloud Compliance Standard for Encryption defines roles and responsibilities.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Solutions for managing encryption keys and cryptographic libraries at Oracle must be approved per the Corporate Security Solution Assurance Process (CSSAP). Oracle defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include: • Locations and technologies for storing encryption keys • Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures • Changing default encryption keys • Replacement schedule for various types of encryption keys For more information, see oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html.
		OCI stores master encryption keys securely in a FIPS validated hardware security module (HSM) by default. Keys cannot be exported from the HSM in plain text. Connections to the customer administration console, APIs, or host region must be made over an encrypted protocol using HTTPS and TLS 1.2 or above. Data stored on OCI Block Volume, Object Storage, File Storage, and Exadata Cloud Service storage is encrypted at rest by using AES 256-bit encryption. OCI Data Transfer uses AES 256 for encryption of data at rest. OCI Vault offers the ability to create master encryption keys and data encryption keys, rotate keys to generate new cryptographic material, enable or disable keys for use in cryptographic operations, assign keys to resources, and use keys for encryption and decryption.
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to only use up-to-date versions of approved security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms. For more information, see oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html.
		See CEK-03.1.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
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 defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include: • Locations and technologies for storing encryption keys • Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures • Changing default encryption keys • Replacement schedule for various types of encryption keys For more information, see oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html.
		Changes to infrastructure configurations and services supporting OCI follow the Cloud Compliance Standard for Change Management and are documented in an access-controlled ticketing system, tested, and peer-reviewed prior to implementation. See CCC-06.1 for more details.
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Solutions for managing encryption keys at Oracle must be approved per the Corporate Security Solution Assurance Process (CSSAP). Oracle defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include: • Locations and technologies for storing encryption keys • Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures • Changing default encryption keys • Replacement schedule for various types of encryption keys For more information, see oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html.
		The Cloud Compliance Standard for Encryption, which is supported by Oracle Software Security Assurance (OSSA) standards on cryptography, outlines the roles and responsibilities, as well as the objectives to protect the confidentiality, integreity, and availability of customer information whenever cryptographic protections are employed. This standard applies to data transmitted into, out of, or within the OCI environments as well as data stored under Oracle's control within OCI.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Representatives from Corporate Security and development organizations define recommended practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence. For more information, see oracle.com/corporate/security-practices/corporate/governance/global-product-security.html.
		The OCI Global Enterprise Risk team is responsible for identifying, analyzing, measuring, mitigating or responding to, and monitoring risk specific to the OCI organization. Risk assessments are performed annually across OCI to identify threats and risks that could impact the security, confidentiality, or availability of the system. The risk assessment is modeled after National Institute of Standards and Technology (NIST) Special Publication 800-30 Rev. 1 guidelines and incorporates risk assessment requirements from the ISO/IEC 27001:2013 standard. Risks are reviewed, assigned an owner, and remediated in line with the OCI risk management assessment program. The results of internal audits, external audits, customer audits, and other compliance activities are collated and form inputs into OCI's risk assessment process.
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	Vault allows customers to centrally manage the encryption keys that protect their data and the secret credentials that they use to securely access resources. Before the introduction of secrets as a resource, OCI Vault was known as OCI Key Management. Customers can use the Vault service to create and manage vaults, keys, and secrets. Vaults securely store master encryption keys and secrets. Specifically, depending on the protection mode, keys are stored either on the server or on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 2 security certification. OCI Object Storage, Block Volume, File Storage, and Streaming services integrate with the Vault service to support encryption at rest of data in buckets, block or boot volumes, file systems, and stream pools. OCI Container Engine for Kubernetes integrates with the Vault service to support the creation of new clusters with encrypted Kubernetes secrets at rest in the key-value store. Integration with OCI Identity and Access Management (IAM) allows customers to control who and what services can access which keys and secrets and what they can do with those resources. Integration with OCI Audit allows customers to monitor key and secret usage. Audit tracks administrative actions on vaults, keys, and secrets. Vault uses the AES as its encryption algorithm, and its keys are AES symmetric keys.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
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?	An internal and external audit of the System is conducted by an independent party on an annual basis. OCI evaluates and communicates internal control findings in a timely manner to those parties responsible for taking corrective action. Findings are reviewed and tracked through resolution. A Corrective Action/Preventive Action (CAPA) review is completed after the resolution of an Incident Command Center SEV1 incident that met the CAPA review requirements. The OCI Global Enterprise Risk team is responsible for identifying, analyzing, measuring, mitigating or responding to, and monitoring risk specific to the OCI organization. Risk assessments are performed annually across OCI to identify threats and risks that could impact the security, confidentiality, or availability of the system. The risk assessment is modeled after National Institute of Standards and Technology (NIST) Special Publication 800-30 Rev. 1 guidelines and incorporates risk assessment requirements from the ISO/IEC 27001:2013 standard. Risks are reviewed, assigned an owner, and remediated in line with the OCI risk management assessment program. The results of internal audits, external audits, customer audits, and other compliance activities are collated and form inputs into OCI's risk assessment process.
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	See CEK-09.1.
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services. See oracle.com/corporate/security-practices/corporate/governance/global-product-security.html. Solutions for managing encryption keys at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). OCI services use industry accepted technologies and processes for cryptographic key generation and key management, in accordance with the OCI Cloud Compliance Standard for Encryption and supported by the OCI Cloud Compliance Standard Cryptography.
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	In accordance with the OCI Cloud Compliance Standard for Encryption which is supported by the OCI Standard Cryptography, the OCI Vault service offers the ability to create master encryption keys and data encryption keys, rotate keys to generate new cryptographic material, enable or disable keys for use in cryptographic operations, assign keys to resources, and use keys for encryption and decryption.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	In accordance with the OCI Cloud Compliance Standard for Encryption which is supported by the OCI Standard Cryptography, the OCI Vault service offers the ability to create master encryption keys and data encryption keys, rotate keys to generate new cryptographic material, enable or disable keys for use in cryptographic operations, assign keys to resources, and use keys for encryption and decryption.
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?	When a key is disabled or scheduled for deletion, it is made unusable for cryptographic operations. When scheduled for deletion, it is deleted from the HSM within 30 days or less.
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	See CEK-13.1.
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?	Customers are responsible for appropriately safeguarding encryption keys that they own, manage, and maintain. Vault allows customers to centrally manage the encryption keys that protect their data and the secret credentials that they use to securely access resources. Before the introduction of secrets as a resource, OCI Vault was known as OCI Key Management. Customers can use the Vault service to create and manage vaults, keys, and secrets. Vaults securely store master encryption keys and secrets. Specifically, depending on the protection mode, keys are stored either on the server or on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 2 security certification.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
		OCI Object Storage, Block Volume, File Storage, and Streaming services integrate with the Vault service to support encryption at rest of data in buckets, block or boot volumes, file systems, and stream pools. OCI Container Engine for Kubernetes integrates with the Vault service to support the creation of new clusters with encrypted Kubernetes secrets at rest in the key-value store. Integration with OCI IAM allows customers to control who and what services can access which keys and secrets and what they can do with those resources. Integration with OCI Audit allows customers to monitor key and secret usage. Audit tracks administrative actions on vaults, keys, and secrets. Vault uses the AES as its encryption algorithm, and its keys are AES symmetric keys.
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?	The OCI Cloud Compliance Standard for Encryption defines the processes, procedures, and technical measures by which OCI keys are managed. When a key is disabled or scheduled for deletion, it is made unusable for cryptographic operations. When scheduled for deletion, it is deleted from the HSM within 30 days or less. Key lifecycle management events are logged and available to enable auditing and reporting on changes in status of cryptographic keys. OCI Vault offers the ability to create master encryption keys and data encryption keys, rotate keys to generate new cryptographic material, enable or disable keys for use in cryptographic operations, assign keys to resources, and use keys for encryption and decryption.
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	The OCI Cloud Compliance Standard for Encryption defines the processes, procedures, and technical measures by which OCI keys are managed. When a key is disabled or scheduled for deletion, it is made unusable for cryptographic operations. When scheduled for deletion, it is deleted from the HSM within 30 days or less. OCI Vault offers the ability to create master encryption keys and data encryption keys, rotate keys to generate new cryptographic material, enable or disable keys for use in cryptographic operations, assign keys to resources, and use keys for encryption and decryption.
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 managed keys are securely archived and recoverable by the key owner to guard against hardware failures, software failures, human errors or malicious actions, natural disasters, or other incidents. Organizations should implement periodic testing to validate that key material for which Oracle has a corporate, legal, contractual, or fiduciary responsibility to manage is being properly archived and that the key material can be recovered by the key owner. Virtual Private Vault customers can back up and recover cryptographic key materials protected by HSM to and from a secure repository that is restricted to authorized personnel only.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services. See oracle.com/corporate/security-practices/corporate/governance/global-product-security.html. Solutions for managing encryption keys at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). OCI standards and processes include security requirements for key creation, use, storage, and protection. OCI stores master encryption keys securely in a FIPS validated hardware security module (HSM) by default. Keys cannot be exported from the HSM in plain text. When a key is disabled or scheduled for deletion, it is made unusable for cryptographic operations. When scheduled for deletion, it is deleted from the HSM within 30 days or less.
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 can back up and recover cryptographic key materials protected by HSM to and from a secure repository that is restricted to authorized personnel only. Customers are responsible for managing the life cycle of cryptographic keys, including key generation, key activation, key rotation, re-encryption of old data using new keys, and key disabling and deletion.
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?	Key lifecycle management events are logged and available to enable auditing and reporting on changes in status of cryptographic keys.

Control Domain: Data Center Security

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Oracle's Media Sanitization Policy specifies requirements including secure disposal of equipment and media used for data storage. This policy is established, documented, approved, communicated, enforced, and maintained as part of Oracle Security Policy. The OCI Cloud Compliance Standard for Asset Management describe the procedures for asset lifecycle management including secure disposal.
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Oracle's Media Sanitation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information that is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. For more information, see oracle.com/corporate/security-practices/corporate/information-assets-classification.html.
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	The Oracle Media Sanitization and Disposal Policy outlines the requirements for media sanitization and disposal and is reviewed and updated annually. The OCI Cloud Compliance Standard for Asset Management describes the process for asset lifecycle management of OCI information assets, including secure disposal. OCI Cloud Compliance Standards are reviewed and updated no less than annually.
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Oracle's Information Systems Inventory Policy requires that Lines of Business (LOBs) maintain accurate and comprehensive inventories of information systems, hardware, and software. This inventory must be managed within an approved inventory system under whose authority the Policy is established, documented, approved, communicated, implemented, enforced, and maintained. For more information, see oracle.com/corporate/security-practices/corporate/information-assets-classification.html. The OCI Cloud Compliance Standard for Asset Management outlines the procedures for the proper handling of assets. The Oracle Systems Decommissioning and Repurposing Policy requires that repurposing of information systems must be carried out by an Oracle employee or approved contractor and recorded and tracked to ensure that the security of the hardware asset is maintained throughout the transfer process.
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	OCI services log any changes to information assets and the location of an asset in the inventory register during asset acquisition, development, utilization, maintenance, and disposal.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address the relocation or transfer of hardware, software, or data or information to any location) are reviewed annually and updated as needed.
		See DCS-02.1. The OCI Cloud Compliance Standard for Asset Management describes the procedures for asset lifecycle management of OCI information assets. OCI Cloud Compliance Standards are reviewed and updated no less than annually.
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. For more information, see oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html.
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address safe and secure working environments) are reviewed annually and updated as needed.
		OCI reviews internal controls and Cloud Compliance Standards identified to meet the requirements of the control framework, relevant standards, and regulatory, legal, and statutory requirements at least annually.
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Oracle's Information Systems Inventory Policy requires that Lines of Business (LOBs) maintain accurate and comprehensive inventories of information systems, hardware, and software. This inventory must be managed within an approved inventory system under whose authority the Policy is established, documented, approved, communicated, implemented, enforced, and maintained. For more information, see oracle.com/corporate/security-practices/corporate/information-assets-classification.html. The OCI Cloud Compliance Standard for Asset Management establishes procedures for monitoring and maintaining OCI assets. The Oracle Systems Decommissioning and Repurposing Policy requires that repurposing of information systems must be carried out by an Oracle employee or approved contractor and recorded and tracked to ensure that the security of the hardware asset is maintained throughout the transfer process. Oracle Global Information Security (GIS) establishes and maintains corporate information security policies. Policies are reviewed and revised by GIS at least annually. OCI reviews internal controls and OCI Compliance Standards identified to meet the requirements of the control framework, relevant standards, and regulatory, legal, and statutory requirements at least annually.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address the secure transportation of assets) are reviewed annually and updated as needed.
		The OCI Cloud Compliance Standard for Asset Management is reviewed for completeness and accuracy no less than annually.
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Oracle's formal Information Protection Policy sets forth the requirements for classifying and handling public and confidential information. For more information, see oracle.com/corporate/security-practices/corporate/information-assets-classification.html.
		OCI system owners must handle assets in a manner suitable with their confidentiality levels as defined in the Oracle Information Protection Policy.
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	The Oracle Information Systems Inventory Policy requires that Lines of Business (LOBs) 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, and data held on information systems, and information needed for disaster recovery and business continuity purposes.
		OCI information assets are recorded in an OCI Security-approved asset register upon creation or purchase. OCI servies use IT inventory management to discover, track, and centrally manage hardware, software, and data throughout their life cycle.
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Oracle Global Physical Security uses a risk-based approach to physical and environmental security. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained. For more information, see oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html.
		The OCI Data Center Services (DCS) Program Management, Audit, Security, and Safety (PASS) team performs an assessment of data center and PoP site control environments, including physical security controls and environmental safeguards, prior to the data center hosting production traffic (go-live) and then thereafter in accordance with the schedule defined in the Data Center Assessment Program. The Data Center Assessment Program is completed through multifaceted review and analysis techniques to comprehensively evaluate the effectiveness of controls at the data centers. This involves artifact and evidence collection and review, on-site observation, and interviews with data center personnel.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
		Evidence collection includes the review of data center attestation reports, or internationally recognized certifications, by OCI. In the event a data center does not have an attestation report or internationally recognized certification, OCI performs an on-site assessment of the site's control environment, in accordance with the schedule defined in the Data Center Assessment Program. On-site data center observations include the following areas if applicable to the site: • External areas including parameters, parking lots, and outside equipment storage • Reception and lobby areas, office spaces, and conference rooms • Data halls • Oracle cages and suites • Generators, batteries, fuel storage, and heating, ventilation, and air conditioning (HVAC) equipment • Delivery and staging areas • Loading docks
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	The goal is to balance prevention, detection, protection, and response, while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. The OCI Data Center Services (DCS) Program Management, Audit, Security, and Safety (PASS) team performs an assessment of data center and PoP site control environments, including physical security controls and environmental safeguards, prior to the data center hosting production traffic (go-live) and then thereafter in accordance with the schedule defined in the Data Center Assessment Program. The Data Center Assessment Program is completed through multifaceted review and analysis techniques to comprehensively evaluate the effectiveness of controls at the data centers. This involves artifact and evidence collection and review, on-site observation, and interviews with data center personnel. Evidence collection includes the review of data center attestation reports, or internationally recognized certifications, by OCI. In the event a data center does not have an attestation report or internationally recognized certification, OCI performs an on-site assessment of the site's control environment, in accordance with the schedule defined in the Data Center Assessment Program. On-site data center observations include the following areas if applicable to the site: • External areas including parameters, parking lots, and outside equipment storage • Reception and lobby areas, office spaces, and conference rooms • Data halls • Oracle cages and suites • Generators, batteries, fuel storage, and heating, ventilation, and air conditioning (HVAC) equipment • Delivery and staging areas

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
		• Loading docks
DCS-08.1	Is equipment identification used as a method for connection authentication?	The Oracle Cloud Network Access (OCNA) VPN that is used by OCI staff to connect to OCI's infrastructure uses both machine certificates and other identifiers to validate that the device is Oracle owned and provisioned before allowing access to OCI resources. Access to production assets is managed through bastion servers and access to both the bastion servers and network assets are managed through a central permissions system. Access and activity on the bastion servers are logged and monitored, per Oracle policy.
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Oracle has implemented the following physical access protocols: • Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors. • Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors. Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises. Visitors are required to sign a visitor's register, be escorted or observed when they are on Oracle premises, and be bound by the terms of a confidentiality agreement with Oracle. Security monitors the possession of keys or access cards and the ability to access facilities. Staff leaving Oracle's employment must return keys and cards, and key and cards are deactivated upon termination. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Oracle use a mixture of 24/7 onsite security officers or patrol officers, depending on the risk or protection level of the facility. In all cases, officers are responsible for patrols, alarm response, and recording of security incidents. Oracle has implemented centrally managed electronic access control systems with integrated intruder alarm capability. The access logs are kept for a minimum of 6 months. The retention period for CCTV monitoring and recording ranges from 30 to 90 days minimum, depending on the facility's functions and risk level. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Personnel are trained in incident response and escalation procedures to address security and availability events that may arise. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Data centers that host 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 that house OCI 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 incident response and escalation procedures to address security and availability events that may arise. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	See DCS-12.1.
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	See DCS-12.1.
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	See DCS-12.1.

Control Domain: Data Security & Privacy Lifecycle

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Oracle's information-asset classification determines corporate data-security requirements for Oracle-managed systems. Oracle policies provide global guidance for appropriate controls designed to protect corporate, cloud, and customer data in accordance with the data classification. For more information, see oracle.com/corporate/security-practices/corporate/data-protection/.
		OCI has designed and implemented a set of robust standards that outline detailed requirements for various processes undertaken and managed by Oracle personnel, and provides direction for all activities related to OCI services and operations. The OCI Cloud Compliance Standard for Information Security establishes procedures to protect data in and about OCI.
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address data security and privacy) are reviewed annually and updated as needed.
		OCI Cloud Controls and Standards are reviewed at least annually, and updated as needed.
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Oracle's Media Sanitation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information that is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. For more information, see oracle.com/corporate/security-practices/corporate/data-protection/.
		OCI services rigorously sanitize and dispose of media that is no longer required, becomes unusable, is outside the Oracle retention schedule, or is going to be reused by implementing reviews, approvals, tracking, and documentation. OCI bare metal provisioning wipes flash-based storage systems in accordance with NIST 800-88 prior to release or disposal.
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	OCI maintains an inventory of sensitive production data, including production code and inventory assets.
DSP-04.1	Is data classified according to type and sensitivity levels?	Oracle categorizes information into four classes: Public, Internal, Restricted, and Highly Restricted. Each classification requires corresponding levels of security controls, such as encryption requirements for non-public data. For more information, see oracle.com/corporate/security-practices/corporate/information-assets-classification.html.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Network architecture diagrams identify environments and data flows between them.
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Network architecture diagrams are reviewed at least annually. System and network changes go through change management, as well as security review, and updates to diagrams are made, as needed.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Oracle's Information Systems Asset Inventory Policy requires that Lines of Business (LOBs) maintain accurate and comprehensive inventories of information systems, hardware systems, and software systems that hold critical and highly critical information assets in OCI. The OCI Cloud Compliance Standard for Asset Management describes the procedures for maintaining an accurate inventory of OCI assets throughout their life cycles, including hardware, software, and data.
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	See DSP-06.1.
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	The Corporate Security Solution Assurance Process (CSSAP) is followed for existing OCI services prior to implementing new features. Services must successfully complete the Oracle Release Management (ORM) process, which includes the CSSAP, prior to general availability. Services must successfully complete the Customer Readiness Program Process prior to inclusion in compliance assessments. This process requires security and privacy reviews performed by OCI Release Management, Compliance Onboarding, Privacy, Enterprise Risk Management, Resilience and Crisis Management, and if applicable, Public Sector Compliance Assurance.
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	See DSP-07.1.
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	See the Oracle Services Privacy Policy at oracle.com/legal/privacy/services-privacy-policy.html. See DSP-07.1.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
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?	See the Oracle Services Privacy Policy at oracle.com/legal/privacy/services-privacy-policy.html. Oracle provides customers with information and assistance reasonably necessary to conduct their own data protection impact assessment, by sharing security, privacy, and regulatory compliance-related materials in one of the following ways: • Through My Oracle Support, Document ID 111.1, or another applicable primary support tool provided for OCI services • Upon request, if such access to My Oracle Support (or other primary support tool) is not available
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)?	The standards set forth the requirements for the management of encryption keys. The standards and processes include security requirements for key creation, use, storage, and protection. In accordance with the OCI Cloud Compliance Standard for Encryption, which is supported by the OCI Cloud Infrastructure Standard Cryptography, OCI Vault provides the ability to create master encryption keys and data encryption keys, rotate keys to generate new cryptographic material, enable or disable keys for use in cryptographic operations, assign keys to resources, and use keys for encryption and decryption. Customers are responsible for establishing a geographic location (also referred to as a “home region”) in which to initially locate their tenancy. Customers’ data stays within this region unless they choose to move data outside the region. Customers are responsible for designing, developing, testing, implementing, operating, and maintaining administrative and technical safeguards to prevent or detect unauthorized access, use, and disclosure during input, processing, retention, output, and disposition of data to, within, or from their applications.
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)?	Customers are responsible for defining, implementing, and evaluating processes, procedures, and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
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)?	See the Oracle Services Privacy Policy at oracle.com/legal/privacy/services-privacy-policy.html. Customers are responsible for defining, implementing, and evaluating processes, procedures, and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.
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)?	Oracle complies with all applicable laws and regulations. For more information, see oracle.com/legal/privacy/. Customers are responsible for defining, implementing, and evaluating processes, procedures, and technical measures for the transfer and subprocessing of personal data within the service supply chain, according to any applicable laws and regulations.
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?	The Oracle Services Privacy Policy covers the privacy practices that Oracle Corporation and its subsidiaries and affiliates employ when providing support, consulting, cloud, or other services to its customers. Oracle established this privacy policy to clarify that the use of information to which it may be provided access in order to provide services is more limited than the use of information covered by Oracle's general privacy policy. See oracle.com/legal/privacy/services-privacy-policy.html. Customers are responsible for designing, developing, testing, implementing, operating, and maintaining administrative and technical safeguards to prevent or detect unauthorized access, use, and disclosure during input, processing, retention, output, and disposition of data to, within, or from their applications.
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Not applicable. OCI does not allow production data to be used in non-production environments.
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	The OCI Cloud Standard for Information Security defines the procedures for data storage and retention, in accordance with applicable Oracle policies, including the Oracle Services Privacy Policy. See oracle.com/legal/privacy/services-privacy-policy.html. Customers are responsible for defining, implementing, and evaluating processes, procedures, and technical measures to ensure their own data retention, archiving, and deletion practices are in accordance with application laws and regulations.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	The Corporate Security Solution Assurance Process (CSSAP) is followed for existing services prior to implementing new features. Services must successfully complete the Oracle Release Management (ORM) process, which includes the CSSAP, prior to general availability. The Oracle Acceptable Use Policy for Systems and Resources is designed to help Oracle protect the security and integrity of information and Oracle systems and resources. It provides guidance to employees, suppliers, contractors, and partners on how they may and may not use systems and resources while performing their job. OCI services must successfully complete the Customer Readiness Program Process prior to inclusion in compliance assessments. This process requires security and privacy reviews performed by OCI Release Management, Compliance Onboarding, Privacy, Enterprise Risk Management, Resilience and Crisis Management, and if applicable, Public Sector Compliance Assurance.
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	The Oracle Third-Party Information Access Request Policy provides the requirements for responding to requests for access to confidential information from third parties, evaluating whether the access requests are legally mandatory, and determining appropriate actions including any required notices or disclosures to the public, customers, affected individuals, or law enforcement authorities. For more information, see the Data Processing Agreement for Oracle Services at oracle.com/contracts/cloud-services/. Customers are responsible for designing, developing, testing, implementing, operating, and maintaining administrative and technical safeguards to prevent or detect unauthorized access, use, and disclosure during input, processing, retention, output, and disposition of data to, within, or from their applications.
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	In accordance with the terms of the Data Processing Agreement for Oracle Services, Oracle informs customers of requests to provide personal information, and uses reasonable efforts to redirect the authority to the customers, unless otherwise required by law. See oracle.com/contracts/cloud-services/.
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?	The Oracle Information Systems Inventory Policy requires an accurate inventory of all information systems and devices that hold critical and highly critical information assets throughout their life cycle through an approved inventory system. This policy defines required identifying attributes to be recorded for server hardware, software, and data held on information systems, and information needed for disaster recovery and business continuity purposes. Customers select the data region in which to locate their OCI tenancy, and Oracle does not move their content unless initiated by the customer.

Control Domain: Governance, Risk & Compliance

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Global Information Security (GIS) defines policies for the management of information security across Oracle. Additionally, GIS sets direction and provides advice to help protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners, and employees. GIS also coordinates the reporting of information security risk to senior leadership such as the Oracle Security Oversight Committee and Board of Directors. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle. For more information, see oracle.com/corporate/security-practices/corporate/governance/global-information-security.html.
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address governance, risk, and compliance) are reviewed annually and updated as needed. OCI Cloud Compliance Standards are reviewed and updated at least annually, or more often as new technology and other changes dictate.
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Oracle has an established, formal, documented, and leadership-sponsored enterprise risk management program that includes policies that direct Oracle LOBs to have procedures and standards for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks. Corporate Security Architecture manages a cross-organization working group focused on security architecture (including a policy for the management of security risks), with the goal of collaboratively guiding security for Oracle cloud services. Participation includes members from Oracle cloud service development, operations, and governance teams. Oracle Privacy and Security Legal manages the cross-organization oversight of privacy risks. For more information, see oracle.com/legal/privacy/. The Chief Corporate Architect, who reports directly to the Executive Chairman and Chief Technology Officer (CTO), is one of the directors of the Oracle Security Oversight Committee (OSOC). The Chief Corporate Architect manages the Corporate Security departments, which guide security controls at Oracle. These departments drive the corporate security programs, define corporate security policies, and provide global oversight for Oracle's security policies and requirements.
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Oracle Corporate Security policies are reviewed annually and updated as needed. OCI Cloud Compliance Standards are reviewed and updated at least annually, or more often as new technology and other changes dictate.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Global Information Security (GIS) manages a security exception management process to review deviations from Corporate information security policies.
		The OCI Compliance Exceptions program is established to document, review, approve, and remediate gaps in OCI's compliance posture. Approved exceptions are temporary deviations from Oracle policies and standards and are tracked to remediation.
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Oracle Global Information Security manages the Information Security Manager (ISM) Program. Information Security Managers serve as security advocates within their respective LOBs to increase awareness of and compliance with Oracle's security policies, processes, standards, and initiatives.The OCI Compliance Standards program documents processes and procedures to ensure that OCI personnel and services adhere to compliance obliations across a variety of domains.
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, security, operation, maintenance, and monitoring of OCI services. For more information, see the Hosting and Delivery Policies at oracle.com/corporate/contracts/cloud-services/.
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	OCI reviews internal controls and Cloud Compliance Standards identified to meet the requirements of the control framework, relevant standards, and regulatory, legal, and statutory requirements at least annually.
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Oracle is a member of the Information Technology-Sharing and Analysis Center (IT-ISAC) organization. See it-isac.org/home. In addition, the OCI Security team subscribes to or engages other relevant security issue disclosure channels.

Control Domain: Human Resource Security

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	In accordance with Oracle policy, background checks are required for individuals being considered for employment. For more information, see oracle.com/corporate/careers/background-check.html. The Oracle Recruiting Privacy Policy (Privacy Policy) describes the privacy and security practices that Oracle Corporation, and its subsidiaries and affiliates employ when collecting, using, and handling (processing) personal information about individuals in connection with online and offline recruitment activities. It also explains the choices that individuals have in relation to these processing activities.
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	In accordance with Oracle policy, background checks are required for individuals being considered for employment. For background check information organized by local law and regulation, see oracle.com/corporate/careers/background-check.html.
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address candidate and employee background checks) are reviewed annually and updated as needed.
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 employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. For more information, see oracle.com/corporate/security-practices/corporate/human-resources-security.html.
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as needed. Oracle has formal requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, internet access, enterprise data, customer data, and other company resources available to Oracle employees, contractors, and visitors. For more information, see oracle.com/corporate/security-practices/corporate/communications-operations-management.html.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy. For more information, see oracle.com/corporate/security-practices/corporate/human-resources-security.html. The Oracle Information Protection Policy sets forth the requirements for classifying and handling confidential information, including requirements for visual disclosure.
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	The Oracle Endpoint Device Securtiy Policy sets physical and logical security guidelines for employee endpoint devices. Oracle corporate security policies are reviewed annually and updated as needed.
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?	Oracle Global Information Security (GIS) defines policies for the management of information security across Oracle. For more information, see oracle.com/corporate/security-practices/corporate/governance/global-information-security.html. Data centers that host 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. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html. OCI's Cloud Compliance Standard for Data Protection Assurance and Safeguarding describe the procedures for protecting data in and about OCI, including the transfer, storage, retention, and protection of data.
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Oracle Corporate Security policies (including polices intended to protect information accessed, processed, or stored at remote sites and locations) are reviewed annually and updated as needed. See HRS-04.1.
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see oracle.com/corporate/security-practices/corporate/access-control.html.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see oracle.com/corporate/security-practices/corporate/access-control.html.
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	See HRS-02.1.
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	See HRS-02.1.
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Oracle's information asset classification determines corporate data-security requirements for Oracle-managed systems. Oracle policies provide global guidance for appropriate controls designed to protect corporate, cloud, and customer data in accordance with data classification. Oracle's corporate security controls can be grouped into three categories: administrative, physical, and technical security controls. • Administrative controls include logical access control and human resource processes. • Physical controls are designed to prevent unauthorized physical access to servers and data-processing environments. • Technical controls include secure configurations and encryption for data at rest and in transit. For more information, see oracle.com/corporate/security-practices/corporate/data-protection/. The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. For more information, see oracle.com/corporate/security-practices/corporate/access-control.html.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
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?	See HRS-02.1.
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Security reviews, assessments, and audits are conducted periodically to confirm compliance with Oracle information-security policies, procedures, and practices. Employees who fail to comply with these policies, procedures, and guidelines may be subject to disciplinary action up to and including termination of employment. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy. For more information, see oracle.com/corporate/security-practices/corporate/human-resources-security.html.
HRS-11.2	Are regular security awareness training updates provided?	See HRS-11.1.
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	See HRS-11.1.
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	See HRS-11.1.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	See HRS-11.1.

Control Domain: Identity & Access Management

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. For more information, see oracle.com/corpoate/security-practices/corporate/access-control.html.
		The OCI Cloud Compliance Standard for Access Control describe logical access control requirements for systems in the OCI environment, including authentication, authorization, access approval, provisioning, and revocation. OCI IAM lets customers control who has access to their cloud resources. Customers can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm.
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including policies applicable to IAM) are reviewed annually and updated as needed.
		The Cloud Compliance Standard for Access Controls is reviewed no less than annually and updated as needed.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Oracle has strong password policies (including length and complexity requirements) for Oracle network, operating system, email, database, and other accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. Identity management systems are required to comply with Corporate Security Architecture requirements. For more information, see oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.
		OCI's Cloud Compliance Standard for Access Control requires that OCI services and systems adhere to the Oracle Password Policy.
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including password complexity and protection requirements) are reviewed annually and updated as needed.
		OCI Cloud Compliance Standards are reviewed and updated at least annually or more often as new technology and other changes dictate.
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Logical access controls for applications and systems must provide identification, authentication, authorization, accountability, and auditing functionality. Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. For more information, see oracle.com/corporate/security-practices/corporate/access-control.html.
		Access to OCI user groups and resources are approved, stored, and reviewed in a permission management system prior to access provisioning. OCI managers and asset owners audit accesses and permissions at least quarterly to validate users' continued need for access and privileges.
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Operations are organized into functional groups, where each function is performed by separate groups of employees. Examples of functional groups include developers, database administrators, system administrators, and network engineers. For more information, see oracle.com/corporate/security-practices/corporate/communications-operations-management.html. Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. For more information, see oracle.com/corporate/security-practices/corporate/access-control.html.
		The Cloud Compliance Standard for Access Control defines authorization requirements for OCI services. OCI services must actively manage authorization privileges based on the concept of least privilege, dual authorization of a verified business justification, and a separation of duties between production or operation and management activities.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Authorization depends on successful authentication because controlling access to specific resources depends on establishing an entity's or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • **Need to know**: Does the user require this access for their job function? • **Segregation of duties**: Will the access result in a conflict of interest? • **Least privilege**: Is access restricted to only those resources and information required for a legitimate business purpose? For more information, see oracle.com/corporate/security-practices/corporate/access-control.html.
		See IAM-4.01.
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. Metrics are considered Oracle Confidential. For more information, see oracle.com/corporate/security-practices/corporate/access-control.html.
		The OCI Cloud Compliance Standard for Access Control requires that OCI services maintain an audit trail when a user is provisioned, a privilege is granted, an application transaction is performed, or access to the application is modified or terminated.
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see oracle.com/corporate/security-practices/corporate/access-control.html.
		The OCI Cloud Compliance Standard for Access Control describes account disablement procedures for OCI services, including timely deprovisioning and modification of user access.
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	The OCI Cloud Compliance Standard for Access Control requires that OCI managers and asset owners must audit accesses and permissions at least quarterly to validate users' continued need for accesses and privileges.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	See IAM-05.1.
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	See IAM-05.1 and IAM-08.1.
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	See IAM-08.1.
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	Not applicable in OCI. Customers are responsible for defining their own roles for access in their environment.
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	The OCI Cloud Compliance Standard for Access Control requires that OCI services maintain an audit trail when a user is provisioned, a privilege is granted, an application transaction is performed, or access to the application is modified or terminated. Audit logs are stored using a high-availability system that is protected to ensure and validate integrity. The OCI Cloud Standard for Logging and Alerting specifies that OCI services must restrict access to the security information and event monitoring (SIEM) application to designated security staff, who have read-only capability.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	See IAM-12.1.
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	The Logical Access Controls Policy and OCI Cloud Compliance Standard for Access Control describe logical access control requirements for all Oracle systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined users with access to Oracle systems that are not internet-facing, publicly accessible systems. For more details, see IAM-06.1.
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Access to OCI services supporting the System requires multifactor authentication, a VPN connection, and an SSH connection with a user account and password or private key.
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	See IAM-14.1. Customers are responsible for implementing digital certificates in their environment. For more information, see docs.oracle.com/en/cloud/paas/identity-cloud/uaids/digital-certificates.html and oracle.com/security/cloud-security/ssl-tls-certificates/faq/.
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	The OCI Cloud Compliance Standard for Access Control requires that OCI services and systems follow the Oracle Password Policy and Guidelines for Password Management.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	See IAM-12.1.

Control Domain: Interoperability & Portability

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	OCI follows established corporate information security policies and OCI Cloud Compliance Standards, including those relevant to application services and APIs.
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	OCI follows established corporate information security policies and OCI Cloud Compliance Standards, including those relevant to information processing interoperability. OCI's multicloud solutions allow customers to operate and collaborate across different cloud platforms. For more information, see oracle.com/cloud/multicloud/.
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	OCI follows established corporate policies and procedures including those relevant to application development portability. Customers can use OCI Data Transfer to export data currently residing in OCI to their data center offline. For more information, see docs.oracle.com/iaas/Content/File/Tasks/managingsnapshots.htm. Customers retain all rights in and to the content they place in OCI. For a period of 60 days upon termination of Oracle Cloud Services, Oracle will make available, via secure protocols and in a structured, machine-readable form, the customer's content residing in OCI, or keep the service accessible, for the purpose of data retrieval. For more information, see Oracle Cloud Service Contracts at oracle.com/contracts/cloud-services/.
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	OCI has established Service Level Agreements (SLAs) for availability, management, and performance of its services. For additional information, see Section 3: Service Level Objective Policy of the Cloud Services Hosting and Delivery Policies at oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	OCI follows established corporate policies and procedures, which are reviewed annually and updated as needed.
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Customer API calls, including actions from the customer administration Console, are logged and retained for 90 days and cannot be deleted by customers. Customers may request an export of their logs by contacting Oracle and submitting a service request in MyOracle Support (MOS).
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Secure file transfer functionality is built on commonly used network access storage platforms and uses secured protocols for transfer. The functionality can be used to upload files to a secured location, most commonly for data import and export on the OCI service, or downloading files at service termination. Secured data transfer between on-premises and a customer's tenancy, between a customer's environments built within their tenancy, and between a customer's tenancy and other environments at other cloud providers, can be accomplished through a combination of industry standardized network protocols and the customer's design of their private networks.
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Oracle Cloud Hosting and Delivery Policies describe the procedures for customers to retrieve their content upon contract termination, including the data format, duration, scope, and data deletion policy. See oracle.com/contracts/cloud-services/.

Control Domain: Infrastructure & Virtualization Services

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	OCI follows established corporate policies, including those that address infrastructure and virtualization. The Cloud Compliance Standard for Service Security defines the requirements for OCI developers to follow to ensure secure coding guidelines, assess applications for vulnerabilities, and remediate critical vulnerabilities before production deployment. Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers or delivered through Oracle Cloud. For more information, see oracle.com/corporate/security-practices/assurance/.
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	OCI follows established corporate policies, which are reviewed at least annually, and updated as needed. The Cloud Compliance Standard for Service Security, for related OCI controls are reviewed no less than annually, and updated as needed.
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	OCI maintains processes to monitor infrastructure capacity and creates capacity forecasts at least quarterly for critical system components. Oracle uses a variety of software tools to monitor the following items: • The availability and performance of a customer's production services environment • The operation of infrastructure and network components This information is used to verify that OCI is meeting all of its requirements.
IVS-03.1	Are communications between environments monitored?	Oracle employs intrusion-detection systems within the Oracle intranet to provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle uses a network-based monitoring approach to detect attacks on open firewall ports within Oracle's intranet. Events are analyzed using signature detection, which is a pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to Oracle's IT security for review and response to potential threats. The OCI network is segregated to separate customer traffic from management traffic. Network filtering is designed to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted platform components. OCI has implemented load balancers and traffic filters to control the flow of external traffic to OCI components. OCI has established automated controls to monitor and detect internally initiated denial of service (DDoS) attacks, traffic steering, and sinkholing.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IVS-03.2	Are communications between environments encrypted?	Connections to the customer administration console, APIs, or host region must be made over an encrypted protocol using HTTPS and TLS 1.2 or above. Access to customer virtual cloud networks is controlled by a combination of security lists and routing tables configured by the customer. Logical segmentation between cloud customers on the network level is implemented to ensure confidentiality and integrity of data transmitted. Access control lists are configured in each region to deny all traffic that is not explicitly authorized. OCI performs a review of network access control lists, including ports, semiannually.
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	See IVS-03.2
IVS-03.4	Are network configurations reviewed at least annually?	OCI performs a review of network access control lists, including ports, semiannually.
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	OCI maintains network plans and changes to the plans need to be approved.
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Oracle employs standardized system hardening practices across OCI devices. This includes alignment monitoring with base images and baselines, restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, and logging. Baseline configurations come with vendor defaults disabled, and only necessary ports and protocols enabled. System configurations have a baseline, are managed against the baseline, and include all necessary service configurations within the image. Customers then have the opportunity to enable configurations that their tenancies need to operate. Oracle Cloud Marketplace currently offers customers the ability to use Windows, Ubuntu, CentOS, and Oracle Linux images configured with the CIS Security Benchmarks recommendations.
IVS-05.1	Are production and non-production environments separated?	Development and production regions are separated to reduce the risks of unauthorized access or changes to the operational environment.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Access to customer virtual cloud networks is controlled by a combination of security lists and routing tables configured by the customer. Logical segmentation between cloud customers on the network level is implemented to ensure confidentiality and integrity of data transmitted.
IVS-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?	See IVS-04.1. Additionally, the FastConnect service allows customers to establish a private connection to OCI. See docs.oracle.com/en-us/iaas/Content/Network/Concepts/fastconnect.htm#FastConnect. The Data Transfer service uses AES 256 for encryption of data at rest. See docs.oracle.com/en-us/iaas/Content/DataTransfer/home.htm.
IVS-08.1	Are high-risk environments identified and documented?	Network architecture diagrams reflect network segments with additional compliance considerations, as appropriate.
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Oracle employs intrusion-detection systems within the Oracle intranet to provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle uses a network-based monitoring approach to detect attacks on open firewall ports within Oracle's intranet. The OCI network is segregated to separate customer traffic from management traffic. Network filtering is designed to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted platform components. OCI has implemented load balancers and traffic filters to control the flow of external traffic to OCI components. OCI has established automated controls to monitor and detect internally initiated denial of service (DDoS) attacks.

Control Domain: Logging & Monitoring

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Logging and monitoring policies are established, documented, approved, communicated, applied, evaluated, and maintained by Oracle Corporate Security. Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted or failing to record events, or logs being overwritten. For more information, see oracle.com/corporate/security-practices/corporate/communications-operations-management.html. The OCI Cloud Compliance Standard for Logging and Alerting specifies the requirements for the collection, maintenance, and review of audit logs.
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address logging and monitoring) are reviewed annually and updated as needed. Oracle Cloud Compliance Standards are reviewed and updated no less than annually.
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	The OCI Cloud Compliance Standard for Logging and Alerting specifies the requirements for the secure collection, maintenance, and review of audit logs. Customers can configure OCI Audit to retain logs up to 365 days. Customers can also store their own audit logs on OCI Object Storage or Archive Storage.
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	OCI has deployed a security information and event monitoring (SIEM) solution in each region. It ingests and stores security-related logs and alerts from networking devices, hosts, and other components within the infrastructure. Access to logs is controlled in a permissions system and is restricted to authorized personnel. OCI's Detection and Response team (DART) monitors the SIEM for event correlations and other relevant detection scenarios on a 24/7 basis to defend and protect against unauthorized intrusions and activity in the production environment.
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	See LOG-03.1.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	See LOG-03.1.
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	See LOG-03.1.
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	The Security Information and Event Monitoring (SIEM) tool is configured to review the telemetry against predefined rules. Security events detected generate an automated ticket with a severity rating and are tracked to resolution by the OCI Detection and Response Team.
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	The clocks of servers supporting services and bastion servers are synchronized through a Network Time Protocol (NTP) server, which uses the Global Positioning System (GPS) as its source.
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	The OCI Cloud Compliance Standard for Logging and Alerting specifies the requirements for the collection, maintenance, and review of audit logs.
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	OCI reviews internal controls and OCI Cloud Compliance Standards identified to meet the requirements of the control framework, relevant standards, and regulatory, legal, and statutory requirements at least annually. The OCI security teams are constantly updating security detections as the threat environment changes and new security risks emerge.
LOG-08.1	Are audit records generated, and do they contain relevant security information?	See LOG-03.1

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	The OCI Cloud Compliance Standard for Logging and Alerting describes multiple layers of security to protect logs from unauthorized access, modification, or deletion, including the following measures: • Restricting access to log configuration capabilities to individuals with privileged access • Encrypting log data in transit • Classifying log records in accordance with the Information Protection Policy • Continuously monitoring log data with automated tools
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	The OCI Cloud Compliance Standard for Encryption requires that monitoring of administrative key management operation logs and records is performed at defined intervals to detect incidents resulting in unauthorized access to or use of key material.
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	See LOG-10.1.
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Oracle employees and third-party contractors must have a business need to enter an OCI colocation facility and must receive prior approval. Doors between areas of differing security require authorized badge access, are monitored through logs and cameras, and are audited on a regular basis. OCI Data Center Services maintains access logs for all data center facility entrances and exits in accordance with Oracle's Information Management and Record Retention Policy.
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	The Security Information and Event Monitoring (SIEM) tool is configured to review the telemetry against predefined rules. Security events detected generate an automated ticket with a severity rating and are tracked to resolution by the OCI Detection and Response Team (DART). OCI Security and DART analyze audit processing failures on hosts and take appropriate actions to remediate issues.
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	See LOG-13.1.

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

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Policies and procedures for security incident management, e-discovery, and cloud forensics are established, documented, approved, communicated, applied, evaluated, and maintained with the oversight of Oracle Global Information Security (GIS). Oracle evaluates and responds to any event when Oracle suspects that Oracle-managed customer data has been unproperly handled or accessed. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the GIS organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LOBs). GIS defines roles and responsibilities for the incident response teams embedded within the LOBs. All LOBs must comply with GIS incident response guidance about detecting events and timely corrective actions. Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures that improve security posture and defense in depth. Formal procedures and systems are used within the LOBs to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary. For more information, see oracle.com/corporate/security-practices/corporate/security-incident-response.html. The Oracle Cloud Compliance Standard for Resilience and Crisis Management describes OCI's approach for coordinating, documenting, and improving actions for resilience, business continuity, disaster recovery, and incident response.
SEF-01.2	Are policies and procedures reviewed and updated annually?	Oracle Corporate Security policies and procedures that address security incident management, e-discovery, and cloud forensics are reviewed annually and updated as needed. OCI Cloud Compliance Standards are reviewed and updated no less than annually.
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	See SEF-01.1.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Oracle Corporate Security policies and procedures that address timely management of security incidents are reviewed annually and updated as needed.
		See SEF-01.1.
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LOBs). Corporate requirements for LOB incident-response programs and operational teams are defined per incident type: • Validating that an incident has occurred • Communicating with relevant parties and notifications • Preserving evidence • Documenting an incident itself and related response activities • Containing an incident • Addressing the root cause of an incident • Escalating an incident For more information, see oracle.com/corporate/security-practices/corporate/security-incident-response.html.
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	The Oracle's Lines of Business (LOBs) security incident response plans are updated as needed. For more information, see oracle.com/corporate/security-practices/corporate/security-incident-response.html.
		OCI's Detection and Response Team (DART) conducts security incident response exercises at least annually to identify potential impacts to customers and other business relationships that represent critical intrasupply chain business process dependencies. OCI exercises each service's Service Resiliency Plan (SRP) at least annually. OCI maintains a Business Impact Analysis (BIA) and Service Resiliency Plan (SRP) for each service. The plans are reviewed annually and have the following characteristics: • Include a defined purpose and scope, aligned with relevant dependencies • Are accessible to and understood by those who use them • Have an assigned owner and include documented roles and responsibilities • Include detailed recovery procedures and reference information and the method for plan invocation

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
SEF-05.1	Are information security incident metrics established and monitored?	Information security incident metrics are established and monitored with oversight by Oracle Global Information Security.
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	See SEF-01.1.
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	If Oracle determines that a conformed security incident involving personal information processed by Oracle has occurred, Oracle promptly notifies impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared. Incident history is also Oracle Confidential and is not shared externally.
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	See SEF 01.1. Oracle complies with applicable SLAs, laws, and regulations. For more information, see oracle.com/corporate/security-practices/corporate/security-incident-response.html.
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Oracle maintains points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

Control Domain: Supply Chain Management, Transparency & Accountability

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Managing security and privacy in the cloud is often a shared responsibility between the cloud customer and the cloud service provider. The distribution of responsibilities between the cloud service provider and customer also varies based on the nature of the cloud service (IaaS, PaaS, SaaS). Before deploying Oracle cloud services, Oracle strongly recommends that cloud customers formally analyze their cloud strategy to determine the suitability of using the applicable Oracle cloud services in light of their own legal and regulatory compliance obligations. Making this determination remains solely the responsibility of customers. For information about the Oracle Cloud Compliance Shared Management Model, see oracle.com/cloud/compliance/. Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers. Oracle suppliers are required to protect the data and assets Oracle entrusts to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when accessing Oracle or Oracle customer facilities, networks, or information systems; handling Oracle confidential information; or controlling custody of Oracle hardware assets. Suppliers are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards. For more information, see oracle.com/corporate/security-practices/corporate/supply-chain/.
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Oracle Cloud Hosting and Delivery Policies are reviewed no less than annually and are updated as needed. Customers can subscribe to policy update alerts at oracle.com/contracts/cloud-services/. OCI is designed based on a shared responsibility model in which both Oracle and customers are responsible for aspects of security, availability, and confidentiality. Details about the responsibilities of Oracle and customers (user entities) are documented in the Oracle Cloud Hosting and Delivery Policies at oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html. Additionally, Complementary User Entity Controls (CUECs) are documented in the OCI SOC 1 and SOC 2 Reports, which are reviewed, updated, and approved on a biannual basis.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	The Oracle Supplier Security Management Policy, which enforces the Oracle Supplier Information and Physical Security Standards, describes the shared security responsibilities of the Oracle suppliers. Oracle suppliers and partners are required to protect the data and assets that Oracle entrusts to them. The Supplier Information and Physical Security Standard details the security controls that Oracle's suppliers and partners are required to adopt when accessing Oracle or Oracle customer facilities, networks, or information systems; handling Oracle confidential information; or controlling custody of Oracle hardware assets. Suppliers and partners are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards. For more information, see oracle.com/corporate/security-practices/corporate/supply-chain/.
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	The Oracle supplier agreement template specifies supplier's responsibility to adhere to the Supplier Code of Ethics and Business Conduct and the Oracle Supplier Information and Phsyical Security Standards. For more information, see oracle.com/corporate/security-practices/corporate/supply-chain/.
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	The OCI CSA STAR CCM Report includes Complementary User Entity Controls (CUECs) that indicate which controls should be implemented by the user entities (customers).
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	See STA-03.1 and STA-04.1.
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	OCI controls and procedures are subject to internal audits no less than annually, and independent third-party assessments every six months, including the CSA STAR CCM v4 requirements. For more information, see oracle.com/corporate/cloud-compliance/.
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	OCI maintains an inventory of supply-chain relationships with colocation data center suppliers.
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Supplier risk is included in Oracle's Risk Management Program. OCI conducts periodic risk assessments of high-risk, third-party colocation providers.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Oracle has standard terms and conditions that govern the use of Cloud Services that are publicly available and indicate the date of the most recent update. During the customer order process, customers are required to acknowledge the Oracle Cloud Services Agreement, which outlines customer responsibilities and Oracle's responsibilities, objectives, and commitments. Amendments to the standard Oracle Cloud Services Agreement require advanced approval. For more information, see the Oracle Cloud Hosting and Delivery Policies at oracle.com/corporate/contracts/cloud-services/.
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Third-party supplier agreements, policies, and processes are reviewed no less than annually as part of the OCI SOC and ISO audit programs.
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Audits of OCI's internal controls are planned, approved, and communicated across the business. The scope of the audits includes reviewing the effectiveness of the implementation of security operations.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Oracle suppliers are required to protect the data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when accessing Oracle or Oracle customer facilities, networks, or information systems; handling Oracle confidential information; or controlling custody of Oracle hardware assets. Suppliers are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards. For more information, see oracle.com/corporate/security-practices/corporate/supply-chain/suppliers-partners.html.
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Oracle's Supplier Security Management Policy requires all LOBs that use third-party providers to maintain a program that manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual review, where appropriate per the risk to data confidentiality, availability, or integrity introduced by the way each particular supplier's goods or services are leveraged. For more information, see oracle.com/corporate/security-practices/corporate/supply-chain/.
		In accordance with the schedule defined in the Data Center Assessment Program, OCI periodically performs an assessment of in-scope data center and PoP site's control environments, including physical security controls, environmental safeguards, and media destruction. Identified issues are evaluated and tracked through resolution.
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	OCI reviews in-scope data center and PoP site's provider attestation reports, or internationally recognized certifications, at least annually. Identified issues are evaluated and tracked. If a site does not have an attestation report or internationally recognized certification, OCI performs an assessment annually of the site's control environment, including physical security controls and environmental safeguards.

Control Domain: Threat & Vulnerability Management

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	The Oracle Patching and Security Alerts Implementation Policy requires the deployment of the Oracle Critical Patch Update and Security Alert updates as well as associated recommendations. This policy also includes requirements for remediating vulnerabilities in non-Oracle technology using a risk-based approach. For more information, see oracle.com/corporate/security-practices/corporate/communications-operations-management.html and oracle.com/corporate/security-practices/assurance/vulnerability/.
		The OCI Cloud Compliance Standard for Vulnerability Management includes the processes, rules, and mechanisms used to prevent the introduction of vulnerabilities in the OCI environment and their remediation.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address threat and vulnerability management) are reviewed annually and updated as needed.
		OCI Cloud Compliance Standards are reviewed annually and updated as needed.
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops, and mobile devices. Additionally, all computers running a Windows operating system that holds Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to LOB management to verify deployment of device encryption for their organization. For more information, see oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html.
		Oracle's Server Security Policy requires endpoint protection to be installed and operational with up-to-date malware signatures on servers that are owned and managed by Oracle or third parties operating on Oracle's behalf. Oracle's Endpoint Device Security Policy establishes similar requirements for Oracle employee's user devices. These documents are evaluated and updated on an annual basis. OCI has established programs and procedures governing the implementation and upkeep of solutions providing such malware protection in this environment.
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address asset management and malware protection) are reviewed annually and updated as needed.
		Additionally, see TVM-02.1.
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	The Cloud Compliance Standard for Vulnerability Management includes the procedures, rules, and mechanisms to prevent exposure to, assess, and remediate vulnerabilities in the OCI environment. This includes procedures for assessing the vulnerability risk, based on the Common Vulnerability Scoring System (CVSS) Base Score, and implementing appropriate remediation timelines based on the severity level.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	The Cloud Compliance Standard for Vulnerability Management includes the procedures, rules, and mechanisms to prevent exposure to, assess, and remediate vulnerabilities in the OCI environment. OCI performs external vulnerability scans weekly. Identified vulnerabilities are investigated and tracked to resolution. OCI performs internal vulnerability scans weekly, which include the discovery of end-of-support systems. Identified vulnerabilities are investigated and tracked to resolution.
TVM-05.1	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 uses various technical measures to evaluate and identify updates for third-party and open-source libraries. Authenticated vulnerability scans of systems deployed into the environment as well as scans of predeployment system images have been implemented to identify such libraries and determine whether security fixes are needed. These programs are governed by corporate policies and business unit procedures that are evaluated on an annual basis.
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	A penetration test of the System is conducted by independent third parties at least annually.
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	OCI performs internal and external vulnerability scans at weekly.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Oracle uses the Common Vulnerability Scoring System (CVSS) to report the relative severity of security vulnerabilities when it discloses them. CVSS information is provided in the risk matrices published in Critical Patch Update and Security Alert Advisories as individual metrics that cover the technical aspects of the vulnerabilities, such as the preconditions required for successful exploitation. Common Vulnerabilities and Exposures (CVE) numbers are used by Oracle to identify the vulnerabilities listed in the risk matrices in Critical Patch Update and Security Alert advisories. CVE numbers are unique, common identifiers for publicly known information about security vulnerabilities. The CVE program is cosponsored by the office of Cybersecurity and Communications at the US Department of Homeland Security and is managed by MITRE corporation. Oracle is a CVE Numbering Authority (CNA), which means that Oracle can issue CVE numbers for vulnerabilities in its products. For more information, see oracle.com/corporate/security-practices/assurance/vulnerability/. Oracle's Information Security Policy, which applies to all users and information systems within Oracle, requires that information security controls be aligned with ISO 27002. This includes the management of technical vulnerabilities.
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	OCI uses an internally developed application to aggregate security findings from multiple sources (including vulnerability scans) and assign findings to the appropriate service team. This application allows service teams to manage their findings and integrate with ticketing systems for automated queuing of remediation work, including notification and automatic escalations as necessary. The system also provides a summary of remediation work across the organization and is used to drive day-to-day vulnerability management efforts.
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	See TVM-04.1.

Control Domain: Universal Endpoint Management

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Oracle Endpoint Device Security Policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops, and mobile devices. Desktops and laptops that receive, store, access, transmit, or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to LOB management to verify deployment of device encryption for their organization. Oracle employees are required to comply with email instructions from Oracle Information Technology (OIT) and are responsible for promptly reporting to the Oracle employee help desk any virus or suspected virus infection that cannot be resolved by antivirus software. Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. For more information, see oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html.
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address universal endpoint management) are reviewed annually and updated as needed. OCI follows the Oracle Endpoint Device Security policy, which is reviewed no less than annually and is updated as needed.
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?	See UEM-01.1. This list is approved by Oracle Corporate Architecture and maintained by OIT.
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	See UEM-01.1. Endpoint validation is performed by automation approved by Oracle Corporate Architecture and maintained by OIT. Oracle-managed endpoints are tracked centrally in inventory systems. Business-critical software installed on the endpoints is checked regularly, and software update alerts are issued to users to meet compliance requirements according to Oracle policies and standards. When an endpoint is out of compliance, an email notification is sent to the user and management to make the necessary updates.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Oracle's Information Systems Asset Inventory Policy requires that LOBs maintain accurate and comprehensive inventories of information systems, hardware, and software Oracle policy specifies the data (or fields) that must be maintained about these information systems in the approved system inventory. For more information, see oracle.com/corporate/security-practices/corporate/information-assets-classification.html.
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?	Desktops and laptops that receive, store, access, transmit, or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to LOB management to verify deployment of device encryption for their organization. To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full disk encryption software on their laptops and desktops, except where approved for justifiable business purposes. Data on the disk can be accessed only through the use of a private key stored as a password-protected file on the disk. A preboot login manager allows authorized users to log in to unlock the key, boot the operating system, and access the data. For more information, see oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html.
		Dynamic Access Policies are configured to validate the following items on endpoints before granting access to the infrastructure supporting OCI services: • Devices are running up-to-date software, including anti-malware software and compliance monitoring tools that validate endpoint encryption. • A local firewall is installed. The Oracle Cloud Network Access (OCNA) VPN is configured to time out after 24 hours of connectivity. Devices that support Windows and Mac operating systems are configured to lock automatically after 15 minutes of inactivity. Oracle managed endpoints are tracked centrally in inventory systems. Business-critical software installed on the endpoints is checked regularly, and software update alerts are issued to users to meet compliance requirements according to Oracle policies and standards. When an endpoint is out of compliance, an email notification is sent to the user and management to make the necessary updates.
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	See UEM-05.1.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	The Oracle Information Technology (OIT) organization keeps antivirus products and Windows Server Update Services (WSUS) up-to-date with virus definitions and security updates. OIT is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. OIT provides automation to verify antivirus configuration. Oracle employees are required to comply with email instructions from OIT and are responsible for promptly reporting to the Oracle employee help desk any virus or suspected virus infection that cannot be resolved by antivirus software. Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. For more information, see oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html.
		Changes to OCI managed endpoint operating systems follow the OCI Cloud Compliance Standard for Change Management.
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	See UEM-05.1.
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Antivirus software must be scheduled to perform daily threat definition updates and virus scans. For more information, see oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html.
UEM-10.1	Are software firewalls configured on managed endpoints?	See UEM-09.1.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Dynamic Access Policies are configured to validate the following items on endpoints before granting access to the infrastructure supporting OCI services: • Devices are running up-to-date software including anti-malware software and compliance monitoring tools that validate endpoint encryption. • A local firewall is installed. The Oracle Cloud Network Access (OCNA) VPN is configured to time out after 24 hours of connectivity. Devices that support Windows and Mac operating systems are configured to lock automatically after 15 minutes of inactivity. Oracle managed endpoints are tracked centrally in inventory systems. Business-critical software installed on the endpoints is checked regularly, and software update alerts are issued to users to meet compliance requirements according to Oracle policies and standards. When an endpoint is out of compliance, an email notification is sent to the user and management to make the necessary updates. The Security Information and Event Monitoring (SIEM) tool is configured to review the telemetry against predefined rules including detections related to data loss prevention. Security events detected generate an automated ticket with a severity rating and are tracked to resolution by the OCI Detection and Response Team (DART). Customers are responsible for maintaining all required policies and procedures relevant to their own environment. Customers can leverage endpoint protection in the Oracle Cloud Marketplace. See cloudmarketplace.oracle.com/marketplace/en_US/homePage.jspx.
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Oracle managed endpoints are tracked centrally in inventory systems. Business-critical software installed on the endpoints is checked regularly, and software update alerts are issued to users to meet compliance requirements according to Oracle policies and standards. When an endpoint is out of compliance, an email notification is sent to the user and management to make the necessary updates. Oracle's IAM can restrict access based on IP address.
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	OCI managed endpoint devices have remote wipe capability enabled.

QUESTION ID	CONSENSUS ASSESSMENT QUESTION	ORACLE RESPONSE
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Oracle has formal requirements for its suppliers to confirm that they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when they are performing the following actions: • Accessing Oracle and Oracle customers' facilities, networks, or information systems • Handling Oracle confidential information and Oracle hardware assets placed in their custody In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. For more information, see oracle.com/corporate/security-practices/corporate/supply-chain/. Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile-device security and good practices.

CONNECT WITH US

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

 blogs.oracle.com  facebook.com/oracle  twitter.com/oracle

CAIQ for <Product ZZZZ>