ORACLE

# Consensus Assessment Initiative Questionnaire (CAIQ) v4 for Oracle SaaS Cloud Applications

April 2025 | Version 1.0

## PURPOSE STATEMENT

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

The answers contained in this CAIQ version 4.0 are related to specific Oracle cloud offerings as listed in the "Oracle cloud services in Scope" section below.

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

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

## DISCLAIMER

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

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

## ORACLE CLOUD SERVICES IN SCOPE

This document applies to Oracle SaaS Cloud Applications delivered as a SaaS service deployed on Oracle Public Cloud Regions as listed on this page: https://docs.oracle.com/en/cloud/saas/index.html.

Please note that Industry Applications are excluded from the scope of this document.

# CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ) VERSION 4

## Control Domain: Audit & Assurance

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **A&A-01.1** | Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained? | Oracle's Business Assessment & Audit (BA&A) is an independent global audit organization which performs global 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 (LOB) and business units. Any key risks or control gaps identified by BA&A during these reviews are tracked through remediation. These reviews, identified risks, or control gaps are confidential and shared with executive leadership and Oracle's Board of Directors.<br><br>The audit rights of customers for whom Oracle processes data are described in your agreement. For more information, see https://www.oracle.com/contracts/cloud-services/. |
| | | Oracle SaaS Cloud Compliance maintains a SaaS Compliance Program. It provides the audit process for SaaS Cloud Applications in accordance with the SaaS Engineering Compliance Program and SaaS Cloud Security Organization Standard to maintain internal and external audit plans. Each audit is performed on an annual basis and tested against industry standards such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, PCI-DSS, and AICPA Trust Services Criteria (SOC1, SOC 2, SOC 3). For more information, see: https://www.oracle.com/corporate/cloud-compliance/ |
| **A&A-01.2** | Are audit and assurance policies, procedures, and standards reviewed and updated at least annually? | Oracle SaaS Cloud Compliance control-related audit and assurance policies, procedures, and standards are reviewed at least annually. |
| **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 https://www.oracle.com/corporate/security-practices/corporate/governance/business-assessment-audit/ |
| | | Oracle SaaS Compliance conducts audits and governance framework assurance assessments in accordance with SaaS Cloud Security Organization Standards for the professional practice of internal auditing. |
| **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). |
| | | Oracle SaaS Compliance conducts audits and governance framework assurance assessments to address risk-based audit plans on identifying, assessing, and prioritizing the highest risk areas within SaaS Cloud Applications. Risks are identified, rated, and discussed in accordance with the risks identified in the risk |

| | | |
|---|---|---|
| | | assessment report and mitigation activities are considered. For more information, see: https://www.oracle.com/corporate/cloud-compliance/ |
| **A&A-04.1** | Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit? | Oracle SaaS Compliance identifies key audit compliance objectives relevant to SaaS Cloud Application standards, regulations, legal/contractual and statutory requirements, in addition any new controls introduced during the audit review period findings. SaaS Compliance Audit plans incorporate consistency to verify compliance to requirements. |
| **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? | Oracle SaaS Compliance executes a standardization and management process that is defined and implemented to support and approve the Audit program development and strategy for SaaS Cloud Applications. |
| **A&A-06.1** | Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained? | Any key risks or control gaps identified by Oracle's Business Assessment & Audit (BA&A) during these reviews are tracked through remediation. Risk-based action plans to address audit findings are established, documented, and communicated to BA&A for approval by Oracle's Lines of Business with evaluation by BA&A. |
| | | Oracle SaaS Compliance implements a SaaS Remediation Management (RM) methodology and maintains a formal, risk-based Corrective Action Plan (CAP) to mitigate risks associated with audit findings that are identified in SaaS Cloud Applications with a defined remediation process. |
| **A&A-06.2** | Is the remediation status of audit findings reviewed and reported to relevant stakeholders? | Risks identified by Oracle's Business Assessment & Audit (BA&A) and associated action item status are confidential and shared with executive leadership and Oracle's Board of Directors. |
| | | Oracle SaaS Compliance defines a formal business response that is provided to relevant key stakeholders with decision making authority. The remediation activities are formally reviewed to provide corrective actions with SaaS Cloud Application owners until resolved. |

## Control Domain: Application & Interface Security

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **AIS-01.1** | Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of | 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.<br>For more information, see https://www.oracle.com/corporate/security-practices/assurance/ |

| | | |
|---|---|---|
| | the organization's application security capabilities? | Oracle SaaS Cloud Applications follows the OSSA methodology, including Standards Secure Software Development Lifecycle (SSDLC). Oracle Corporate Security Solution Assurance Process (CSSAP) provides a centralized review and approval process for compliance to security policies. |
| **AIS-01.2** | Are application security policies and procedures reviewed and updated at least annually? | Oracle SaaS Cloud Security standards and procedures follow the Oracle Corporate Security policies and are reviewed annually and updated as needed. |
| **AIS-02.1** | Are baseline requirements to secure different applications established, documented, and maintained? | Oracle requires Oracle Cloud services be deployed in a specific configuration, or a small number of configurations. The security of cloud configurations are to be planned from the design phase by the development team. The developers implementing the service need to be aware of the planned configuration. Testing is required to be performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment.<br><br>Additionally, cloud development teams are required to deliver the service to cloud operations teams in a secured configuration. Use of containers, such as Docker and automated deployment pipelines, can help development teams satisfy this requirement. |
| | | Baseline requirements for SaaS Cloud Applications are documented and maintained. Secure configuration is evaluated during security reviews, and security scans and testing are performed to check secure configuration of the deployed services. |
| **AIS-03.1** | Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations? | Oracle SaaS Cloud maintains a set of technical and operational metrics to help meet business objectives, security requirements, and compliance obligations to define what should be implemented and when, including security compliance requirements. |
| **AIS-04.1** | Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements? | To ensure that Oracle products are developed with consistently high security assurance, and to help developers avoid common coding mistakes, Oracle employs formal Secure Coding Standards. Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. All Oracle developers are required to be familiar with these standards and apply them when designing and building products. The coding standards have been developed over a number of years and incorporate best practices as well as lessons learned from ongoing vulnerability testing by Oracle's internal product assessment teams. The Secure Coding Standards are a key component of Oracle Software Security Assurance and adherence to the Standards is assessed throughout the supported life of all Oracle products. |
| | | Oracle SaaS Cloud teams follow an SSDLC process and are required to take OSSA training which covers Oracle Secure Coding Standards. Compliance with Secure Coding Standards is being checked through various mechanisms during the SSDLC including security reviews, code reviews, and static code analysis and testing. |

| | | |
|---|---|---|
| **AIS-05.1** | Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals? | Security assurance analysis and testing assess security qualities of Oracle products against various types of attacks. There are two broad categories of tests: static and dynamic analysis.<br><br>**Static security analysis** of source code is the initial line of defense used during the product development cycle. Oracle uses a commercial static code analyzer as well as a variety of internally developed tools, to catch problems while code is being written.<br><br>Typically, analysis of these scan reports involves senior engineers from the product teams who are well-familiar with the product code sorting out false positives from real issues and reducing the number of false positives.<br><br>**Dynamic analysis** activity takes place during latter phases of product development because it requires that the product or component be able to run. Dynamic analysis is aimed at externally visible product interfaces and APIs, and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing within Oracle.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html |
| | | Oracle SaaS Cloud Security executes various security testing scenarios, using both static code and dynamic analysis tools as part of the manual and automated testing process, including security penetration tests on Oracle SaaS Cloud Applications. |
| **AIS-05.2** | Is testing automated when applicable and possible? | SaaS Cloud Security testing for SaaS applications is automated when possible. |
| **AIS-06.1** | Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner? | Strategies and capabilities are defined and implemented to deploy new code for SaaS applications in a secure manner. Testing must be performed on the product with pre-deployment tests performed in an environment identical to the production environment. Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. |
| **AIS-06.2** | Is the deployment and integration of application code automated where possible? | Oracle SaaS applications use automated tools where applicable and available for integration, build and deployment of application code. |
| **AIS-07.1** | Are application security vulnerabilities remediated following defined processes? | Oracle SaaS Cloud Applications has defined metrics to monitor vulnerabilities as they are identified through remediation. The process follows the Security Health Review and Vulnerability Management Advocacy Program to monitor all vulnerabilities through remediation. |
| **AIS-07.2** | Is the remediation of application security vulnerabilities automated when possible? | Security vulnerabilities are remediated through the build and release pipeline. All SaaS Cloud Application security updates are delivered through security patches, and this process is fully automated once a fix is available. |

## Control Domain: Business Continuity Management & Operational Resilience

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **BCR-01.1** | Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained? | The Risk Management Resiliency Program (RMRP) objective is to establish a business resiliency framework to enable efficient Line of Business (LOB) response to business interruption events affecting Oracle's operations. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/<br><br>The RMRP is comprised of several sub-programs: emergency response to unplanned and emergent events, crisis management of serious incidents, technology disaster recovery and business continuity management. The program goal is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored.<br><br>The RMRP is implemented and managed locally, regionally, and globally. The RMRP program management office provides executive scorecard reporting on program activities, planning and plan testing status within the LOBs. |
| | | The Risk Management Resiliency Program (RMRP) establishes the SaaS Cloud Applications Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) implementation. The SaaS Pillar document serves as the policy to attest to the recovery test scenarios and efficacy of the standards and regulatory compliance requirements. Incident management and operational procedures are defined, including a Business Impact Analysis (BIA), and plans for each critical function, with Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), and Recovery Point Objective (RPO). The plan's include continuity strategies for recovering from disasters and SaaS Cloud Application disruptions. |
| **BCR-01.2** | Are the policies and procedures reviewed and updated at least annually? | The RMRP policy mandates an annual operational cycle for (LoB) planning, evaluation, training, validation, and executive approvals for critical business operations.<br><br>Oracle's Risk Management Resiliency Program defines requirements and standards for all Oracle LOBs regarding plans for and response to potential business disruption events. It also specifies the functional LOB roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across geographies. A centralized RMRPProgram Management Office (PMO) has oversight responsibilities for the LoB compliance to the program. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/ |
| | | Oracle SaaS Cloud Applications follows the RMRP operational services resilience attestation BC program and annual test performance. The SaaS Cloud Applications service level DR Kits, BIA, BC/DR plans, procedures, and QA testing is reviewed and approved at least annually, updated as needed during changes, and communicated to constituents. Tier-1 critical services are reviewed and approved quarterly. |
| **BCR-02.1** | Are criteria for developing business continuity and operational resiliency | The RMRP Program is generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance. For more information about the program and requirements |

| | | |
|---|---|---|
| | strategies and capabilities established based on business disruption and risk impacts? | for Oracle Lines of Business, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/ |
| | | Oracle SaaS Cloud Services conducts a Risk Assessment and BIA that is reviewed annually. The service criticality analysis is reviewed bi-annually as established at the global RMRP level. To support the management and oversight of risk across all SaaS Cloud Applications, the SaaS Risk Management Program is aligned with standards that apply across SaaS lines of business. The risk management framework (RMF) is maintained and updated by SaaS Cloud Security (SCS) Risk Management and implemented by management at all levels of SaaS. |
| **BCR-03.1** | Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite? | The RMRP PMO develops guidance as aids to LoB Risk Managers in managing their LoB's business continuity plans, testing and training procedures. The RMRP program requires all LoBs to:<br>• Identify relevant business interruption scenarios, including essential people, resources, facilities and technology<br>• Define business continuity plans and procedures to effectively manage and respond to these risk scenarios, including emergency contact information<br>• Obtain approval of the plans from the LoB's executive<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/ |
| **BCR-04.1** | Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan? | Oracle SaaS Cloud Business Continuity Plan includes a routine Business Impact Assessment (BIA) and resilience strategies for the SaaS Cloud services. Oracle SaaS Cloud Applications relies on the Cloud Provider high availability infrastructure for operational resiliency. The plan is reviewed and approved at least annually and updated as needed. |
| **BCR-05.1** | Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans? | LOBs are required to annually review their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new technology or revised business processes. Critical LoBs must:<br>• 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<br>• Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information<br>• Revise business continuity plans based on changes to operations, business requirements, and risks<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/ |
| | | Oracle SaaS Cloud Business Continuity Plan and Disaster Recovery Plan includes a Business Impact Assessment, disaster scenarios, processes, risk assessment, and procedures for critical functions. The plans are reviewed and approved at least annually and updated as needed. |

| | | |
|---|---|---|
| **BCR-05.2** | Is business continuity and operational resilience documentation available to authorized stakeholders? | Oracle SaaS Cloud Business Continuity and Disaster Recovery (BCDR) Program for Business Continuity (BC) and operational resilience documentation is available to authorized personnel and SaaS customers. The complete plan is an internal Oracle SaaS Cloud document. Assessment of the plans is available in the SOC 2 type 2 reports. |
| **BCR-05.3** | Is business continuity and operational resilience documentation reviewed periodically? | During every exercise, SaaS Cloud DR Kit documentation is reviewed and updated. Top level documentation like BIA is reviewed at least annually and updated as needed. |
| **BCR-06.1** | Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur? | Oracle SaaS Cloud Business Continuity and Disaster Recovery (BCDR) Program has a regimented risk scenario testing cadence; conduct quarterly operational resilience table-top and an annual end-to-end quality assurance testing exercise. There are multiple testing exercises, including Global RMRP tabletop, service specific annual tabletop for Tier-2 services, and service specific 1 switchover/failover + 3 tabletop exercises for tier-1 spread across quarters. |
| **BCR-07.1** | Do business continuity and resilience procedures establish communication with stakeholders and participants? | The internal DR Kit documentation includes a communication plan for each SaaS Service to be used during a crisis. |
| **BCR-08.1** | Is cloud data periodically backed up? | Oracle periodically conducts SaaS Cloud backups of the customer's production data to minimize data loss in the event of an incident. The backup contains provisions for backup systems and configurations and all necessary data required to maintain operational resilience. |
| **BCR-08.2** | Is the confidentiality, integrity, and availability of backup data ensured? | For integrity, backups are encrypted in transit and at rest. Backups are taken on Object Storage Service (OSS) which is resilient and driven by Oracle Identity and Access Management (IAM)policies providing for confidentiality and availability. SaaS Cloud Applications have implemented Recovery Manager (RMAN) to automate backups of customer data to maintain confidentiality and integrity of incremental backups that are taken daily/weekly. RMAN encrypts the backups, and they are stored at both the primary and DR data centers. |
| **BCR-08.3** | Can backups be restored appropriately for resiliency? | SaaS Cloud Disaster Recovery (DR) restoration tests are performed regularly, and operational resilience is monitored for Oracle Cloud customers. A log of the restoration test is kept and reviewed by the audit team for external accreditation. |
| **BCR-09.1** | Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters? | Oracle SaaS Cloud DRP includes disaster scenarios. A communication plan is maintained and updated frequently with evaluations based on periodic DR exercises. Oracle SaaS Cloud is required to conduct an annual review of plans with the objective of maintaining operational recovery capability reflecting changes to the risk environment, including natural and man-made disasters, as well as new or revised business processes. |
| **BCR-09.2** | Is the disaster response plan updated at least annually, and when significant changes occur? | Oracle SaaS Cloud Disaster Recovery Plan (DRP) and procedures are reviewed, updated, and approved at least annually and updated as needed. |

| | | |
|---|---|---|
| **BCR-10.1** | Is the disaster response plan exercised annually or when significant changes occur? | Oracle SaaS Cloud has a documented DR plan to perform annual testing to simulate disaster scenarios that model catastrophic events that may disrupt SaaS Cloud Application services. The DR plan and procedures are reviewed, updated at least annually, and updated as needed. |
| **BCR-10.2** | Are local emergency authorities included, if possible, in the exercise? | Oracle SaaS Cloud Security and physical security perform DR exercises in case of a real emergency. The teams and procedures will be activated in the event of a disaster and the team will contact relevant emergency personnel during an event. |
| **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 https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html |
| | | Oracle Cloud Infrastructure deploys a resilient computing infrastructure designed to maintain service availability zones and continuity in the event of a disaster. Oracle Cloud Applications provides an extensive set of high availability features, such as process death detection and restart, server clustering, server migration, cluster integration, Gridlink, load balancing, failover, backup and recovery, rolling upgrades, and rolling configuration changes, which protect an enterprise deployment from unplanned downtime and minimize planned downtime. These protection solutions include a standby site that is geographically located at a different location than the production site. |

## Control Domain: Change Control & Configuration Management

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **CCC-01.1** | Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)? | Oracle SaaS Cloud maintains an Information Security Standard in supplement with the Information Security Risk Management Policy and in accordance with the Security Organization Policy. The approval of SaaS Cloud risk management practices and procedures are supported by the Cloud Change Management Standard and guidelines that include established Change Management (CM) processes, inclusive of change management controls and industry best practices for cloud application services. |

| | | |
|---|---|---|
| **CCC-01.2** | Are the policies and procedures reviewed and updated at least annually? | Oracle SaaS Cloud standards and procedures are reviewed annually and updated as needed . |
| **CCC-02.1** | Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed? | Oracle SaaS Cloud Operation and Oracle Cloud Service Center (OCSC) for SaaS Cloud Applications establishes a standard change control process and includes approval and testing. A defined and developed testing strategy is executed for pre-production environments and post validation procedures. Automated tests and testing scenarios are predefined and updated as needed. |
| **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 SaaS Cloud Operation and Oracle Cloud Service Center (OCSC) for SaaS Cloud Applications change management process includes a documented risk assessment for internal and external assets and a risk plan that the change owner manages to address and mitigate risks throughout the change request process. |
| **CCC-04.1** | Is the unauthorized addition, removal, update, and management of organization assets restricted | Oracle SaaS Cloud Security standards are in place to outline restrictions for adding, removing, and updating Oracle SaaS Cloud assets. All changes to assets are registered in the asset inventory and the relevant team can perform changes to the asset inventory. Changes to cloud production asset inventory are approved by the owner prior to the change and logged in the change management process. Technical restrictions are in place where safeguards are needed. |
| **CCC-05.1** | Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs? | Oracle SaaS Cloud Operation and Oracle Cloud Service Center (OCSC) for SaaS Cloud Applications updates, upgrades, and planned maintenance windows are clearly communicated and adhered to established service level agreements (SLA) for availability and performance for customers by leveraging the formal SaaS Cloud Change Management (CM) process. |
| **CCC-06.1** | Are change management baselines established for all relevant authorized changes on organizational assets? | Oracle SaaS Cloud Change Management (CM) aligns with industry best practices. Baselines are established and SaaS Cloud Security review for all relevant authorized changes, backup plans, notifications to customers, and testing in lower environments before implementing changes to production on Oracle SaaS Applications. |
| **CCC-07.1** | Are detection measures implemented with proactive notification if changes deviate from established baselines? | Oracle SaaS Cloud Operation and Oracle Cloud Service Center (OCSC) manages detection measures and notifications when a deviation exists within a SaaS Cloud application or infrastructure component. The process is automated by scanning all software components for security and coding standards and performed on a regular schedule to alert, monitor, and triage the event. |
| **CCC-08.1** | Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process? | An emergency change control procedure is in place for managing urgent change requests within SaaS Cloud Applications or infrastructure components. |

| | | |
|---|---|---|
| **CCC-08.2** | Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process? | Oracle SaaS Cloud Security follows an approved and documented exception process that is defined and aligns with security risks and the associated SaaS Cloud Applications business needs. |
| **CCC-09.1** | Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns? | Processes are in place to proactively roll back changes to a previously known "good state" to secure SaaS Cloud Applications. Standard operating procedures (SOP) define the steps to follow, including implementation, pre/peri/post validation, and rollback, as applicable. |

## Control Domain: Cryptography, Encryption & Key Management

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **CEK-01.1** | Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained? | Oracle has formal cryptography, encryption, key management requirements, cryptographic algorithms and protocols. Compliance with these requirements is monitored by Oracle Global Product Security. Oracle products are required to use up-to-date versions of approved security-related implementations. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms. Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption when data is at rest (in storage) on laptops, devices, and removable media. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/ |
| | | Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption, cryptographic algorithms and key management. Oracle SaaS Cloud Security follows OSSA standards that align with industry best practices and NIST requirements, Oracle SaaS Cloud products and services are required to only use up-to-date versions of approved security-related implementations. |
| **CEK-01.2** | Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including policies that address cryptography, encryption, and key management) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud Security standards and procedures that address cryptography, encryption, and key management, are reviewed annually and updated as needed. |
| **CEK-02.1** | Are cryptography, encryption, and key management roles and responsibilities defined and implemented? | Oracle SaaS Cloud Security assigns a Security Lead who is responsible, along with the senior manager for their teams, for the security of SaaS Cloud Applications that defines, manages, and monitors their internal security assurance process functions of cryptography, encryption, and key management. |
| **CEK-03.1** | Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards? | Oracle SaaS Cloud Security follows Oracle cryptography standards. The security technologies outline standard cryptographic and key management implementations that support approved libraries designed to protect information assets at rest and in transit. |

| | | |
|---|---|---|
| **CEK-04.1** | Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability? | Oracle SaaS Cloud Security follows the approved OSSA standard, using appropriate encryption algorithms at rest and data in transit. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/ |
| **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? | Oracle SaaS Cloud Security follows the approved product security OSSA standards for all security related mandatory changes to SaaS Cloud internal and external sources. |
| **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? | Oracle SaaS Cloud Security follows the OSSA standards and procedures for Oracle Cloud SaaS products and services that employ approved encryption keys and defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement to protect SaaS Cloud Applications and services from malicious changes throughout their lifecycle. |
| **CEK-07.1** | Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions? | Representatives from Corporate Security and development organizations define recommended practices related to using and implementing cryptography in Oracle products, derived from frequent reviews of existing industry practices and current threat intelligence.<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html |
| | | Oracle SaaS Cloud Information Security Risk Management Standard identifies potential SaaS information security risks, including cryptography, encryption, and key management through continued risk assessments on SaaS Cloud Applications, including risk visibility and risk remediation activities for all key management operations. Encryption algorithms and key lengths are monitored by the product security team and security operations center regularly to validate only appropriate and sufficient configuration is being used. |
| **CEK-08.1** | Are CSPs providing CSCs with the capacity to manage their own data encryption keys? | Break Glass and Database Vault for Oracle SaaS Cloud Applications is an optional service that provides customers control over data encryption keys. |

| | | |
|---|---|---|
| **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? | Oracle SaaS Cloud follows the OSSA approved standards and security technologies vulnerability handling process for protecting encryption and key management security vulnerability fixes on a timely risk prioritized basis. The key management systems are reviewed by accreditation auditors and are also reviewed by the product security team. The review includes vulnerability scans and configuration management according to SaaS Cloud Security and Privacy standards. |
| **CEK-09.2** | Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)? | Oracle SaaS Cloud Security follows the OSSA standards and procedures for encryption and key management system methods. The review includes vulnerability scans, pen testing, and configuration management by the product security teams and audited annually and updated as needed. |
| **CEK-10.1** | Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications? | Oracle SaaS Cloud Security follows the Oracle standards and procedures for Key generation using Oracle approved implementations, methods, and parameters. Cryptographic key generations are used in accordance with the Global Product Security Secure Coding Standards and Cryptography and Directive and Approved Security Technologies Standards for Cryptographic Algorithms. |
| **CEK-11.1** | Are private keys provisioned for a unique purpose managed, and is cryptography secret? | Private keys are under the purview of the SaaS Cloud customer. Oracle SaaS Cloud Applications do not maintain or provide private keys. |
| **CEK-12.1** | Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements? | Cryptographic keys follow a rotation key management life cycle from generation, storage, distribution, use and destruction while maintaining integrity and confidentiality of SaaS Cloud Applications data. Cryptographic keys are revoked and removed before the end of the established cryptoperiod (when a key is known to have been 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. |
| **CEK-13.1** | Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions? | Cryptographic key expiration and revocation are defined, implemented, and evaluated and immediately revoked and replaced in the event the symmetric key, the asymmetric private key, and/or the password protecting the asymmetric private key have been compromised or no longer valid. Oracle SaaS Cloud Security follows the OSSA standards and procedures in accordance with the OSSA Key Management standards and guidance. |
| **CEK-14.1** | Are processes, procedures and technical measures to destroy | Oracle SaaS Cloud cryptographic key destruction processes and procedures and technical measures are defined and implemented to address key destruction and removal of unneeded keys in accordance with |

| | | |
|---|---|---|
| | 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? | an automatic process and occurs when the customer and or entity is removed from the SaaS Cloud Applications. |
| **CEK-15.1** | Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions? | Oracle SaaS Cloud follows OSSA key management lifecycle; key generation process to create keys in a pre-activated state. All key management processes, implementations and operations are defined, implemented, and include approved security technologies. |
| **CEK-16.1** | Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions? | Oracle SaaS Cloud follows OSSA key management lifecycle services and automates the process of rotating, suspending, creating, and deleting keys to support the monitoring, review, and approval of key transitions. |
| **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? | See CEK-13.1. |
| **CEK-18.1** | Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions? | Oracle SaaS Cloud Security standards, including procedures and standards that address cryptography, encryption, and key management support the key Management life cycle implementation to manage archived keys in a secure repository. |
| **CEK-19.1** | Are processes, procedures, and technical measures to encrypt information in specific scenarios | Oracle SaaS Cloud standards and procedures follow additional authenticated data (AAD) to protect information that needs to be authenticated. It supports common use cases and specific scenarios used for |

| | | |
|---|---|---|
| | (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? | SaaS Application services and product features or as countermeasure to SaaS Applications that are defined, implemented, and evaluated against NIST standards. |
| **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? | See CEK-7.1. |
| **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? | See CEK-7.1 |

## Control Domain: Data Center Security

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **DCS-01.1** | Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained? | Oracle's Media Sanitization Policy specifies requirements including secure disposal of equipment and media used for data storage. This policy is established, documented, approved, communicated, and maintained.<br><br>Oracle SaaS Cloud maintains Media Sanitization and Disposal procedures, and standards for the secure disposal of equipment used on SaaS managed systems, cloud storage, information in hard copy and on applicable electronic storage media that refers to Oracle SaaS customers' or vendors/suppliers, or on the personal hardware assets of Oracle SaaS users and contingent workers where confidential information is no longer required, and is enforced to protect from security threats that would compromise the retrieval and reconstruction of confidential information. |

| | | |
|---|---|---|
| **DCS-01.2** | Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed? | Oracle SaaS Cloud applies data retention and disposal destruction in accordance with the SaaS Cloud Media Sanitization and Disposal standard, SaaS Cloud PI Data Protection standard, and procedures for managing and moving data during destruction. |
| **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? | Oracle Corporate Security policies (including policies that address secure disposal of equipment outside the organization's premises) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud policies, procedures, and standards for the secure disposal of equipment used on SaaS managed systems, cloud storage, information in hard copy and on applicable electronic storage media that refers to Oracle SaaS customers' or vendors/suppliers, or on the personal hardware assets of Oracle SaaS users and contingent workers where confidential information is no longer required are reviewed annually and updated as needed. |
| **DCS-02.1** | Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained? | Oracle's Information Systems Inventory Policy requires that Line of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware and software. This policy is established, documented, approved, communicated, and maintained. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html |
| | | Third-party contractual agreements in accordance with the Oracle Supplier Information and Physical Security standards provide audit rights to ensure the requirements meet relocation or transfer compliance. SaaS Cloud Applications customer data is deleted and irrecoverable as per any contractual agreements. |
| **DCS-02.2** | Does a relocation or transfer request require written or cryptographically verifiable authorization? | Oracle SaaS Cloud Security requires SaaS Cloud Application customers to follow the cryptography guidance of relocation services by submitting a formal request in My Oracle Support (MOS). Only approved and authenticated customers have access to the portal. |
| **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 policies that address the relocation or transfer of hardware, software, or data/information to any location) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud Security maintains Media Sanitization and Disposal standards, and third-party contractual agreements in accordance with the Oracle Supplier Information and Physical Security standards and are reviewed annually and updated as needed. |
| **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.<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html |
| | | Procedure reviews are done by LOB  Oracle SaaS Cloud Security maintains a Personnel Security Standard that is supported by the Oracle Physical Security policy that describes the requirements for maintaining a safe and secure work environment. For more information, see: |

| | | |
|---|---|---|
| | | https://www.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 policies that address safe and secure working environments) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud Security Personnel Security Standard, including Oracle Physical Security policy for maintaining a safe and secure work environments are reviewed annually and updated as needed. |
| **DCS-04.1** | Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained? | Oracle SaaS Cloud Security maintains Information Protection standards and procedures to help ensure the handling of SaaS Cloud confidential information is securily transmitted to and from SaaS Cloud Customers and third-parties for the secure transportation of physical media. For more informattion, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection |
| **DCS-04.2** | Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually? | Oracle Corporate Security policies (including policies that address the secure transportation of assets) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud Security Information Protection standards and procedures are reviewed annually and updated as needed. |
| **DCS-05.1** | Is the classification and documentation of physical and logical assets based on the organizational business risk? | Oracle's formal Information Protection Policy sets forth the requirements for classifying and handling public and confidential information. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html |
| | | Oracle SaaS Cloud Security Logical Access Controls policy, Ifollows Oracle's formal Information Protection Policy standards that determine the classification scheme, based on SaaS Cloud Applications risk assessments, and documentation requirements for assets according to the sensitivity and criticality of information they store, transmit, and receive in SaaS Cloud Applications that contain confidential (restricted or highly restricted) information. |
| **DCS-06.1** | Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system? | The Oracle Information Systems Inventory Policy requires that Lines of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware and software. Inventories must be managed within an approved inventory system. This policy defines required identifying attributes to be recorded for server hardware, software, data held on information systems, and information needed for disaster recovery and business continuity purposes. |
| | | Oracle SaaS Cloud Security catalogues and tracks assets following the Oracle Information Systems Inventory Policy which requires accurate and comprehensive inventory of information systems, hardware, and software. Inventories must be managed within an approved inventory system. All system access is provisioned on a need-to-know basis. |
| **DCS-07.1** | Are physical security perimeters implemented to safeguard personnel, data, and information systems? | Oracle Global Physical Security uses a risk-based approach to physical and environmental security. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html |

| | | |
|---|---|---|
| | | Oracle SaaS Cloud provides assurance for physical security perimeters to safeguard personnel, data, and information systems in accordance with the Data Center Assessment Program. Oracle Cloud physical security secures data center perimeter to prevent unauthorized users to Oracle SaaS Cloud Applications information. The effectiveness of physical security controls is assessed and implemented by Global Physical Security. See: https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html |
| **DCS-07.2** | Are physical security perimeters established between administrative and business areas, data storage, and processing facilities? | The goal is to balance prevention, detection, protection, and response, while maintaining a work environment that fosters collaboration among Oracle employees.<br>See DCS 07.1 |
| **DCS-08.1** | Is equipment identification used as a method for connection authentication? | The Oracle Cloud Network Access (OCNA) VPN that Oracle staff use to connect to Oracle SaaS Cloud Applications uses both machine certificates and other identifiers to validate that the device is Oracle owned and provisioned before allowing access to resources. Oracle SaaS Cloud Application manages equipment identification in alignment with the ISO 27001 standard. |
| **DCS-09.1** | Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms? | Oracle has implemented the following protocols:<br>• Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors.<br>• Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises.<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html |
| **DCS-09.2** | Are access control records retained periodically, as deemed appropriate by the organization? | Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors. Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises.<br>Visitors are required to sign a visitor's register, be escorted and/or observed when they are on Oracle premises, and/or be bound by the terms of a confidentiality agreement with Oracle.<br>Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving Oracle's employment must return keys/cards and key/cards are deactivated upon termination.<br>For more information, see: https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html |

| | | |
|---|---|---|
| **DCS-10.1** | Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated? | Oracle uses a mixture of 24/7 onsite security officers or patrol officers, depending on the risk/protection level of the facility. In all cases officers are responsible for patrols, alarm response, and recording of security incidents.<br><br>Oracle has implemented centrally managed electronic access control systems with integrated intruder alarm capability and CCTV monitoring and recording. The access control system logs and CCTV recordings are retained for a period of 30-90 days as defined in Oracle's Record Retention Policy which are based on the facility's function, risk level and local laws.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html |
| **DCS-11.1** | Are datacenter personnel trained to respond to unauthorized access or egress attempts? | Personnel are trained in incident response and escalation procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html |
| **DCS-12.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms? | Data centers hosting Oracle cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria.<br><br>Oracle cloud service data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Personnel are trained in procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html |
| **DCS-13.1** | Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained? | Please see DCS-12.1 |
| **DCS-14.1** | Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness? | Please see DCS-12.1 |
| **DCS-15.1** | Is business-critical equipment segregated from locations subject to | Please see DCS-12.1 |

| | | |
|---|---|---|
| | a high probability of environmental risk events? | |

## Control Domain: Data Security & Privacy Lifecycle

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **DSP-01.1** | Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level? | Oracle's information-asset classification determines corporate data-security requirements for Oracle-managed systems. Oracle policies provide global guidance for appropriate controls designed to protect corporate, cloud and customer data in accordance with the data classification. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/ |
| | | Oracle SaaS Cloud maintains standards and procedures on data classification, protection, and handling throughout its data lifecycle, according to legal and regulatory requirements. Oracle SaaS Cloud follows Oracle's information asset classification policy thatprovides global guidance for appropriate controls designed to protect corporate, cloud, and customer data in accordance with the data classification. The Oracle Information Protection Policy sets forth the requirements for classifying and handling confidential information, including requirements for visual disclosure. The policy applies to all Oracle users and to all confidential information, whether the information belongs to Oracle, customers, or a third party. |
| **DSP-01.2** | Are data security and privacy policies and procedures reviewed and updated at least annually? | Oracle policies (including policies that address data security and privacy) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud security standards and procedures for data security and privacy are reviewed 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 SaaS Cloud industry accepted methods are applied for secure data disposal from storage media. Oracle's media sanitation and disposal policy defines requirements for removal of information from electronic storage media and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. |
| **DSP-03.1** | Is a data inventory created and maintained for sensitive and personal information (at a minimum)? | Oracle SaaS Cloud is required by Oracle to document and maintain data inventories and data flows. This documentation is for internal use only. The customer is responsible for creating their data inventory. |
| **DSP-04.1** | Is data classified according to type and sensitivity levels? | Oracle categorizes information into four classes- Public, Internal, Restricted, and Highly Restricted-with each classification requiring corresponding levels of security controls, such as encryption requirements for non-Public data. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html |
| **DSP-05.1** | Is data flow documentation created to identify what data is processed | Oracle SaaS Cloud Services documents the flow of customer PI through the product or service. The diagrams include details such as inbound and outbound SaaS Cloud customer traffic, ports and protocols, |

| | | |
|---|---|---|
| | and where it is stored and transmitted? | customer roles (such as end user & admin), data flows through the application, static data stores (such as SFTP servers and storage), and email gateways where applicable. All Oracle SaaS Cloud services provide this documentation during the Corporate Security Solutions Assurance Process (CSSAP) and/or upon request. |
| **DSP-05.2** | Is data flow documentation reviewed at defined intervals, at least annually, and after any change? | Oracle SaaS Cloud Data Flow documentation is reviewed at least annually and updated as needed. |
| **DSP-06.1** | Is the ownership and stewardship of all relevant personal and sensitive data documented? | Oracle's Information Systems Asset Inventory policy requires that SaaS Cloud Security maintain accurate and comprehensive inventories of information systems, hardware, and software. Ownership and stewardship of all relevant personal and sensitive data is documented. The customer is the controller of their data. |
| **DSP-06.2** | Is data ownership and stewardship documentation reviewed at least annually? | Oracle SaaS Cloud customers own their data and manage access to their SaaS Cloud Applications. Review and schedules are at the discretion of the customer. Oracle SaaS Cloud standards that address ownership and stewardship are reviewed annually and updated as needed. |
| **DSP-07.1** | Are systems, products, and business practices based on security principles by design and per industry best practices? | Oracle SaaS Cloud Services are based on the ISO/IEC 27001/27017, including other security standards that define security principles by design best practices for SaaS Cloud Applications. For more information, see: https://www.oracle.com/corporate/cloud-compliance/ |
| **DSP-08.1** | Are systems, products, and business practices based on privacy principles by design and according to industry best practices? | Oracle SaaS Cloud Services are based on the ISO/IEC 27002, including other privacy standards that define principles by design best practices for SaaS Cloud Applications. For more information, see: https://www.oracle.com/corporate/cloud-compliance/ |
| **DSP-08.2** | Are systems' privacy settings configured by default and according to all applicable laws and regulations? | Oracle SaaS Cloud privacy settings are configured following a Privacy by Design (PbD) methodology and according to applicable default privacy standards, laws, and regulations. Oracle SaaS Cloud adopts Privacy by Design (PbD) best practices. |
| **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? | Oracle SaaS Cloud performs security and privacy impact assessments (PIAs) for all new products and system feature enhancements we wish to bring to market. Oracle legal teams perform Data Privacy Impact Assessments (DPIAs) in accordance with the Oracle Services Privacy Policy. |
| **DSP-10.1** | Are processes, procedures, and technical measures defined, | SaaS Cloud Corporate Single Sign-On standard sets forth the requirements to ensure proper authentication and identity management for SaaS Cloud users when accessing Oracle SaaS Cloud |

| | | |
|---|---|---|
| | 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)? | environments. The standard includes requirements for application authentication and specific user requirements to protect unauthorized access of personal (PI) or sensitive data. Oracle SaaS Cloud Services follows the Oracle Cloud – PII Data Protection Standard and procedures, as part of the privacy-by-design framework. Oracle Cloud Services provide functionality where a customer can restrict or object to the use of or transfer of customer PI. |
| **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)? | Oracle SaaS Cloud Services follows the Oracle Cloud – PII Data Protection Standard and procedures, as part of the privacy-by-design framework. Oracle Cloud Services provide functionality where a customer, data subjects requests, can securely process customer data subjects related requests to request access, modify, or delete personal data (PI rectified, corrected, or erased) applicable to security, privacy, and regulatory requirements. |
| **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 DSP 10.1 and DSP 11.1. |
| **DSP-13.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)? | Please see the Oracle privacy policies at https://www.oracle.com/legal/privacy/ |
| | | Oracle SaaS Cloud has processes, procedures, and technical measures in place for the transfer and sub-processing of personal data within the service supply chain. Oracle and Oracle Affiliates employees, as well as any third-party sub-processors that process personal identifiable information (PII), are subject to appropriate written confidentiality agreements, including regular training on information protection, and compliance with Oracle policies concerning protection of confidential information. Established privacy risk assessments evaluate the transfer and sub-processing of personal data within the SaaS Cloud service. |
| **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? | Oracle SaaS Cloud Services follows the Oracle Cloud – PII Data Protection Standard and procedures, as part of the privacy-by-design framework. Oracle SaaS Cloud Services follows the Data Processing Agreement regarding third-party vendors or sub-processors that process customer personal information. Oracle engages Oracle affiliates and third-party sub processors access to services personal information to assist in the provision of services, such sub-processors shall be subject to the same level of data protection and security as Oracle under the terms of your order for services. Oracle is responsible for its sub-processors' compliance with the terms of your order for services. For more information, see: https://www.oracle.com/legal/privacy/services-privacy-policy/ |
| **DSP-15.1** | Is authorization from data owners obtained, and the associated risk | Oracle SaaS Cloud replicating or using production data in non-production environments is not performed. Oracle will not use customer data in non-production environments or for testing purposes. Oracle SaaS |

| | | |
|---|---|---|
| | managed, before replicating or using production data in non-production environments? | cloud production and non-production environments are logically and physically segregated. Additionally, procedures are in place to help ensure production data is not used in non-production environments. Oracle SaaS Cloud customers may request a Production to Test (P2T) copy and data can be masked using Oracle's Data Masking solution to prevent sensitive data being used in the test environment. |
| **DSP-16.1** | Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations? | Oracle SaaS Cloud customers maintain responsibility for their data residing in their environment.<br><br>SaaS Cloud can be configured by the customer to meet their objectives for data retention, archiving and deletion practices per their business requirements, applicable laws, and regulations. During the use of Oracle SaaS Cloud Applications, Oracle Cloud customers maintain responsibility for their data residing in their environment. Oracle SaaS Cloud Services provide a variety of configurable controls as part of the subscribed service. Customer data is data uploaded or generated for use within the subscribed Oracle SaaS Cloud Services. |
| **DSP-17.1** | Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle? | Oracle SaaS Cloud standards, procedures, and technical measures are defined and implemented to protect sensitive data throughout its lifecycle. The customer remains solely responsible for their user access to the service provided. During the use of Oracle SaaS Cloud Applications, Oracle Cloud customers maintain responsibility for their data residing in their environment. Oracle SaaS Cloud Services provide a variety of configurable information protection services as part of the subscribed service. |
| **DSP-18.1** | Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations? | Oracle SaaS Cloud Services will promptly inform the SaaS Cloud customer of requests to provide access to Personal Identifiable Information (PII), unless otherwise required by law, for more information see Oracle Cloud Services Contracts – OCI - Privacy Documents: https://www.oracle.com/contracts/cloud-services/ |
| **DSP-18.2** | Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation? | Oracle SaaS Cloud Services will promptly inform the SaaS Cloud customer of requests to provide access to Personal Information unless otherwise required by law, for more information see Oracle Cloud Services Contracts – OCI – Privacy Documents: https://www.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? | Oracle SaaS Cloud has processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locations where data is processed or backed up, for more information see Oracle Cloud Services Contracts – OCI – Privacy Documents: https://www.oracle.com/contracts/cloud-services/ |

## Control Domain: Governance, Risk & Compliance

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **GRC-01.1** | Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained? | Global Information Security (GIS) defines policies for the Line of Business management of information security across Oracle. Additionally, GIS sets direction and provides advice to help protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners and employees. GIS also coordinates the reporting of information security risk to senior leadership such as the Oracle Security Oversight Committee and Board of Directors. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html |
| | | The SaaS Cloud Information Security Governance program defines standards and procedures that are reviewed and approved by organizational leadership to guide the development and maintenance of a comprehensive information security program. |
| **GRC-01.2** | Are the policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including policies that address governance, risk, and compliance) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud Security standards and procedures are reviewed on an annual basis and updated as needed. |
| **GRC-02.1** | Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks? | The Chief Corporate Architect is one of the directors of the Oracle Security Oversight Committee (OSOC) and manages the Corporate Security departments which guide security controls at Oracle. These departments drive the corporate security programs, define corporate security policies, and provide security assurance oversight of Lines of Business.<br><br>Corporate Security Architecture manages a cross-organization working group focused on security architecture of corporate and cloud systems. Participation includes members from cloud service development, operations, and governance teams. Each Line of Business is responsible implementing associated procedures.<br><br>Oracle Privacy & Security Legal manages the cross-organization oversight of privacy risks. For more information, see https://www.oracle.com/legal/privacy/ |
| **GRC-03.1** | Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs? | Oracle Corporate Security policies are reviewed annually and updated as needed. |
| | | The SaaS Cloud Information Security Standards are reviewed and updated annually, including when a substantial organizational change occurs. |
| **GRC-04.1** | Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs? | Global Information Security (GIS) manages a security exception program which oversees LoB exception and exception management activity. |
| | | The SaaS Cloud Information Security Governance program follows a standard process to identify, report, and manage deviation from SaaS Information Security Standards. Approved exceptions are managed, logged, and tracked when there are deviations. |

| | | |
|---|---|---|
| **GRC-05.1** | Has an information security program (including programs of all relevant CCM domains) been developed and implemented? | Oracle SaaS Cloud compliance program ensures CCM domains are mapped to SaaS Cloud Applications and is CSA STAR certified. For more information, see https://www.oracle.com/corporate/cloud-compliance/ |
| **GRC-06.1** | Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented? | Oracle SaaS Information Security Governance defines Roles and Responsibilities for planning, implementing, operating, assessing, and improving information security programs that are documented in SaaS Information Security Standards and supported by Global Information Security Policies. |
| **GRC-07.1** | Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented? | Oracle SaaS Security standards, regulations, legal/contractual, and statutory requirements are identified and documented. The customer remains solely responsible for its regulatory compliance in its use of any Oracle SaaS Cloud Applications. The customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing. |
| **GRC-08.1** | Is contact established and maintained with cloud-related special interest groups and other relevant entities? | Oracle is an Information Technology-Information Sharing and Analysis Center (IT-ISAC) organization. For more information, see https://www.it-isac.org/home and https://openssf.org/about/members/ |

## Control Domain: Human Resource Security

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **HRS-01.1** | Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained? | In accordance with Oracle policy, background checks are required for individuals being considered for employment. For more information, see https://www.oracle.com/corporate/careers/background-check.html<br><br>The Oracle Recruiting Privacy Policy describes the privacy and security practices of Oracle when collecting, using and handling (processing) personal information about job applicants in connection with our online and offline recruitment activities. It also explains the choices candidates have in relation to these processing activities, see https://www.oracle.com/legal/privacy/recruiting-privacy-policy/. |
| **HRS-01.2** | Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk? | In accordance with Oracle policy, background checks are required for individuals being considered for employment. For background check information organized by local law and regulation, see https://www.oracle.com/corporate/careers/background-check.html |

| | | |
|---|---|---|
| **HRS-01.3** | Are background verification policies and procedures reviewed and updated at least annually? | Oracle Human Resources policies (including policies that address candidate and employee background checks) are reviewed annually and updated as needed.<br><br>Oracle's SaaS Cloud security standard policies for candidates 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's Acceptable Use Policy (AUP) guides the use of organizationally owned or managed assets. Employees must sign a confidentiality agreement as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. For more information, see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html<br><br>Oracle SaaS Cloud Personnel Security Standard helps ensure employees maintain the confidentiality of customer data, including SaaS physical and network access requirements. All employees are responsible for understanding and following corporate policies and SaaS standards. |
| **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 SaaS Cloud Personnel Security Standards are reviewed annually and updated as needed. |
| **HRS-03.1** | Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained? | Each employee is required to complete information-protection awareness training upon hiring and every two years. The course instructs employees on their obligations under Oracle policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs and are required by company policy. For more information see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html |
| **HRS-03.2** | Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually? | Oracle SaaS Cloud Personnel Security Standard provides key requirements to protect unattended workspaces to conceal confidential data, including data handling in physical, network, and government access environments, and 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 Line of Business management of information security across Oracle. For more information see https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html<br><br>Data centers hosting cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among |

| | | |
|---|---|---|
| | | other criteria. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html |
| | | Oracle SaaS Cloud follows Oracle's physical security standards and policies for defining, developing, implementing, and managing physical security for the protection of Oracle's employees, facilities, business enterprise, and assets, including guidelines to protect SaaS Cloud personal information, device safety and security, and physical security technology. |
| **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 policies intended to protect information accessed, processed, or stored at remote sites and locations) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud follows Oracle's physical security standards and policies, including guidelines intended to protect information accessed, processed, or stored at remote sites and locations, are reviewed annually and updated as needed. |
| **HRS-05.1** | Are return procedures of organizationally-owned assets by terminated employees established and documented? | In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| **HRS-06.1** | Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel? | Oracle SaaS Cloud Personnel Security standards and procedures define the roles and responsibilities concerning changes in employment and are documented and communicated to all personnel. |
| **HRS-07.1** | Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets? | Please see HRS-02.1 |
| **HRS-08.1** | Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements? | Please see HRS-02.1 |
| **HRS-09.1** | Are employee roles and responsibilities relating to information assets and security documented and communicated? | Oracle Cloud SaaS employee roles and responsibilities relating to information assets and security are defined, documented and communicated. Oracle SaaS Cloud PI data protection standards, information protection, information management, and record retention policies provide global guidance for appropriate controls designed to protect cloud and customer data in accordance with data classification. |

| | | |
|---|---|---|
| **HRS-10.1** | Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals? | Please see HRS-02.1 |
| **HRS-11.1** | Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained? | Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Employees who fail to comply with these policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment.<br><br>Each employee is required to complete information-protection awareness training upon hiring and every two years. The course instructs employees on their obligations under Oracle policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs and are required by company policy.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html |
| **HRS-11.2** | Are regular security awareness training updates provided? | Please see HRS-11.1 |
| **HRS-12.1** | Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training? | Please see HRS-11.1 |
| **HRS-12.2** | Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function? | Please see HRS-11.1 |
| **HRS-13.1** | Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations? | Oracle SaaS Cloud employees are required to complete security awareness training at least annually, depending on the employee's role, or other qualifying criteria to maintain legal, statutory, and regulatory compliance obligations. |

## Control Domain: Identity & Access Management

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **IAM-01.1** | Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained? | Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services.<br>The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| | | Oracle SaaS Cloud Security maintains a Logical Access Control Policy and Logical Access Controls Standard that sets forth the access requirements for Oracle SaaS Cloud owners and systems that is documented, approved, communicated, implemented, applied, evaluated, and maintained. |
| **IAM-01.2** | Are identity and access management policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including policies applicable to identity and access management) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud Security Logical Access Control Policy and Logical Access Controls Standard are reviewed annually and updated as needed. |
| **IAM-02.1** | Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained? | Oracle has strong password policies (including length and complexity requirements) for the Oracle network, operating system, email, database and other accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. Identity management systems are required to comply with Corporate Security Architecture requirements. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html |
| | | Oracle SaaS Cloud Security maintains a password standard to protect the confidentiality, integrity, and availability of SaaS Cloud information assets that is documented, approved, communicated, implemented, applied, evaluated, and maintained. |
| **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. |
| | | Oracle SaaS Cloud Security Password Standards are reviewed annually and updated as needed. |
| **IAM-03.1** | Is system identity information and levels of access managed, stored, and reviewed? | Oracle SaaS Cloud Security follows the SaaS Cloud Security Logical Access Control standard for all SaaS Cloud owners access level and systems are managed, stored and reviewed periodically to ensure compliance. |

| | | |
|---|---|---|
| **IAM-04.1** | Is the separation of duties principle employed when implementing information system access? | Oracle SaaS Cloud Security enforces well-defined roles, allowing for segregation of duties among operation users which is defined in the SaaS Logical Access Controls Standard. Operations are organized into functional groups, where each function is performed by separate groups of employees (e.g., database administrators, system administrators, and network engineers). 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. |
| **IAM-05.1** | Is the least privilege principle employed when implementing information system access? | Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are required to be based on the following principles:<br>• Need to know: Does the user require this access for his job function?<br>• Segregation of duties: Will the access result in a conflict of interest?<br>• Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| | | Oracle SaaS Cloud Security access is provided on a need-to-know and least-privileged basis for employees and approved third parties when implementing information system access to SaaS cloud environments. The principle of least trust is individually attributable or provides a one-to-one user-to-account when providing access to all SaaS Cloud Applications data and information. |
| **IAM-06.1** | Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes? | Oracle SaaS Cloud Security user accounts are managed with a provisioning process. Access to user groups and resources are approved in the permissions system prior to access provisioning. An expiration date is required for temporary access requests. SaaS Cloud users supporting the SaaS Cloud Applications and services are defined and implemented to authorize, record, and communicate data and assets access changes for users who are authorized to administer the device or asset. |
| **IAM-07.1** | Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies? | Oracle Lines of Business are required to regularly review network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| | | Oracle SaaS Cloud Security disables and revokes SaaS Cloud accounts if an employee leaves the company for any reason. SaaS Cloud entitlements are automatically disabled when there are system identity changes, and it is required to request new entitlements. The de-provision process prevents the user from accessing protected networks and devices in cloud environments. |
| **IAM-08.1** | Are reviews and revalidation of user access for least privilege and separation of duties completed with | Oracle SaaS Cloud reviews entitlements on a quarterly audit basis and updates SaaS Cloud users and their access for least privilege and separation of duties with organization risk tolerance to meet SaaS Cloud compliance, security requirements,. |

| | | |
|---|---|---|
| | a frequency commensurate with organizational risk tolerance? | |
| **IAM-09.1** | Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate? | Oracle SaaS Cloud Security follows an approved separation of duties process for the segregation of privileged access roles with technical measures that define the requirements to implement data access, encryption, key management, and logging capabilities. Oracle SaaS Cloud employs the principle of least privilege allowing only authorized users access. |
| **IAM-10.1** | Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period? | Oracle SaaS Cloud access processes are defined and implemented. Privileged Access roles and rights have processes to ensure they are reviewed on a quarterly basis. Privileged Account passwords expire on a shortened cycle. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| **IAM-10.2** | Are procedures implemented to prevent the culmination of segregated privileged access? | See IAM-06.1 |
| **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? | IAM-06.1 |
| **IAM-12.1** | Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated? | Oracle SaaS Cloud adheres to the Logging and Log Analysis Standard and follows the Oracle Corporate Logging and Log Analysis Policy to ensure the logging infrastructure is defined, implemented, and evaluated to address technical measures and logging best practices. SaaS Cloud users are only granted permission to access log data based on their assigned role. |
| **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? | Oracle SaaS Cloud Security Logical Access Controls Standards and access-control policies ensure users are identifiable through unique identification and access permission based on their assigned role. Approved users use different permission credentials to access only the data explicitly granted to SaaS cloud environments. |
| **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? | Oracle SaaS Cloud Security Logical Access Controls Standard defines processes, procedures, and technical measures for authenticating access to Oracle Cloud systems, applications and data assets, including multi-factor authentication (MFA) for a least-privileged user and sensitive data access. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| **IAM-14.2** | Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted? | Oracle SaaS Cloud Security uses external and internal certificate authorities for digital certification generation. For SaaS Cloud customer facing URLs, Oracle uses external certificate authority vendors. For internal application communication, Oracle uses an external certificate authority. |
| **IAM-15.1** | Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated? | Oracle SaaS Cloud Password Standard ensures processes, procedures, and technical measures are in place for the secure management of passwords. Password managed components protect the confidentiality, integrity, and availability of Oracle SaaS Cloud information assets. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| **IAM-16.1** | Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated? | Oracle SaaS Cloud Corporate Single Sign-On Standards and technical controls sets forth the processes, procedures, and technical measures to ensure proper authentication are in place to verify user's requirement access to Oracle SaaS Cloud information assets. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/ |

## 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)? | Oracle SaaS Cloud Security documents available APIs for Oracle Cloud Applications that are in place for communications between application services. For more information, see: https://docs.oracle.com/en/cloud/ |

| | | |
|---|---|---|
| **IPY-01.2** | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability? | Oracle SaaS Cloud Applications follows policies and procedures for communication between components information processing, including interoperability. Customers are provided network protocol information necessary to use the services. |
| **IPY-01.3** | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability? | Oracle SaaS Cloud Applications follows policies and procedures established and maintained to support application development portability and application deployment on major operating systems (Windows, MAC, Linux). |
| **IPY-01.4** | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence? | Oracle SaaS Cloud security maintains Standards and procedures for information transfer that is defined and published in the SLA Cloud Services. For more information, see Oracle Cloud Services Contracts: https://www.oracle.com/contracts/cloud-services/ |
| **IPY-01.5** | Are interoperability and portability policies and procedures reviewed and updated at least annually? | Oracle SaaS Cloud Security standards and procedures follows architecture reviews as part of the development, process, including, interoperability and, portability of SaaS Cloud Applications and 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? | Oracle SaaS Cloud customer API calls, including actions from the customer administration console, are logged and retained for 90 days and cannot be deleted by customers. Where applicable, CSC's can programmatically retrieve their data via an application interface. Oracle SaaS Cloud Application customers may request an export of their logs by contacting Oracle Cloud Services. |
| **IPY-03.1** | Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data? | Oracle SaaS Cloud security implements a secure file transfer functionality that is built on commonly used network access storage platforms and uses a secured protocols for transfer. The functionality can be used to upload files to a secure location (i.e., data import/export) on Oracle Cloud hosted service or downloading files at service termination. Secured data transfer between on-premises and a customer's tenancy; between customer's 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?<br>a. Data format<br>b. Duration data will be stored<br>c. Scope of the data retained and | Oracle Cloud Hosting and Delivery Policies and the Oracle PaaS and IaaS Public Cloud Services Pillar document set forth Oracle Cloud Service Level Objective Policy which defines Target Service Availability Level and Target Service Uptime. This includes a provision specifying customer access to data upon contract termination. At the end of the Service Period, the customer's content is available for retrieval during a retrieval period set forth in the Service Specifications or required by law. Remaining content will be deleted or otherwise rendered unrecoverable. Data deletion best practices are described in more detail |

| | | |
|---|---|---|
| | made available to the CSCs<br>d. Data deletion policy | in the Service Specifications. For more information, see: https://www.oracle.com/contracts/cloud-services/ |

## Control Domain: Infrastructure & Virtualization Services

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **IVS-01.1** | Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained? | Oracle SaaS Cloud follows a Network Security Standard and procedures that are established and approved by Global Information Security (GIS) and follows GIS information security policies, For more information, see: https://www.oracle.com/corporate/security-practices/corporate/ |
| **IVS-01.2** | Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually? | Oracle SaaS Cloud Network Security Standards are established and approved by Global Information Security (GIS) and follow information security policiesand are reviewed 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? | Oracle SaaS Cloud Services collects and monitors capacity and utilization data. This data is used to plan for adequate capacity to meet current availability, quality, projected, and anticipated needs of the customer to minimize disruptions to the SaaS Cloud Applications and service level agreements (SLA). |
| **IVS-03.1** | Are communications between environments monitored? | Oracle SaaS Cloud Security follows the OSSA standards for SaaS Cloud Applications and employs active continuous monitoring on the attack surface in accordance with OCI firewall logging and Network Intrusion Detection Systems to identify and block suspicious traffic and security attacks. Oracle Cloud Services monitors log system errors and security alerts for incident management and forensic purposes for security event analysis. |
| **IVS-03.2** | Are communications between environments encrypted? | Communications between SaaS Cloud Applications environments are encrypted, including SaaS Cloud user/device authentication via passwords and multi-factor authentication. RBAC management principles are adopted with authorizing controls. |
| **IVS-03.3** | Are communications between environments restricted to only authenticated and authorized connections, as justified by the business? | Oracle SaaS Cloud Security follows the OSSA standards for Oracle SaaS Cloud Applications to ensure environments are restricted to only authenticated and authorized connections by configuring and enabling secure communications. |
| **IVS-03.4** | Are network configurations reviewed at least annually? | SaaS Cloud Security standards and procedures for network configurations are reviewed annually and updated as needed. |

| | | |
|---|---|---|
| **IVS-03.5** | Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls? | Oracle SaaS Cloud Security follows the Oracle Cloud Network Security Standard and the OSSA standards to ensure configurations are supported and documented on configuring the security on the SaaS Cloud Applications. |
| **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 SaaS Cloud Security employs standardized system hardening practices across Oracle SaaS Cloud Applications network configurations and connections. This includes restricting protocol access, removing or disabling unnecessary software and services, unnecessary user accounts, patch management, and logging. |
| **IVS-05.1** | Are production and non-production environments separated? | Oracle SaaS Cloud Services production and non-production SaaS Cloud Application environments are logically and physically segregated. Additionally, procedures are in place to ensure production data is not used in non-production environments. |
| **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? | To mitigate security risks associated with SaaS Cloud Application customer data that are comingling inherent in multi-tenant clouds, SaaS Cloud environments are provisioned in Oracle's Isolated Tenancy Model, isolating one customer from other Oracle Cloud customers. Data is segregated from other Oracle Cloud customer data via dedicated database, virtual machines and VLANs. |
| **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? | Access to Oracle SaaS Cloud Applications is through a secure communication protocol. Staging networks are segregated from production-level networks and utilized when migrating production data to virtual servers. Physical servers, applications, and virtual machines are not moved. New environments are provisioned using a hardened master image with customer data migrated once the provisioning process is complete. Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Customer configuration information (e.g., connection strings, application settings) supplied through the management portal is protected while in transit and at rest. |
| **IVS-08.1** | Are high-risk environments identified and documented? | Oracle SaaS Information Security Risk Management Standard addresses a risk management process to identify SaaS Cloud Application risks in high-risk environments associated with specific SaaS Applications and SaaS Risk Treatment SLAs to protect customer data from misuse or compromise. |
| **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 SaaS Cloud maintains a Network Security Standard and procedures that are established and approved by Global Information Security (GIS) and adhere to Network Security Management controls using only secure protocols, encrypted traffic, Network Intrusion Detection Systems and processes on all SaaS Cloud Network systems and devices and configured to log system events, network events, and NetFlow to the Cloud Security SIEM. Oracle Cloud Security has established automated controls to monitor and detect 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, evaluated, and maintained by Oracle Corporate Security.<br><br>Oracle Lines of Business (LoBs) are required to capture and store logs for certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html |
| | | Oracle SaaS Cloud security standards are in place to follow Oracle logging and monitoring procedures and are aligned with industry best practices. |
| **LOG-01.2** | Are policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including policies that address logging and monitoring) are reviewed annually and updated as needed. |
| | | LOB is responsible implementing associated procedures. Oracle SaaS Cloud security standards are reviewed and approved annually and updated as needed. |
| **LOG-02.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention? | Oracle SaaS Cloud Security has a defined SaaS Cloud logging and Log Analysis standard and follows Oracle logging and log analysis policy. Logs are automatically collected from the SaaS Cloud Applications and retention of customer data adheres to any applicable government and compliance requirements. |
| **LOG-03.1** | Are security-related events identified and monitored within applications and the underlying infrastructure? | The Oracle SaaS Cloud Logging and Log Analysis Standard sets forth the requirements for regular system monitoring for log generation, storage, retention, and analysis to identify and remediate suspicious and unauthorized activities within SaaS Cloud Applications. |
| **LOG-03.2** | Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics? | Oracle SaaS Cloud Applications uses a proprietary event management system that is defined and implemented to identify and alert, and uses other alarms, when specific events occur in SaaS Cloud Applications and components. The alarm configuration is based on regulatory requirements, industry standards, SaaS Cloud infrastructure conducts internal penetration testing system actions and responses, and security operations round-table discussions. The SIEM users can quickly triage events based on the severity and criticality of the content of the event, including systems, applications, users, or regulatory environment. |
| **LOG-04.1** | Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability? | Oracle SaaS Cloud Logging and Log Analysis Standard defines security and parameters (including retention) for SaaS Cloud Application logs. These logs are restricted and provided on a need-to-know basis. Where possible, log files are protected by SHA 2 cryptographic hash sum and are monitored. Logs on intranet-accessible systems are relocated daily to systems that are not intranet accessible. |

| | | |
|---|---|---|
| **LOG-05.1** | Are security audit logs monitored to detect activity outside of typical or expected patterns? | Oracle SaaS Cloud follows the logging and log analysis policy and audit requirements to identify and remedy suspicious and unauthorized activities which may impact the confidentiality, integrity and availability of SaaS Cloud Applications and information assets on third-party systems. |
| **LOG-05.2** | Is a process established and followed to review and take appropriate and timely actions on detected anomalies? | Oracle SaaS Cloud Detection and Response Team (DART) has defined procedures and processes to ensure appropriate and timely actions are taken on detected anomalies. |
| **LOG-06.1** | Is a reliable time source being used across all relevant information processing systems? | Oracle information system clocks for SaaS Cloud components are synchronized via Network Time Protocol (NTP) to a primary and secondary authoritative time source. |
| **LOG-07.1** | Are logging requirements for information meta/data system events established, documented, and implemented? | Oracle SaaS Cloud x follows the Oracle Cloud Services Logging and Log Analysis standard which defines the standards for log generation, storage, retention, analysis, and log archived retention periods. |
| **LOG-07.2** | Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment? | Oracle SaaS Cloud Security logging processes and threat landscape are continually reviewed, and logging requirement updates are made as necessary to include changing threats. The scope is reviewed annually and updated as needed. If necessary, the scope may be reviewed more frequently. |
| **LOG-08.1** | Are audit records generated, and do they contain relevant security information? | Oracle SaaS Cloud components are configured to log events in accordance with the Oracle SaaS Cloud Security Logging and Log Analysis Standard. The scope of audited events is reviewed and updated at least annually or whenever there is a change in the threat environment. The Oracle SaaS Cloud Security Logging and Log Analysis Standard addresses the required auditable events, content of audit records, audit storage capacity, and responses to auditing failures. |
| **LOG-09.1** | Does the information system protect audit records from unauthorized access, modification, and deletion? | Oracle Security Incident and Event Management (SIEM) is configured on a need-to-know and least privilege basis to protect audit information and logging tools from unauthorized access, modification, and deletion. Oracle SaaS Cloud Security analysts are notified when attempts are detected. |
| **LOG-10.1** | Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls? | Oracle SaaS Cloud monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. There are logs generated and mechanisms in place to review and respond to activity. |
| **LOG-11.1** | Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage? | Oracle SaaS Cloud monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. There are logs generated and mechanisms in place to review activity. |

| | | |
|---|---|---|
| **LOG-12.1** | Is physical access logged and monitored using an auditable access control system? | Oracle SaaS Cloud follows the Logical Access Controls policy and associated requirements to monitor physical access logs. Access mechanisms are configured in a Central Logging System (CLS) to not allow malicious and unintentional alteration of the logs. The standard retention policy for logs is 90 days. |
| **LOG-13.1** | Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated? | Oracle SaaS Cloud processes and measures for reporting and monitoring system anomalies and failures are in place. Oracle SaaS Cloud components generate an alert to accountable service operations teams when audit failure events occur. |
| **LOG-13.2** | Are accountable parties immediately notified about anomalies and failures? | Oracle SaaS Cloud accountable parties are immediately notified about anomalies and failures, SaaS Cloud Applications leverages a Security Information and Event Management (SIEM) solution to correlate information such as system events, firewall logs, WAF logs, network flows from the environment, and to alert on any potential security event. Oracle SaaS Cloud Security personnel monitor the SIEM 24x7x365 and have defined processes to escalate events as needed. This process includes reporting and notification requirements to system owners and Oracle leadership. |

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

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **SEF-01.1** | Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained? | Policies and procedures for security incident management, e-discovery, and cloud forensics are established, documented, approved, communicated, applied, evaluated, and maintained with the oversight of Oracle Global Information Security.<br><br>Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed data has been unproperly handled or accessed. Note that cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available logs and other tooling. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to security events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for security event and incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs).<br><br>GIS defines roles and responsibilities for the incident response teams embedded within the Lines of Business (LoBs). All LoBs must comply with GIS incident response guidance about detecting events and timely corrective actions.<br><br>Upon discovery of an incident, Oracle defines an incident response plan for rapid and effective incident investigation, response, and recovery. Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |

| | | |
|---|---|---|
| | | LOB is responsible implementing associated procedures. Oracle SaaS Cloud Information Security Standard follows the Oracle Global Information Security (GIS) incident management, e-discovery, and cloud digital forensics policy and is applied, evaluated, and maintained. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |
| **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 forensics are reviewed annually and updated as needed.<br><br>Oracle SaaS Cloud Information Security Standards and Incident Response Plan and procedures are reviewed annually and updated as needed. |
| **SEF-02.1** | Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained? | Please see SEF-01.1 |
| **SEF-02.2** | Are policies and procedures for timely management of security incidents reviewed and updated at least annually? | Oracle Corporate Security policies and procedures that address timely management of security incidents are reviewed annually and updated as needed.<br><br>Oracle SaaS Cloud Security policies and procedures for timely management of security events are reviewed annually and updated as needed with the approval of GIS and in accordance with the Corporate Incident Response Plan (CIRP). |
| **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:<br>• Validating that an incident has occurred<br>• Communicating with relevant parties and notifications<br>• Preserving evidence<br>• Documenting an incident itself and related response activities<br>• Containing an incident<br>• Addressing the root cause of an incident<br>• Escalating an incident<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |

| | | |
|---|---|---|
| **SEF-04.1** | Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes? | The Oracle SaaS Cloud Security Incident Response Team (IRT) conducts specialized training to test the effectiveness of the Incident Response Plan (IRP), as it applies to Incident Management and Response GIS policies and is reviewed annually and updated as needed. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |
| **SEF-05.1** | Are information security incident metrics established and monitored? | Information security incident metrics are established and monitored in each Line of Business (LoB) 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? | Oracle SaaS Cloud Information Security Standards and Incident Response Plan are reviewed annually and updated as needed. Incident handling processes, procedures, and technical measures are implemented to support SaaS Cloud Applications and triage security-related events in an efficient and timely manner. |
| **SEF-07.1** | Are processes, procedures, and technical measures for security breach notifications defined and implemented? | In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents and incident history are not shared externally. |
| **SEF-07.2** | Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations? | Please see SEF-01.1<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |
| **SEF-08.1** | Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities? | Oracle maintains points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. |

## Control Domain: Supply Chain Management, Transparency & Accountability

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

| | | |
|---|---|---|
| | communicated, applied, evaluated, and maintained? | Oracle has policies designed to protect the safety of its supply chain, guide how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as selects third-party technology used in corporate and cloud environments. Additionally, Oracle has policies to mitigate the risks associated with the malicious alteration of products before installation by customers.<br><br>Oracle suppliers are required to comply with the Supplier Information and Physical Security Standards of mandatory security controls. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/<br><br>Oracle's Supplier Management Security Policy defines requirements for Lines of Business supplier management programs, to guide selection and management of suppliers each LOB utilizes. |
| | | Oracle SaaS Cloud Security follows security standards and practices of the Shared Security Responsibility Model (SSRM) to implement and meet the Supplier Security Management Policy (SSMP) requirements when engaging and using suppliers. |
| **STA-01.2** | Are the policies and procedures that apply the SSRM reviewed and updated annually? | Oracle SaaS Cloud Security standard follows the Supplier Security Policy and the Supply Chain Security Standard for implementing a Shared Security Responsibility Model (SSRM) process that is reviewed and updated annually and updated as needed. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html. |
| **STA-02.1** | Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering? | Oracle SaaS Cloud Security Shared Security Responsibility Model (SSRM) is applied, documented, implemented, and managed throughout the supply chain for the SaaS Cloud Security Applications. For more information, see: https://www.oracle.com/corporate/suppliers/?er=221886 |
| **STA-03.1** | Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain? | Oracle SaaS Cloud Security follows the Supplier Security Policy and the Supply Chain Security Standard to provide SSRM guidance on the supply chain approval process with Oracle SaaS Cloud products and services. |
| **STA-04.1** | Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering? | Oracle Cloud Hosting and Delivery Policies describe the customer (tenant) security obligations. Also, the Oracle Data Processing Agreement includes the responsibilities of the data controller (tenant/customer) versus data processor (Oracle). For more information see the Oracle Hosting and Delivery Policies and the Oracle Data Processing Agreement at https://www.oracle.com/contracts/cloud-services/ |
| **STA-05.1** | Is SSRM documentation for all cloud services the organization uses reviewed and validated? | Oracle SaaS Cloud Security SSRM documentation is reviewed annually and updated as needed. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html |
| **STA-06.1** | Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed? | Oracle SaaS Cloud Security conducts third-party security assessments in scope with audit standards, including Supplier activities that are aligned with external regulations. |

| | | |
|---|---|---|
| **STA-07.1** | Is an inventory of all supply chain relationships developed and maintained? | Oracle SaaS Cloud developed and maintains an inventory of all supply chain relationships. These agreements define the security, privacy, and compliance controls prior to the onset of services. Oracle SaaS Cloud Security follows the Global Information security (GIS) supplier security program to develop and maintain supply chain relationships. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain |
| **STA-08.1** | Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs? | Oracle SaaS Cloud establishes and maintains a program designed to assess suppliers' risk factors, a risk-based analysis, and appropriate security measures to protect confidential information within the supply chain that is periodically reviewed annually and updated as needed. |
| **STA-09.1** | Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms?<br>• Scope, characteristics, and location of business relationship and services offered<br>• Information security requirements (including SSRM)<br>• Change management process<br>• Logging and monitoring capability<br>• Incident management and communication procedures<br>• Right to audit and third-party assessment<br>• Service termination<br>• Interoperability and portability requirements<br>• Data privacy | See STA-03.1 |
| **STA-10.1** | Are supply chain agreements between CSPs and CSCs reviewed at least annually? | Oracle SaaS Cloud service agreements between CSPs and CSCs are reviewed annually and updated as needed. For more information, see: https://www.oracle.com/be/corporate/contracts/cloud-services/contracts.html |
| **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? | SaaS Cloud assessments are conducted at least annually in alignment with the SaaS Risk Treatment SLAs to define conformance and to effectively update treatment plans. |
| **STA-12.1** | Are policies that require all supply chain CSPs to comply with information security, confidentiality, | Oracle Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when accessing Oracle or Oracle customer facilities, networks and/or information systems, handling Oracle confidential information, or controlling custody of |

| | | |
|---|---|---|
| | access control, privacy, audit, personnel policy, and service level requirements and standards implemented? | Oracle hardware assets. Suppliers are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/suppliers.html |
| **STA-13.1** | Are supply chain partner IT governance policies and procedures reviewed periodically? | Oracle's Supplier Security Management Policy requires all lines of business to maintain a program which manages risk for their suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual supplier review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each supplier's goods or services are leveraged. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ |
| | | The Oracle SaaS Cloud Standard sets forth the requirements governing third-party SaaS Cloud networks, applications, information systems, and servers that are reviewed annually and updated as needed. |
| **STA-14.1** | Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented? | See STA-11.1. |

## Control Domain: Threat & Vulnerability Management

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **TVM-01.1** | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation? | Oracle has formal practices designed to identify, analyze, and remediate the technical security vulnerabilities that may affect our enterprise systems and Oracle Cloud environments.<br><br>The Oracle IT, security and development teams monitor relevant vendor and industry bulletins, including Oracle's own security advisories, to identify and assess relevant security patches. Additionally, Oracle requires that vulnerability scanning using automated scanning systems be frequently performed against the internal and externally facing systems it manages. Oracle also requires that penetration testing activities be performed periodically in production environments.<br><br>Oracle's strategic priority for the handling of discovered vulnerabilities in Oracle Cloud is to remediate these issues according to their severity and the potential impact to the Oracle Cloud Services. The Common Vulnerability Scoring System (CVSS) Base Score is one of the criteria used in assessing the relative severity of vulnerabilities. Oracle requires that identified security vulnerabilities be identified and tracked in a defect tracking system.<br><br>Oracle aims to complete all cloud service remediation activities, including testing, implementation, and reboot/reprovision (if required) within planned maintenance windows. However, emergency maintenance will be performed as required to address severe security vulnerabilities, as described in the Oracle Cloud Hosting and Delivery Policies and, as applicable, associated Pillar documentation. |

| | | |
|---|---|---|
| | | Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud.<br><br>Customers and security researchers can report suspected security vulnerabilities to Oracle: How to Report Security Vulnerabilities to Oracle or by submitting a Service Request in their support system.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html and https://www.oracle.com/corporate/security-practices/assurance/vulnerability/ |
| | | Oracle SaaS Cloud has formal practices designed to identify, analyze, and remediate security vulnerabilities that may affect SaaS Cloud Applications. The SaaS Cloud Threat and Vulnerability Management Standard and procedures define processes to manage discovered vulnerabilities within Oracle SaaS Cloud environments; identifying, maintaining awareness, and to remediate vulnerabilities in all Oracle SaaS Cloud Applications and systems with defined security requirements. |
| **TVM-01.2** | Are threat and vulnerability management policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including policies that address threat and vulnerability management) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud Threat and Vulnerability Management Standard and procedures 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 hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption for their organization. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html |
| | | Oracle SaaS Cloud Security policies and best practices are in place to protect against malware on SaaS Cloud managed assets. Endpoint Management solutions include antivirus scanning, intrusion protection, and firewall solutions on endpoint devices to be applied, evaluated, and maintained on laptops, desktops, and mobile devices. |
| TVM-02.2 | Are asset management and malware protection policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including policies that address asset management and malware protection) are reviewed annually and updated as needed. |
| | | Oracle SaaS Cloud security standards, including standards that address asset management and malware protection, are reviewed annually and updated as needed. |
| TVM-03.1 | Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency | Oracle's SaaS Cloud processes, procedures, and technical measures are defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications - based on the identified risk. |

| | | |
|---|---|---|
| | responses to vulnerability identifications (based on the identified risk)? | |
| 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? | Oracle SaaS Cloud processes, procedures, and technical measures have been defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators on at least a weekly basis and antivirus updates generally occur daily. |
| 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)? | Oracle SaaS Cloud Security Threat and Vulnerability Management standard including processes, procedure, and technical measures are defined, implemented, and evaluated to identify updates for SaaS Cloud applications that use third-party open-source libraries are defined and supported in the Threat and Vulnerability management policy. Oracle SaaS Cloud follows the OSSA standard specific to Supply Chain Security. Additionally, the security and development teams monitor relevant vendor and industry bulletins, including Oracle's security advisories, to identify and assess relevant security patches. Various security testing activities are performed by the SaaS Cloud Application teams throughout the development cycle to identify potential events. These activities include using static and dynamic analysis tools, as well as vulnerability assessment tools. Customers and security researchers can report suspected security vulnerabilities to Oracle per the process documented at Oracle.com: How to Report Security Vulnerabilities to Oracle or by submitting a Service Request in their designated support system (for example, My Oracle Support (MOS) or Support Cloud). |
| TVM-06.1 | Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing? | Oracle SaaS Cloud processes, procedures, and technical measures are in place for independent third-party penetration testing. Oracle regularly performs penetration testing and security assessments against Oracle Cloud infrastructure, platforms, and applications to validate and improve the overall security of Oracle Cloud Services. Additionally, security assessments and penetration tests are performed by a third-party on SaaS Cloud Applications at least annually. Third party penetration testing summary results are available to customers upon request. |
| TVM-07.1 | Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly? | Oracle SaaS Cloud Threat and Vulnerability Management standard defines the methodology for managing discovered vulnerabilities within the SaaS Cloud environment. This standard also defines the scanning requirements and configurations identification and detection tools and processes; remediation timelines; as well as threat intelligence detection of SaaS managed assets at least monthly. For more information see: https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html |
| TVM-08.1 | Is vulnerability remediation prioritized using a risk-based model | Oracle uses the Common Vulnerability Scoring System (CVSS) to report the relative severity of security vulnerabilities when it discloses them. CVSS Base Score information is provided in the risk matrices published in Critical Patch Update and Security Alert Advisories. Oracle uses Common Vulnerabilities and Exposures (CVE) numbers to identify the vulnerabilities listed in the risk matrices in Critical Patch Update |

| | | |
|---|---|---|
| | from an industry-recognized framework? | and Security Alert advisories. For more information, see: https://www.oracle.com/corporate/security-practices/assurance/vulnerability/ |
| | | Oracle SaaS Cloud uses Common Vulnerability Scoring System (CVSS) to report relative severity of security vulnerabilities. Vulnerabilities are remediated in order of the risk they pose to users. This process is designed to patch the security holes with the greatest associated risk first, resulting in optimizing the security posture of all Oracle customers. |
| TVM-09.1 | Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification? | Oracle SaaS Cloud Security Vulnerability Management Security Standard establishes the requirements to track and report vulnerabilities including identification and remediation updates. For more information on Critical Patch Updates, Security Alerts and Bulletins see Critical Patch Updates, Security Alerts and Bulletins. |
| TVM-10.1 | Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals? | Oracle SaaS Cloud security has defined metrics to monitor vulnerabilities as they are identified through remediation processes, including the Security Health Review and Vulnerability Management Advocacy Program to monitor all vulnerabilities and remediation steps monthly. |
| Control Domain: Universal Endpoint Management | | |
| Question ID | Consensus Assessment Question | Oracle Response |
| UEM-01.1 | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints? | Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops, and mobile devices. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption.<br><br>Oracle employees are required to comply with email instructions from Oracle Information Technology teams and are responsible for promptly reporting to the Oracle employee helpdesk any virus or suspected virus infection that cannot be resolved by antivirus software. Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html |
| | | Oracle SaaS Cloud Security maintains a security standard that follows the GIS Endpoint Device Security policy and legal Information Protection policy to ensure security requirements for all Cloud SaaS user endpoint devices and Cloud SaaS Application user endpoint protection environments which hold customer data are protected and are aligned with industry standards and reviewed during re-accreditation. |
| UEM-01.2 | | Oracle Corporate Security policies (including policies that address universal endpoint management) are reviewed annually and updated as needed. |

| | | |
|---|---|---|
| | Are universal endpoint management policies and procedures reviewed and updated at least annually? | Oracle SaaS Cloud Security maintains a security standard in accordance with the GIS Endpoint Device Security policy and Legal Information Protection policy that are reviewed annually and 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? | Please see UEM-01.1. This list is approved by Oracle Corporate Architecture and maintained by Oracle Information Technology. |
| | | Oracle SaaS Cloud Security defines applicable requirements for Universal Endpoint Management (UEM) when accessing or storing Oracle SaaS Cloud data and privacy information. |
| UEM-03.1 | Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications? | Please see UEM-01.1. Endpoint validation is performed by automation approved by Oracle Corporate Architecture and maintained by Oracle Information Technology. |
| | | Oracle SaaS Cloud Security implements processes to validate endpoint device compatibility with operating systems and applications with the Universal Endpoint Management (UEM) services requirements. |
| UEM-04.1 | Is an inventory of all endpoints used and maintained to store and access company data? | Oracle's Information Systems Asset Inventory Policy requires that Line of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware and software. |
| UEM-05.1 | Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, 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 lines of business management to verify deployment of device encryption.<br><br>To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full disk encryption software on their laptops and desktops, except where approved for justifiable business purposes. Data on the disk can only be accessed through the use of a private key stored as a password-protected file on the disk. A preboot login manager allows authorized users to login to unlock the key, boot the operating system, and access the data. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html |
| | | Oracle SaaS Cloud Services devices that maintain Oracle SaaS Cloud customer information on user devices must be encrypted using an Oracle Corporate approved endpoint encryption solution that validates endpoint encryption compliance monitoring, and a local firewall is installed to enforce policies and security controls. |
| UEM-06.1 | Are all relevant interactive-use endpoints configured to require an automatic lock screen? | Oracle SaaS Cloud Services devices have a secure desktop management software installed on interactive-used endpoints that is configured to require an automatic lock screen, automatically locks the screen after a defined period of inactivity. SaaS Cloud Applications enforce an automatic lock screen as a default setting that cannot be changed. |

| | | |
|---|---|---|
| UEM-07.1 | Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process? | The Oracle Information Technology keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. OIT is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. OIT provides automation to verify antivirus configuration.<br><br>Oracle employees are required to comply with email instructions from OIT and are responsible for promptly reporting to the Oracle employee helpdesk any virus or suspected virus infection that cannot be resolved by antivirus software.<br><br>Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer.<br><br>For more information, see: https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html |
| | | Oracle SaaS Cloud follows the Endpoint Device Security Policy requirement to follow the change management process during security updates to endpoint operating systems and SaaS applications patches to protect all user endpoint devices. |
| UEM-08.1 | Is information protected from unauthorized disclosure on managed endpoints with storage encryption? | Please see UEM-05.1. |
| UEM-09.1 | Are anti-malware detection and prevention technology services configured on managed endpoints? | Antivirus software must be scheduled to perform threat definition updates and virus scans. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html |
| UEM-10.1 | Are software firewalls configured on managed endpoints? | Oracle SaaS Cloud follows the SaaS Network Security Standard for virtual firewall rules. The internal software firewalls are configured on endpoint devices to protect SaaS Cloud Applications. |
| UEM-11.1 | Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment? | Oracle SaaS Cloud Applications do not have a commercial DLP deployed. Oracle SaaS Cloud Security workstations with access to scoped data and servers containing SaaS Cloud Services information is managed with DLP-type technologies to secure confidential information and endpoints. |
| UEM-12.1 | Are remote geolocation capabilities enabled for all managed mobile endpoints? | Unless required by regional or governmental regulations, geolocation capabilities are not in place for mobile endpoints. |
| UEM-13.1 | Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices? | Oracle SaaS Cloud Security sets forth the standards, procedures, and security requirements to secure desktop and mobile device management software with remote wipe capabilities. For more information please see: https://www.oracle.com/secure-global-desktop/#rc30p2 |

| | | |
|---|---|---|
| UEM-14.1 | Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets? | Oracle has formal requirements for its suppliers to confirm they protect 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:<br>• Accessing Oracle and Oracle customers' facilities, networks and/or information systems<br>• Handling Oracle confidential information, and Oracle hardware assets placed in their custody<br><br>In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ |
| | | SaaS Cloud Security defines third-party security requirements for its suppliers to confirm they protect third-party information that is entrusted to them. The Oracle SaaS Cloud Third-Party Access Standard defines security controls that Oracle SaaS Cloud vendors and third parties must comply; technical and contractual measures that are defined, implemented, and evaluated when accessing Oracle SaaS Cloud Applications and services assets. |

## 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