ORACLE

# Consensus Assessment Initiative Questionnaire (CAIQ) v4.0 for Oracle Health Insurance Cloud Services (OHI CS)

March 2025| Version 4.0

## 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

List your GIU Service in scope

This documentation applies to the following cloud offering of Oracle Health Insurance Cloud Services (OHI CS) for the OHI CS customers i.e. customers of one or a combination of the following cloud services:

- Oracle Health Insurance Policy Administration Cloud Service
- Oracle Health Insurance Claims Administration Cloud Service
- Oracle Health Insurance Claims and Policy Administration Cloud Service, SMB

## ORACLE CLOUD INFRASTRUCTURE AND GLOBAL INDUSTRY UNITS

The services listed above as in scope for this document run with Oracle Cloud Infrastructure (OCI). The Global Industry Units (GIUs) rely on a base set of security controls enforced by OCI for the Operating Systems and Network

security layers.  For all answer that refer to OCI Security Standards and/or processes the GIU has no ability and/or access to manage those functions.  Where the GIU has additional controls those will be specified.  For additional information on the specifics for answers referring to OCI Standards you can find the OCI CAIQ at https://www.oracle.com/corporate/security-practices/cloud/

# CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ) VERSION 4

| Control Domain: Audit & Assurance | | |
|---|---|---|
| **Question ID** | **Consensus Assessment Question** | **Oracle Response** |
| **A&A-01.1** | Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained? | Oracle's Business Assessment & Audit (BA&A) is an independent global audit organization which performs global processes and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards and select laws and regulations across Oracle's Lines of Business (LOB) and business units. Any key risks or control gaps identified by BA&A during these reviews are tracked through remediation. These reviews, identified risks, or control gaps are confidential and shared with executive leadership and Oracle's Board of Directors.<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/.<br><br>The audit rights of customers of Oracle services are described in the Oracle Services Privacy Policy. For more information, see https://www.oracle.com/legal/privacy/services-privacy-policy.html |
| | | Oracle Health Insurance Cloud Services implement audit and assurance policies, procedures, and standards documented and approved. Oracle Health Insurance Cloud Services performs HIPAA, SOC 1 and SOC 2 audits annually, as well as IRAP bi-annually. These are available for customer review upon request. |
| **A&A-01.2** | Are audit and assurance policies, procedures, and standards reviewed and updated at least annually? | GIU Standards that follow Oracle Corporate Security policies are reviewed annually and updated as needed. |
| **A&A-02.1** | Are independent audit and assurance assessments conducted according to relevant standards at least annually? | See A&A-01.1. Oracle's Business Assessment & Audit (BA&A) is independent. Its operational activities and procedures are conducted at least annually in alignment with the Institute of Internal Auditors (IIA) Standards. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/business-assessment-audit/ |
| | | Independent external audits and assessments of Oracle Health Insurance Cloud Services are conducted on an annual or bi-annual basis based on the audit. Existing Customers may request access to current audit reports via the Customer Support portal (ICCP) or via contacting Sales directly. |
| **A&A-03.1** | Are independent audit and assurance | 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). |

| | | |
|---|---|---|
| | assessments performed according to risk-based plans and policies? | GIU Service audits are approved based on risk plans reviewed under Oracle risk policies and standards. For more information, see https://www.oracle.com/corporate/cloud-compliance/. |
| **A&A-04.1** | Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit? | Oracle Health Insurance Cloud Services engages with external assessment entities and independent auditors to verify that Oracle Health Insurance Cloud Services have a comprehensive control environment that includes policies, processes, and security controls for the delivery of applications. Infrastructure and Platform services for Oracle Health Insurance Service are provided by Oracle Cloud Infrastructure. These efforts conform with ISO/IEC 27001 standards and Oracle Corporate Security Policies. For more information see: https://www.oracle.com/corporate/cloud-compliance/. |
| **A&A-05.1** | Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence? | An audit management process inclusive of risk analysis, security control assessments, remediation schedules and reporting is in place for Oracle Health Insurance Cloud Services Oracle Health Insurance Cloud Services also undergoes HIPAA, SOC 1 and SOC 2 audits annually, as well as IRAP bi-annually. |
| **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. |
| | | A risk-based corrective plan to remediate audit findings is in place. Any key risks or control gaps identified during an internal or external compliance assessment for Oracle Health Insurance Cloud follow a defined process following a risk-based approach to remediation. |
| **A&A-06.2** | Is the remediation status of audit findings reviewed and reported to relevant stakeholders? | Risks identified by Oracle's Business Assessment & Audit (BA&A) and associated action item status are confidential and shared with executive leadership and Oracle's Board of Directors. |
| | | Oracle Health Insurance Cloud Application's remediation status of audit findings is reviewed and reported to appropriate stakeholders until findings are resolved. |

## Control Domain: Application & Interface Security

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|

| | | |
|---|---|---|
| **AIS-01.1** | Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities? | Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience.<br><br>Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at:<br><br>**Reducing the incidence of security weaknesses in all Oracle products.**<br><br>Oracle Software Security Assurance key programs include Oracle's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups, and the use of automated analysis and testing tools.<br><br>**Reducing the impact of security weaknesses in Oracle products and services**<br><br>Oracle has mature security vulnerability disclosure and remediation practices. The company is committed to treating all customers equally and delivering the best possible security maintenance experience through the Critical Patch Update and Security Alert programs.<br><br>**Fostering security innovations.**<br><br>Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help enable organizations to implement and manage consistent security policies across the hybrid cloud data center: database security and identity management, and security monitoring and analytics.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/assurance/ |
| | | |
| **AIS-01.2** | Are application security policies and procedures reviewed and updated at least annually? | Oracle Health Insurance Cloud Services follows the Oracle Corporate Security policies as well as the OCI Secure Service Development Standard. The policies and standards are reviewed annually and updated as needed. |
| **AIS-02.1** | Are baseline requirements to secure different applications established, documented, and maintained? | Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/configuration.html |
| | | Oracle Health Insurance Cloud development teams are required to deliver the service to cloud operations teams in a secured configuration. The security of cloud configurations is planned from the design phase by the development team. Testing is performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment |
| **AIS-03.1** | Are technical and operational metrics defined and | Technical and operational metrics are in place to help drive compliance to business objectives, security requirements and compliance obligations. Oracle Health Insurance Cloud Services teams maintain a set of defined technical and operational metrics to monitor alignment to business objectives, security requirements and compliance obligations. An |

| | | |
|---|---|---|
| | implemented according to business objectives, security requirements, and compliance obligations? | example program for managing the security of Oracle's architecture is the Corporate Security Solution Assurance Process (CSSAP). CSSAP is a security review process developed by Corporate Security Architecture, Global Information Security, Global Product Security, and Oracle's IT organizations to provide comprehensive information-security management review. |
| **AIS-04.1** | Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements? | To ensure that Oracle products are developed with consistently high security assurance, and to help developers avoid common coding mistakes, Oracle employs formal Secure Coding Standards. Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. All Oracle developers are required to be familiar with these standards and apply them when designing and building products. The coding standards have been developed over several years and incorporate best practices as well as lessons learned from ongoing vulnerability testing by Oracle's internal product assessment teams. The Secure Coding Standards are a key component of Oracle Software Security Assurance and alignment to the Standards is assessed throughout the supported life of all Oracle products. |
| | | Oracle Health Insurance Cloud Services follow the Oracle Software Security Assurance (OSSA) standards throughout the supported lifecycle. For more information, see https://www.oracle.com/corporate/security-practices/assurance/<br><br>Following OCI Secure Service Development Standard, all code reaching production systems, or delivered to customers, must be built using a build system approved by OCI Security. |
| **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 Health Insurance Cloud Services have defined testing strategies as part of our Development Security Operations (DevSecOps) development principles. We consistently validate all Cloud Service application upgrades through a defined vulnerability testing process. Oracle regularly performs penetration and vulnerability testing and security assessments against the Oracle Cloud infrastructure, platforms, and applications. These tests are intended to validate and improve the overall security of Oracle Health Insurance Cloud Services. |

| | | |
|---|---|---|
| **AIS-05.2** | Is testing automated when applicable and possible? | Oracle Health Insurance Cloud Services includes automated testing within the SDLC. |
| **AIS-06.1** | Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner? | Cloud services are deployed in a specific configuration, or a small number of configurations. Testing must be performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment. Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/configuration.html<br><br>Oracle Health Insurance Cloud Service deployments are undertaken over secured connections, code is scanned for potential threats with rigid access control and clear separation of duties throughout the development team. |
| **AIS-06.2** | Is the deployment and integration of application code automated where possible? | Yes, deployment and integration of application code are automated using CI/CD pipelines. |
| **AIS-07.1** | Are application security vulnerabilities remediated following defined processes? | Oracle fixes significant security vulnerabilities based on the likely risk they pose to customers. The issues with the most severe risks are fixed first. Fixes for security vulnerabilities are produced in the following order:<br>• Main code line first—that is the code line being developed for the next major release of the product<br>• For each supported version that is vulnerable:<br>  ○ Fix in the next patch set if another patch set is planned for that supported version<br>  ○ Creation of Critical Patch Update patch<br>For more information, see https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html<br><br>Application security vulnerabilities are identified and remediated following defined processes. Oracle Health Insurance Cloud Services follow a clearly defined process for regularly testing, assessing, evaluating, and maintaining the effectiveness of the technical and organizational security measures such as:regular vulnerability scans are conducted. Oracle Health Insurance Cloud Developers use static and dynamic analysis tools to detect security defects in Oracle code prior to deploying to production. Identified issues are evaluated and addressed in order of priority and severity. Oracle Health Insurance Cloud Services management tracks metrics regarding issue identification and resolution. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html |
| **AIS-07.2** | Is the remediation of application security vulnerabilities automated when possible? | Oracle Health Insurance Cloud Services security vulnerabilities are remediated through the build and release pipeline. All application security updates are delivered through security patches and this process is automated whenever possible. Oracle Health Insurance Cloud Services development teams are required to deliver the service to cloud operations teams in a secured configuration. Testing is performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment |

## Control Domain: Business Continuity Management & Operational Resilience

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **BCR-01.1** | Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained? | The Risk Management Resiliency Program (RMRP) objective is to establish a business resiliency framework to enable efficient Line of Business (LOB) response to business interruption events affecting Oracle's operations. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/<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. |
| | | Oracle Health Insurance Cloud Services have a detailed SaaS Business Continuity / Disaster Recovery (BCDR) Program. The details of the SaaS Cloud Services BCDR program are covered under the Risk Management resiliency Program (RMRP). The program is driven by Policy documents like H&D Policy, DPA and SaaS Pillar Document. Risk Assessment, Business Impact Analysis and Business Continuity Plans are annually reviewed and updated. For operational purposes Crisis Communication Plan, DR Staffing Plan and Disaster Recovery Procedures are maintained. Periodic exercises are executed, results are documented, and findings are followed through to completion. Customer facing Disaster Recovery Test summary reports are published upon completion of each DR test cycle. See for additional information: https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf |
| **BCR-01.2** | Are the policies and procedures reviewed and updated at least annually? | The RMRP policy mandates an annual operational cycle for (LoB) planning, evaluation, training, validation, and executive approvals for critical business operations.<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 RMRP Program Management Office (PMO) has oversight responsibilities for the LoB compliance to the program. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/ |
| | | Oracle Health Insurance Cloud Services policies (including business continuity management and operational resilience policies) are reviewed annually and updated as needed. |
| **BCR-02.1** | Are criteria for developing business continuity and | The RMRP Program is generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance. For more information about the program and requirements for Oracle Lines of Business, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/ |

| | | |
|---|---|---|
| | operational resiliency strategies and capabilities established based on business disruption and risk impacts? | Criteria used for Oracle Health Insurance Cloud Services business continuity and operational resilience strategies are based on industry requirements and aligned with the Oracle RMRP program. |
| **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? | See BCR-03.1 |
| **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 Health Insurance Cloud Services Risk Assessment, Business Impact Analysis and Business Continuity Plans are documented, developed, maintained, and updated to support business continuity and operational resilience plans. |
| **BCR-05.2** | Is business continuity and operational resilience documentation available to authorized stakeholders? | Business Continuity and operational resilience documentation is available to internal authorized stakeholders. |

| | | |
|---|---|---|
| **BCR-05.3** | Is business continuity and operational resilience documentation reviewed periodically? | The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations. See BCR-03.1 |
| | | Oracle Health Insurance Cloud Services reviews its business continuity documentation at least annually in accordance with Oracle Corporate policy and updated as needed. |
| **BCR-06.1** | Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur? | The critical LoBs (including Oracle Health Insurance Cloud Services ) are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resiliencemanagement/business-continuity.html |
| | | Oracle Health Insurance Cloud Services have a detailed SaaS Business Continuity / Disaster Recovery (BCDR) Program. The details of the SaaS Cloud Services BCDR program is covered under the Risk Management resiliency Program (RMRP). Oracle Health Insurance Cloud Services conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability. |
| **BCR-07.1** | Do business continuity and resilience procedures establish communication with stakeholders and participants? | Oracle Health Insurance Cloud Services have a detailed SaaS Business Continuity / Disaster Recovery (BCDR) Program. The details of the SaaS Cloud Services BCDR program is covered under the Risk Management resiliency Program (RMRP). The procedures establish a communication plan for stakeholders and participants.<br>See: https://www.oracle.com/corporate/security-practices/corporate/resilience-management/ |
| **BCR-08.1** | Is cloud data periodically backed up? | Oracle Health Insurance Cloud Services maintains a production backup of data which is undertaken in accordance with the Oracle hosting and delivery policy https://www.oracle.com/corporate/contracts/cloudservices/hosting-delivery-policies.html |
| **BCR-08.2** | Is the confidentiality, integrity, and availability of backup data ensured? | Oracle Health Insurance Cloud Services must meet applicable control plane and data plane backup requirements, as defined by the Cloud Compliance Standard for Resilience and Crisis Management. Backups are monitored, and issues relating to backup failure are tracked to resolution. |
| **BCR-08.3** | Can backups be restored appropriately for resiliency? | Oracle Health Insurance Cloud Services undertakes as published in the "Oracle Hosting and Delivery Policy": https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html. Oracle Health Insurance Cloud Services do not undertake restoration of data on behalf of customers. Customer data should be exported directly via the Oracle Health Insurance Cloud Services. |
| **BCR-09.1** | Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural | Oracle's corporate Disaster Recovery (DR) plan focuses on the resiliency of computing infrastructure supporting Oracle's internal operations and cloud services. Oracle's production data centers are geographically separated and have component and power redundancy, with backup generators in place for availability of data center resources in case of a disaster, whether natural or man-made.<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/disaster-recovery.html. |

| | | |
|---|---|---|
| | and man-made disasters? | Oracle Health Insurance Cloud Services conduct annual reviews of their business continuity plans with the objective of maintaining operational recovery capability. |
| **BCR-09.2** | Is the disaster response plan updated at least annually, and when significant changes occur? | Oracle Health Insurance Cloud Services DR and BCR plans are reviewed annually and updated as needed to maintain operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. |
| **BCR-10.1** | Is the disaster response plan exercised annually or when significant changes occur? | Oracle Health Insurance Cloud Services DR and BCR plans are reviewed annually and exercised annually or as needed when significant changes occur. |
| **BCR-10.2** | Are local emergency authorities included, if possible, in the exercise? | Oracle generally does not involve external 3rd parties during DR exercise. |
| **BCR-11.1** | Is business-critical equipment supplemented with redundant equipment independently located at a reasonable 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 deploys the Oracle Health Insurance Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services. For more information, please refer to the following documents at https://www.oracle.com/contracts/cloud-services/Oracle Industries Cloud Services Pillar Oracle Cloud Hosting and Delivery Policies |

## Control Domain: Change Control & Configuration Management

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|

| | | |
|---|---|---|
| **CCC-01.1** | Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)? | Oracle Health Insurance Cloud Services follow formal change management procedures to provide review, testing, and approval of changes prior to deployment in the Oracle Cloud production environment. Changes made through change management procedures include system and service maintenance activities, management of application upgrades and updates, and coordination of customer specific changes where required. For changes to your services that are governed by Oracle's change control procedures please see: Oracle Cloud Hosting and Delivery Policies. https://www.oracle.com/contracts/cloud-services/ |
| **CCC-01.2** | Are the policies and procedures reviewed and updated at least annually? | Oracle Health Insurance Cloud Services follows Oracle Corporate policies and reviews Oracle Health Insurance Cloud Applications standards annually and updates as needed. |
| **CCC-02.1** | Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed? | Oracle Health Insurance Cloud Services are deployed using a strict, baseline deployment which helps implement consistent deployment standards against each version release. |
| **CCC-03.1** | Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)? | Oracle Corporate Security Solution Assurance Process (CSSAP) is a security review process developed by Corporate Security Architecture, Global Information Security, Global Product Security, Oracle Global IT, and Oracle's IT organizations to provide comprehensive information-security management review whether asset management occurs internally or externally. CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle:<br>• Pre-review: the risk management teams in each line of business must perform a pre-assessment of each project using the approved template<br>• CSSAP review: the security architecture team reviews the submitted plans and performs a technical security design review<br>• Security assessment review: based on risk level, systems and applications undergo security verification testing before production use<br><br>Reviews ensure that projects are aligned with:<br>• Oracle Corporate Security Architecture strategy and direction |

| | | |
|---|---|---|
| | | • Oracle Corporate security, privacy and legal policies, procedures and standards<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html |
| | | Oracle Health Insurance Cloud Services are required to follow the Corporate Security Assurance Process (CSSAP) process. |
| **CCC-04.1** | Is the unauthorized addition, removal, update, and management of organization assets restricted | Oracle's Network Security Policy establishes requirements for network management, network access and network device management, including authentication and authorization requirements for both physical devices and software-based systems.<br><br>For more information, https://www.oracle.com/corporate/security-practices/corporate/access-control.html<br><br>Oracle's Information Systems Asset Inventory Policy requires that an accurate and current inventory be maintained for all information systems holding critical and highly critical information assets in Oracle Corporate and cloud infrastructures, including the physical location.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html |
| | | Oracle Health Insurance Cloud Services follow the Oracle Corporate policies and standards that are in place outlining restrictions for adding, removing, and updating Oracle assets. Additionally, technical restrictions are in place where possible. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html |
| **CCC-05.1** | Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs? | Follow the OCI Secure Service Development Standard:<br><br>• All code reaching production systems, or delivered to customers, must be built using a build system approved by OCI Security.<br>• All applications must be deployed using an approved OCI deployment system.<br>• Production systems must use a mechanism approved by OCI Security to verify code origin and scanning status before deployment. |
| **CCC-06.1** | Are change management baselines established for all relevant authorized changes on organizational assets? | Change management baselines are established for all relevant authorized changes on Oracle Health Insurance Cloud Services assets. |
| **CCC-07.1** | Are detection measures implemented with | Detection measures are implemented with proactive notification for changes to a customer's environment that deviate from established baseline configurations. Oracle Health Insurance Cloud Services use a centralized system for |

| | | |
|---|---|---|
| | proactive notification if changes deviate from established baselines? | managing the access and integrity of device configurations. Change controls are in place to help ensure only approved changes are applied. Independent 3rd party audits are performed to confirm compliance with security and operational procedures. Also, internal scans are performed by OCI on the Oracle Health Insurance Could Services the infrastructure. |
| **CCC-08.1** | Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process? | Oracle Health Insurance Cloud Services have implemented standards and procedures to manage exceptions, including emergencies, in the change and configuration process. |
| **CCC-08.2** | Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process? | Please see CCC-01.1 Oracle Health Insurance Cloud Services exception process aligns with the GRC-04: Policy Exception Process. |
| **CCC-09.1** | Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns? | Changes to Oracle Health Insurance Cloud Services environments do include provisions to revert change if necessary. Processes are in place to proactively roll back changes to a previously known "good state". Standard operating procedures (SOP) define the steps to follow, including implementation, pre/peri/post validation, and rollback, as applicable. |

## Control Domain: Cryptography, Encryption & Key Management

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **CEK-01.1** | Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained? | Oracle has formal cryptography, encryption, key management requirements, cryptographic algorithms and protocols. Compliance with these requirements is monitored by Oracle Global Product Security. Oracle products are required to use up-to-date versions of approved security-related implementations. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms. Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption when data is at rest (in storage) on laptops, devices, and removable media. For more information, seehttps://www.oracle.com/corporate/security-practices/corporate/data-protection/ |
| | | Oracle Health Insurance Cloud Services follows the documented standards supporting Oracle corporate encryption and key management policies. These standards are documented, managed, communicated, applied, and evaluated. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html |

| | | |
|---|---|---|
| **CEK-01.2** | Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including polices that address cryptography, encryption, and key management) are reviewed annually and updated as needed.<br><br>Oracle Health Insurance Cloud Services review encryption and key management procedures at least annually and updates these as needed. |
| **CEK-02.1** | Are cryptography, encryption, and key management roles and responsibilities defined and implemented? | Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services. The group is primarily responsible for making technical decisions and authoring internal standards to address government and industry requirements. Representatives from Corporate Security and development organizations define best practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence, and including roles and responsibilities. CRB's responsibilities include:<br><br>• Creating and maintaining standards for cryptography algorithms, protocols, and their parameters<br>• Providing approved standards in multiple formats, for readability and automation<br>• Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle<br>• Providing practical guidance on using cryptography<br>• Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography<br><br>Oracle Health Insurance Cloud Services review cryptography roles and responsibilities in accordance with Oracle Corporate policy and must be approved by the Corporate Security Solution Assurance Process (CSSAP). For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html |
| **CEK-03.1** | Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards? | Solutions for managing encryption keys and cryptographic libraries at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). Oracle Global IT defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include:<br><br>• Locations and technologies for storing encryption keys<br>• Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures<br>• Changing default encryption keys<br>• Replacement schedule for various types of encryption keys<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html |

| | | |
|---|---|---|
| | | |
| | | Oracle Health Insurance Cloud Services encrypts data at-rest and in transit in accordance both with Oracle corporate policy. |
| **CEK-04.1** | Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability? | Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to only use up-to-date versions of approved security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms.<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html |
| | | Appropriate data protection encryption algorithms are used based on data classification, associated risks, and encryption technology usability for Oracle Health Insurance Cloud Services. |
| **CEK-05.1** | Are standard change management procedures established to review, approve, implement, and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources? | Change management is mandatory for all Oracle cryptography. Oracle Global IT defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include:<br>• Locations and technologies for storing encryption keys<br>• Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures<br>• Changing default encryption keys<br>• Replacement schedule for various types of encryption keys<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html |
| | | Oracle Health Insurance Cloud Services manage its change management processes in relation to cryptography in alignment with Oracle corporate policy |
| **CEK-06.1** | Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, | 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 Health Insurance Cloud Services follows these standards and must be approved per the Corporate Security Solution Assurance Process (CSSAP). |

| | | |
|---|---|---|
| | including residual risk, cost, and benefits analysis? | |
| **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><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html |
| | | Oracle Health Insurance Cloud Services are aligned with Oracle Corporate Security practices regarding the use of cryptography. |
| **CEK-08.1** | Are CSPs providing CSCs with the capacity to manage their own data encryption keys? | No, Oracle Health Insurance Cloud Services undertakes all data encryption on behalf of the Customer. |
| **CEK-09.1** | Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event? | Encryption and key management systems, policies and processes are audited as part of Oracle Health Insurance Cloud Services compliance function. Please see CEK-01.1 |
| **CEK-09.2** | Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)? | Encryption and key management systems, policies, and processes are audited, at a minimum, on an annual basis. |
| **CEK-10.1** | Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications? | Oracle Health Insurance Cloud Services use the up-to-date versions of the Oracle formal cryptography, encryption, and key management requirements and approved security-related implementations. Oracle modifies these standards as industry and technology evolve.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/ |

| | | |
|---|---|---|
| **CEK-11.1** | Are private keys provisioned for a unique purpose managed, and is cryptography secret? | Oracle Health Insurance Cloud Services keys are provisioned and stored in accordance with Oracle policy. Oracle policy and standards require all keys to be managed securely. |
| **CEK-12.1** | Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements? | Oracle has a formal Key Management Program supported by processes, procedures, and recommendations () that define specifics regarding key rotation. For Oracle Health Insurance Cloud Services, cryptographic key rotation occurs based on regulation, certification, or for other security reasons. |
| **CEK-13.1** | Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions? | Oracle Health Insurance Cloud Services cryptographic keys are revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions. |
| **CEK-14.1** | Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions? | Oracle Corporate has defined processes and technical measures in place that define the approved methods for key destruction, revocation of keys stored in hardware security modules and that help address legal and regulatory requirements. Oracle Health Insurance Cloud Services have established and implemented procedures to enforce segregation of key management and key usage duties. Key management encompasses the entire life cycle of cryptographic keys and has identified a method for establishing and managing keys in each management phase from generation, installation, storage, rotation, and destruction. |

| | | |
|---|---|---|
| **CEK-15.1** | Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions? | Oracle Health Insurance Cloud Services has processes, procedures, and technical measures for creating keys in a pre-activated state. Keys are not created prior to authorization to use. |
| **CEK-16.1** | Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions? | Oracle Health Insurance Cloud Services has processes, procedures, and technical measures in place to monitor, review and approve key transitions. Oracle Health Insurance Cloud Services leverages key management software that allows for the approval and change of state for all key change or state 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? | Oracle Health Insurance Cloud Services has processes, procedures, and technical measures in place to deactivate keys as required. Oracle Health Insurance Cloud Services leverages key management software that allows for the deactivation and key change of state. |
| **CEK-18.1** | Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, | Oracle Health Insurance Cloud Services has processes, procedures, and technical measures in place to manage archived keys in a secure repository where access control following the principle of least privilege is in place. |

| | | |
|---|---|---|
| | implemented, and evaluated to include legal and regulatory requirement provisions? | |
| **CEK-19.1** | Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions? | Oracle Health Insurance Cloud Services have formal processes, procedures, and technical measures for encrypting customer data in transit (e.g., HTTPS TLS 1.2, SFTP) and at rest (e.g., currently AES-256). |
| **CEK-20.1** | Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions? | Processes, procedures, and technical measures to assess operational continuity risks are defined, implemented, and evaluated to include legal and regulatory requirement provisions. |
| **CEK-21.1** | Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and | Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services, including legal and regulatory requirements. Oracle Health Insurance Cloud Service's use these key management system processes, procedures, and technical measures as defined. For more information see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html |

| | | |
|---|---|---|
| | regulatory requirements provisions? | |

## 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 Health Insurance Cloud Services have processes and procedures to comply with Oracle's Media Sanitization and Disposal Policy and Enterprise Engineering Media Sanitization and Disposal Standard. |
| **DCS-01.2** | Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed? | Oracle's Media Sanitation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data.<br><br>For more information, https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html<br><br>Oracle Health Insurance Cloud Services is aligned with Oracle's Media Sanitization and Disposal Policy. |
| **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 polices that address secure disposal of equipment outside the organization's premises) are reviewed annually and updated as needed.<br><br>Oracle Health Insurance Cloud Services follow the Oracle Corporate Security policies, including polices that address secure disposal of equipment outside the organization's premises. |
| **DCS-02.1** | Are policies and procedures for the relocation or transfer of hardware, software, or | 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 |

| | | |
|---|---|---|
| | data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained? | Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services, including legal and regulatory requirements. Oracle Health Insurance Cloud Service's use these key management system processes, procedures, and technical measures for its hardware lifecycle and data information policy. Accurate and comprehensive inventories of information systems, hardware and software are maintained and updated regularly. |
| **DCS-02.2** | Does a relocation or transfer request require written or cryptographically verifiable authorization? | Oracle Health Insurance Cloud Services require manager approval for the relocation of all datacenter assets in accordance with published corporate policy. For more information, see the 'Oracle Cloud Change Management Policy' section of the Oracle Cloud Hosting and Delivery Policies document.: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html |
| **DCS-02.3** | Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually? | Oracle Corporate Security policies (including polices that address the relocation or transfer of hardware, software, or data/information to any location) are reviewed annually and updated as needed.<br><br>Oracle Health Insurance Cloud Services follow the Oracle Corporate Security policies, including the polices that address secure disposal of equipment outside the organization's premises. |
| **DCS-03.1** | Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained? | Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html<br><br>Oracle Health Insurance Cloud Services relies on Oracle Global Physical Security to manage all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. |
| **DCS-03.2** | Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually? | Oracle Corporate Security policies (including polices that address safe and secure working environments) are reviewed annually and updated as needed.<br><br>Oracle Health Insurance Cloud Services relies on Oracle Global Physical Security to manage all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. See https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html |

| | | |
|---|---|---|
| **DCS-04.1** | Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained? | For the secure transportation of physical media are established, documented, approved, communicated, enforced, evaluated, and maintained. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/ |
| **DCS-04.2** | Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually? | Oracle Corporate Security policies (including polices that address the secure transportation of assets) are reviewed annually and updated as needed. |
| | | Oracle Health Insurance Cloud Services follows the "Secure Data Transfer using Encrypted Media" Standard Operating Procedure. This SOP defines hardware requirements, encryption levels and the procedural steps that must be taken to transport physical media. This SOP is reviewed annually and updated as needed. |
| **DCS-05.1** | Is the classification and documentation of physical and logical assets based on the organizational business risk? | Oracle's formal Information Protection Policy sets forth the requirements for classifying and handling public and confidential information. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html |
| | | Per the Oracle Information Protection Policy, Oracle Health Insurance Cloud Services information assets are classified according to the sensitivity and criticality of information they store, transmit, and receive. |
| **DCS-06.1** | Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system? | The Oracle Information Systems Inventory Policy requires that Lines of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware, and software. Inventories must be managed within an approved inventory system. This policy defines required identifying attributes to be recorded for server hardware, software, data held on information systems, and information needed for disaster recovery and business continuity purposes. |
| | | Oracle Health Insurance Cloud Services catalogues and tracks assets following the Oracle Information Systems Inventory Policy. This policy requires accurate and comprehensive inventory of information systems, hardware, and software. Inventories must be managed within an approved inventory system. All system access is provisioned on a need-to-know basis. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html |
| **DCS-07.1** | Are physical security perimeters implemented to safeguard personnel, data, and information systems? | Oracle Global Physical Security uses a risk-based approach to physical and environmental security. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html |
| | | Oracle Health Insurance Cloud Services relies on Oracle Global Physical Security to manage all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. |

| | | |
|---|---|---|
| **DCS-07.2** | Are physical security perimeters established between administrative and business areas, data storage, and processing facilities? | The goal is to balance prevention, detection, protection, and response, while maintaining a work environment that fosters collaboration among Oracle employees.<br><br>Oracle Health Insurance Cloud Services relies on Oracle Global Physical Security to manage all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. |
| **DCS-08.1** | Is equipment identification used as a method for connection authentication? | Equipment identification is used as a method for connection authentication. The VPN that Oracle staff use to connect to Oracle Health Insurance Cloud Services uses machine certificates and other identifiers to validate that the device is Oracle owned and provisioned before allowing access to resources. Oracle Health Insurance Cloud Services manages equipment identification in alignment with the ISO 27001 standard. |
| **DCS-09.1** | Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms? | Oracle has implemented the following protocols:<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><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><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><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><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 a high probability of environmental risk events? | Please see DCS-12.1 |

## Control Domain: Data Security & Privacy Lifecycle

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **DSP-01.1** | Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level? | Oracle's information-asset classification determines corporate data-security requirements for Oracle-managed systems. Oracle policies provide global guidance for appropriate controls designed to protect corporate, cloud and customer data in accordance with the data classification. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/ |
| | | Oracle Health Insurance Cloud Services follow Oracle's Information Protection Policy. The policy provides GIU guidance and determines appropriate controls to protect data in accordance with the Oracle data classification and handling of data throughout its lifecycle. Oracle Health Insurance Cloud Services follow Oracle's Information Asset Classification Policy according to all applicable laws and regulations. |
| **DSP-01.2** | Are data security and privacy policies and procedures reviewed and updated at least annually? | Oracle policies (including polices that address data security and privacy) are reviewed annually and updated as needed. |
| | | Oracle Health Insurance Cloud Services security and privacy procedures are reviewed annually and updated as needed in accordance with Oracle Corporate policy. |
| **DSP-02.1** | Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means? | Industry accepted methods are applied for secure data disposal from storage media. Oracle's Media Sanitation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data.<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/ |
| | | Oracle Health Insurance Cloud Services follows Oracle's Media Sanitization and Disposal Policy |
| **DSP-03.1** | Is a data inventory created and maintained for sensitive and personal information (at a minimum)? | Oracle Health Insurance Cloud Services document and maintain data inventories and data flows. |

| | | |
|---|---|---|
| **DSP-04.1** | Is data classified according to type and sensitivity levels? | Oracle categorizes information into four classes- Public, Internal, Restricted, and Highly Restricted-with each classification requiring corresponding levels of security controls, such as encryption requirements for non-Public data. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html |
| **DSP-05.1** | Is data flow documentation created to identify what data is processed and where it is stored and transmitted? | Data flow documentation is created and maintained by Oracle Health Insurance Cloud Services. This documentation is for internal use only. Oracle Health Insurance Cloud Services diagrams are available during a client audit. Customer audits may be performed annually per the Oracle Data Processing agreement, section 7. Please see: https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf |
| **DSP-05.2** | Is data flow documentation reviewed at defined intervals, at least annually, and after any change? | Data Flow documentation is reviewed at least annually and updated as needed. |
| **DSP-06.1** | Is the ownership and stewardship of all relevant personal and sensitive data documented? | Oracle's Information Systems Asset Inventory Policy requires that an accurate and current inventory (including data owners and data stewards) be maintained for all information systems holding critical and highly critical information assets in Oracle Corporate and cloud infrastructures.<br><br>Oracle Health Insurance Cloud Services follow Oracle's Information Systems Asset Inventory Policy that requires Ownership and stewardship of all relevant personal and sensitive data is documented. The customer is the controller of their data. |
| **DSP-06.2** | Is data ownership and stewardship documentation reviewed at least annually? | Oracle Health Insurance Cloud Services follow Oracle's Information Protection Policy that requires Ownership and stewardship of all relevant personal and sensitive data to be documented. The customer is the controller of their data. Oracle is not the controller of the data. Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html https://www.oracle.com/ie/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf |
| **DSP-07.1** | Are systems, products, and business practices based on security principles by design and per industry best practices? | Systems, products, and business practices are based on security principles by design and per international security standards and best practices. Oracle's security policies and practices cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27001:2022 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27002:2022 standards. Oracle Health Insurance Cloud Services are delivered in accordance with Oracle corporate policy. |
| **DSP-08.1** | Are systems, products, and business practices based on privacy principles by design and according to industry best practices? | Oracle Health Insurance Cloud Service systems,, products, and business practices are based on privacy principles by design and per industry best practices. Oracle's privacy policies and practices cover the management of privacy for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with ISO 27018 and SSAE18 SOC1 / SOC2. |

| | | |
|---|---|---|
| **DSP-08.2** | Are systems' privacy settings configured by default and according to all applicable laws and regulations? | Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html<br><br>Privacy settings for Oracle Health Insurance Cloud Services are controlled by the customer. |
| **DSP-09.1** | Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations, and industry best practices? | Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html<br><br>Oracle Health Insurance Cloud Services performs data protection impact assessments for all new products and feature enhancements being brought to market. |
| **DSP-10.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)? | Oracle Health Insurance Cloud Services has processes, procedures, and technical measures in place to help ensure transfer of sensitive data is protected from unauthorized access and is compliant with data transfer laws and regulations. See the following links for additional information: https://www.oracle.com/ie/corporate/contracts/cloud-services/contracts.html https://www.oracle.com/ie/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf |
| **DSP-11.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)? | Oracle Health Insurance Cloud Services has processes, procedures, and technical measures that are defined and implemented to enable Data Subject Rights Requests to access, modify, or delete personal data. Note: Oracle is not the controller of the data. If Oracle directly receives any requests or inquiries from Individuals, it will promptly pass on such requests to customers without responding to the Individual. Otherwise, Oracle will advise the Individual to identify and contact the relevant controller(s). Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html https://www.oracle.com/ie/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf |

| | | |
|---|---|---|
| **DSP-12.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)? | Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html<br><br>Where applicable, Oracle Health Insurance Cloud Services supports privacy regulations such as GDPR. For more detail, please refer to: https://www.oracle.com/security/gdpr/<br><br>Please also refer to SaaS Services delivery policy: https://www.oracle.com/legal/privacy/services-privacy-policy.html Also please see DSP-10.1. |
| **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/<br><br>Oracle Health Insurance Cloud Services have processes, procedures, and technical measures in place for the transfer and sub-processing of personal data within the service supply chain. Oracle and Oracle Affiliates employees, as well as any Third-Party sub-processors that process Personal Information, are subject to appropriate confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with Oracle policies concerning protection of confidential information. |
| **DSP-14.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation? | Health Insurance Cloud Services have processes, procedures, and technical measures defined and implemented to disclose details to data owners of any personal or sensitive data access by sub processors. To the extent Oracle engages Oracle affiliates and third-party sub processors to have access to Services Personal Information to assist in the provision of Services, such sub-processors shall be subject to the same level of data protection and security as Oracle under the terms of Your order for Services. Oracle is responsible for its sub-processors' compliance with the terms of Your order for Services. Oracle maintains lists of Oracle affiliates and sub processors that may process Services Personal Information. Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html |
| **DSP-15.1** | Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments? | Replicating or using production data in non-production environments is not performed for Oracle Health Insurance Cloud Services . Oracle will not use customer data in non-production environments or for testing purposes. Production and non-production environments are logically and physically segregated. Additionally, procedures are in place to ensure production data is not used in non-production environments. |

| | | |
|---|---|---|
| **DSP-16.1** | Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations? | Oracle Health Insurance Cloud Services data retention is 36 months unless otherwise determined by applicable law requirements. Note: Oracle is not the controller of the data. The customer remains solely responsible for data retention. |
| **DSP-17.1** | Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle? | Oracle Health Insurance Cloud Services have processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle. Note: Oracle is not the controller of the data. The customer remains solely responsible for their data. |
| **DSP-18.1** | Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations? | Oracle customers are responsible for the proper handling of any data they choose to collect, store, or process, and to ensure that handling complies with all applicable law and regulation. Oracle makes available Data privacy and Data processing agreements for CSC review; these can be found at https://www.oracle.com/contracts/cloud-services/. In the event Oracle does receive a disclosure request directly from a law enforcement or government authority, Oracle will process the request as described in the Oracle Data Processing Agreement (Section 11) and Oracle's BCR-p (Section 7.2). In addition to publicly available transparency reports (accessible at https://www.oracle.com/legal/law-enforcement-requests-report/), Oracle will also provide annual transparency reports to its data protection authority about the number and types of requests it has received.<br><br>Oracle Cloud Service Agreement - https://www.oracle.com/corporate/contracts/cloudservices/contracts.html#ct07tabcontent1<br><br>Data Processing Agreement - https://www.oracle.com/corporate/contracts/cloudservices/contracts.html#ct07tabcontent1<br><br>Oracle Services Privacy Policy: https://www.oracle.com/legal/privacy/services-privacy-policy/ |
| **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 will promptly inform You (Customer) of requests to provide access to Personal Information unless otherwise required by law. Please see: https://www.oracle.com/ie/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf |
| **DSP-19.1** | Are processes, procedures, and technical measures defined and | Oracle Health Insurance Cloud Services has processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locations where data is processed or backed up. |

| | | |
|---|---|---|
| | implemented to specify and document physical data locations, including locales where data is processed or backed up? | |

## Control Domain: Governance, Risk & Compliance

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **GRC-01.1** | Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained? | Global Information Security (GIS) defines policies for the Line of Business management of information security across Oracle. Additionally, GIS sets direction and provides advice to help protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners, and employees. GIS also coordinates the reporting of information security risk to senior leadership such as the Oracle Security Oversight Committee and Board of Directors. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html |
| | | Oracle Health Insurance Cloud Services have information governance program policies and procedures sponsored by Oracle Global Information Security (GIS) established, documented, approved, communicated, applied, evaluated, and maintained.<br><br>GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html |
| **GRC-01.2** | Are the policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including polices that address governance, risk, and compliance) are reviewed annually and updated as needed. |
| | | Oracle Health Insurance Cloud Services standards and procedures (including those that address governance, risk, and compliance) are reviewed annually and updated as needed. |
| **GRC-02.1** | Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, | 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. |

| | | |
|---|---|---|
| | treatment, and acceptance of cloud security and privacy risks? | 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.<br>Oracle Health Insurance Cloud Services standards and procedures (including those that address cloud security and privacy risks) are reviewed annually and updated as needed. |
| **GRC-04.1** | Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs? | Global Information Security (GIS) manages a security exception program which oversees LoB exception and exception management activity.<br>Oracle Health Insurance Cloud Services follows Oracle Corporate Policies including an approved exception process when deviations from policy occur. |
| **GRC-05.1** | Has an information security program (including programs of all relevant CCM domains) been developed and implemented? | Oracle's Information Security Program has been developed and implemented. Oracle's security policies cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, including employees and contractors. These policies are aligned with the ISO/IEC 27001:2013 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27002:2022 standards. Some Oracle products and services are certified per specific International, industry and government standards such as ISO/IEC 27001:2013 AICPA SSAE Number 18 (SOC), Payment Card Industry Data Security Standards (PCI DSS) and other standards. Oracle Health Insurance Cloud Services undergo IRAP, HIPAA and SOC 1 and SOC 2 audits. These are available for customer review upon request. |
| **GRC-06.1** | Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented? | See GRC-05.1 |
| **GRC-07.1** | Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your | Oracle Health Insurance Cloud Services must comply with relevant standards, regulations, legal/contractual, and statutory requirements applicable to Oracle as identified and documented by Oracle Legal and Corporate Security. Oracle's Business Assessment & Audit (BA&A) is an independent global audit organization which performs global processes and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards and select laws and regulations. See A&A-01.1. |

| | | |
|---|---|---|
| | organization identified and documented? | The customer remains solely responsible for its regulatory compliance in its use of any Oracle Cloud services. The customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing. |
| **GRC-08.1** | Is contact established and maintained with cloud-related special interest groups and other relevant entities? | Oracle Health Insurance Cloud Services maintains contact with cloud-related special interest groups and other relevant entities such as Oracle Autonomous Database and the Oracle Cloud Native Architect groups. |

## 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. |
| **HRS-01.2** | Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk? | In accordance with Oracle policy, background checks are required for individuals being considered for employment. For background check information organized by local law and regulation, see https://www.oracle.com/corporate/careers/background-check.html |

| | | |
|---|---|---|
| **HRS-01.3** | Are background verification policies and procedures reviewed and updated at least annually? | Oracle Human Resources policies (including polices that address candidate and employee background checks) are reviewed annually and updated as needed.<br><br>Oracle Health Insurance Cloud Services follows Oracle Recruiting Privacy and the privacy and security practices of Oracle, |
| **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 Health Insurance Cloud Services relies on Oracle Corporate Security, Legal and Corporate HR policies (including policies that address Acceptable Use). see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html |
| **HRS-02.2** | Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually? | Oracle Corporate Security policies (including the Acceptable Use Policy) are reviewed annually and updated as needed.<br><br>Oracle has formal "acceptable use of asset" policy requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, internet access, and other company resources available to Oracle employees, contractors and visitors.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html<br><br>Oracle Health Insurance Cloud Services team members follow the Oracle Corporate policy for organizationally owned and managed assets. |
| **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 | Oracle Health Insurance Cloud Services follows Oracle standard policies and procedures to conceal confidential data |

| | | |
|---|---|---|
| | data reviewed and updated at least annually? | |
| **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 Health Insurance Cloud Services rely on Oracle Global Physical Security for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. See https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html |
| **HRS-04.2** | Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually? | Oracle Corporate Security policies (including polices intended to protect information accessed, processed, or stored at remote sites and locations) are reviewed annually and updated as needed. |
| | | Oracle Health Insurance Cloud Services rely on Oracle Global Physical Security for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. |
| **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 Health Insurance Cloud Services regularly reviews network and operating system accounts regarding the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle Health Insurance Cloud Services takes appropriate actions to promptly terminate network, telephony, and physical access.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| **HRS-07.1** | Are employees required to sign an employment | Please see HRS-02.1 |

| | | |
|---|---|---|
| | agreement before gaining access to organizational information systems, resources, and assets? | |
| **HRS-08.1** | Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements? | Please see HRS-02.1 |
| **HRS-09.1** | Are employee roles and responsibilities relating to information assets and security documented and communicated? | Oracle's information asset classification determines corporate data-security requirements for Oracle managed systems. Oracle policies and standards provide global guidance for appropriate controls designed to protect the confidentiality, integrity, and availability of corporate data in accordance with the data classification. Required mechanisms are designed to be commensurate with the nature of the corporate data being protected. For example, security requirements are greater for data that is sensitive or valuable, such as cloud systems, source code and employment records.<br><br>Oracle's corporate security controls can be grouped into three categories: administrative, physical, and technical security controls.<br><br>• Administrative controls, including logical access control and human resource processes<br>• Physical controls designed to prevent unauthorized physical access to servers and data processing environments<br>• Technical controls, including secure configurations and encryption for data at rest and in transit<br><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<br><br>https://www.oracle.com/corporate/security-practices/corporate/data-protection/ |
| | | Customers are responsible for the management of identity and access to their data in their use of Oracle Health Insurance Cloud Services. Identity and Access Management processes, procedures, and technical measures are in place for the secure management of users and roles. These are documented here: https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| **HRS-10.1** | Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and | Please see HRS-02.1 |

| | | |
|---|---|---|
| | operational details identified, documented, and reviewed at planned intervals? | |
| **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, | See HRS-11.1 |

| | | |
|---|---|---|
| | statutory, or 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><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 |
| | | Access to OCI infrastructure follows the OCI Operator Access Standard while Oracle Health Insurance Cloud Services follow the Oracle Logical Access Control Policy for its identity and access procedures. |
| **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 Health Insurance Cloud Services follows the Oracle corporate standards for identity and access management policies applicable to identity and access management. |
| **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 Health Insurance Cloud Services follows Oracle Corporate password policies. |
| **IAM-02.2** | Are strong password policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including password complexity and protection requirements) are reviewed annually and updated as needed. |
| | | Customers are responsible for the management of identity and access to their data in their use of Oracle Health Insurance Cloud Services. |
| **IAM-03.1** | Is system identity information and levels of access managed, stored, and reviewed? | System identity information and levels of access is managed, stored, and reviewed. Logical access controls for applications and systems must provide identification, authentication, authorization, accountability, and auditing functionality. Oracle regularly reviews network and operating system accounts regarding the appropriate employee access levels. |

| | | |
|---|---|---|
| | | For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| | | Oracle Health Insurance Cloud Services follows Oracle Corporate access and password policies. |
| **IAM-04.1** | Is the separation of duties principle employed when implementing information system access? | Separation of duties principle is employed when implementing information system access. The Oracle Logical Access Controls Policy and standard describes logical access control requirements for Oracle systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined 'users' with access to Oracle systems, which are not Internet facing publicly accessible systems. Oracle SaaS security has developed its own standard that further extends/refines the one coming from Oracle corporate security, for the SaaS LoB.<br>All Oracle authorization decisions for granting, approval, and review of access are 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? |
| | | Customers are responsible for ensuring the least privilege in their use of Oracle cloud services. Oracle Health Insurance Cloud Services supports Role Based Access adhering to the principle of least privilege and segregation of duty with role management controlled and administered by the customer. |
| **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 |
| | | Customers are responsible for ensuring least privilege in their use of Oracle Health Insurance Cloud Services. Customers are responsible for user access provisioning and role assignment when connecting to Oracle Health Insurance Cloud Services. Oracle Health Insurance Cloud Services support Role Based Access in alignment to the principle of least privilege and segregation of duty within the integrated role management included with the product. |
| **IAM-06.1** | Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes? | A user access provisioning process is defined and implemented. Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. For more information, see<br>https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| | | Customers are responsible for the user access provisioning in their use of Oracle Health Insurance Cloud services. Oracle Health Insurance Cloud Services publishes user access and OIAM provisioning is documented, for more information see:<br>https://www.oracle.com/corporate/security-practices/corporate/access-control.html |

| | | |
|---|---|---|
| **IAM-07.1** | Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies? | Oracle Lines of Business are required to regularly review network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html<br><br>Customers are responsible for user access de-provisioning in their use of Oracle cloud services. |
| **IAM-08.1** | Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance? | Customers are responsible for review and revalidation of user access de-provisioning in their use of Oracle Health Insurance Cloud Services. Oracle reviews and revalidates Oracle administrative user access for least privilege and separation of duties on a quarterly cadence. Oracle Health Insurance Cloud Services service employee access management covers on-boarding, internal/external transitions, and terminations. All terminations are processed automatically through the Oracle Human Resources Management System (HRMS). After a termination is processed, automated notifications are issued for terminations (regardless of type) based on the effective date of the termination. |
| **IAM-09.1** | Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate? | Oracle Health Insurance Cloud Services follows the Oracle Network Security Policy that defines requirements and processes that include segregation of privileged access. |
| **IAM-10.1** | Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period? | Oracle Health Insurance Cloud Services access processes are defined and implemented. Privileged Access roles and rights have processes to ensure they are reviewed on a quarterly basis. Privileged Account passwords expire on a shortened cycle. For more information see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html. |
| **IAM-10.2** | Are procedures implemented to prevent the culmination of | The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. This policy does not apply to publicly accessible, internet-facing Oracle systems or end users. Oracle user access is provisioned through an account- |

| | | |
|---|---|---|
| | segregated privileged access? | provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. All network administration accounts, deployed in an Oracle managed network, must be provisioned, and managed by a corporate sanctioned access governance system. |
| **IAM-11.1** | Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented, and evaluated? | Customers are responsible for review and revalidation of user access de-provisioning in their use of Oracle Health Insurance Cloud Services. Oracle Health Insurance Cloud Services document their customer Identity and access for privileged administrative accounts. .For more information see:<br>https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| **IAM-12.1** | Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated? | Oracle Health Insurance Cloud Services have logging processes that are in place and are reviewed by external third-party auditors for our continued compliance with other Compliance frameworks (i.e., SOC1, SOC2, PCI-DSS and ISO27001.) Logs are immutable where technically possible otherwise compensating controls are in place to ensure a secure logging infrastructure. |
| **IAM-12.2** | Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures? | See IAM-12.1 |
| **IAM-13.1** | Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals | Customers are responsible for the management of identity and access to their data in their use of Oracle Health Insurance Cloud Services. For Oracle Health Insurance Cloud Services, the processes, procedures, and technical measures that ensure OHI users are identifiable through unique identification (or can associate individuals with user identification usage) are defined, implemented, and evaluated. Each OHI user is assigned a unique identifier/account through IAM. |

| | | |
|---|---|---|
| | with user identification usage) defined, implemented, and evaluated? | |
| **IAM-14.1** | Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated? | Customers are responsible for the management of identity and access to their data in their use of Oracle Health Insurance Cloud Services. Each user is assigned a unique identifier/account IAM. For Oracle Health Insurance Cloud Services, the processes, procedures, and technical measures that ensure users are identifiable through IAM unique identification (or can associate individuals with user identification usage) are defined, implemented, and evaluated. |
| **IAM-14.2** | Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted? | Oracle Health Insurance Cloud Services relies on Oracle Cloud Infrastructure Certificates which provides organizations with certificate issuance, storage, and management capabilities, including revocation and automatic renewal. If you have a third-party certificate authority (CA) that you already use, you can import certificates issued by that CA for use in an Oracle Cloud Infrastructure tenancy. Integration with Oracle Cloud Infrastructure Load Balancing lets you seamlessly associate a TLS certificate issued or managed by Certificates with resources that need certificates.<br><br>See https://docs.oracle.com/en-us/iaas/Content/certificates/overview.htm |
| **IAM-15.1** | Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated? | Customers are responsible for the management of identity and access to their data in their use of Oracle Health Insurance Cloud Services. IAM Processes, procedures, and technical measures are in place for the secure management of passwords. These are documented here: https://www.oracle.com/corporate/security-practices/corporate/access-control.html |
| **IAM-16.1** | Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated? | Customers are responsible for the management of identity and access to their data in their use of Oracle Health Insurance Cloud Services. IAM Processes, procedures, and technical measures are in place for the secure management of passwords. Oracle's Access Control security practices define these measures. For administration of network security and network-management devices, Oracle Health Insurance Cloud Services requires Oracle personnel to use secure protocols with authentication, authorization, and strong encryption and are approved via the Corporate Security Solution Assurance Process (CSSAP). See: https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html |

## Control Domain: Interoperability & Portability

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **IPY-01.1** | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)? | Oracle Health Insurance Cloud Services follows Oracle Securing Coding standards and have procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services. |
| **IPY-01.2** | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability? | Oracle Health Insurance Cloud Services have procedures in place for information processing interoperability. |
| **IPY-01.3** | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability? | Oracle Health Insurance Cloud Services are deployed only on Oracle Cloud Infrastructure. Oracle Health Insurance Cloud Service customers wishing to import/export data must follow the published Oracle Health Insurance Cloud Services specific documentation. For more information, see:<br>Oracle Health Insurance Data Privacy Enablement Release 4.24.1 |
| **IPY-01.4** | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, | Oracle Health Insurance Cloud Services follows the Data Processing Agreementand Oracle's Binding Corporate Rules<br>For more information, see: https://www.oracle.com/contracts/cloud-services/ |

| | | |
|---|---|---|
| | portability, integrity, and persistence? | |
| **IPY-01.5** | Are interoperability and portability policies and procedures reviewed and updated at least annually? | Oracle Health Insurance Cloud Services documentation (including interoperability and portability policies) is reviewed annually and updated as needed. |
| **IPY-02.1** | Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability? | Some Oracle Health Insurance Cloud Services support programmatic interfaces (APIs). |
| **IPY-03.1** | Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data? | External connections to Oracle Health Insurance Cloud Services including data import or export is encrypted in accordance with the section 1.5 of the Oracle Hosting and Delivery Polices: https://www.oracle.com/contracts/cloud-services/ |
| **IPY-04.1** | Do agreements include provisions specifying CSC data access upon contract termination, and have the following?<br>a. Data format<br>b. Duration data will be stored<br>c. Scope of the data retained and made available to the CSCs<br>d. Data deletion policy | Oracles Cloud Hosting and Delivery policies include provisions for CSC data access upon contract termination. For a period of 60 days upon termination of the Oracle Cloud Services, Oracle will make available, via secure protocols and in a structured, machine-readable format, Customer Content residing in the production Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by Customer. Any terms and conditions related to Oracle's performance of the applicable services shall be specified in the customer order for services documentation. Please refer to: https://www.oracle.com/contracts/cloud-services/ |

## Control Domain: Infrastructure & Virtualization Services

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|

| | | |
|---|---|---|
| **IVS-01.1** | Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained? | Oracle Health Insurance Cloud Services are deployed only on Oracle Cloud Infrastructure which follows the Oracle Corporate Security Policies. For more information on Oracle Cloud Infrastructure, see the OCI CAIQ at https://www.oracle.com/corporate/security-practices/cloud/ |
| **IVS-01.2** | Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually? | Oracle Health Insurance Cloud Services relies on Oracle Cloud Infrastructure (OCI infrastructure and virtualization. OCI security policies and procedures. |
| **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 Health Insurance Cloud Services are deployed with Oracle managed capacity management and monitoring to help ensure service availability uptime and performance. Oracle Health Insurance Cloud Applications collects and monitors capacity and utilization data. This data is used to plan for adequate capacity to meet current, projected, and anticipated needs and customer service level agreements. |
| **IVS-03.1** | Are communications between environments monitored? | Oracle Health Insurance Cloud Services communication between environments is monitored. Specifically, our intrusion-detection systems within the Oracle Cloud Infrastructure provides continuous surveillance for intercepting and responding to security events as they are identified. Oracle utilizes a network-based monitoring approach to detect attacks on open firewall ports within Oracle's Cloud Infrastructure. Events are analyzed using signature detection, which involves pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to security personnel for review and response to potential threats. For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html. |
| **IVS-03.2** | Are communications between environments encrypted? | Oracle has corporate policies and standards that define the approved cryptographic algorithms and protocols. For all Oracle Health Insurance Cloud Applications connections to the customer administration console, current APIs or host region must be made over an encrypted protocol using HTTPS and TLS 1.2 or above. Encryption is employed to protect data and virtual machine images during transport across public networks. |
| **IVS-03.3** | Are communications between environments restricted to only authenticated and authorized connections, | As defined in the Oracle Network Security Policy, Oracle Health Insurance Cloud Services restricts communication between environments to only authenticated and authorized connections. Please see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html |

| | | |
|---|---|---|
| | as justified by the business? | |
| **IVS-03.4** | Are network configurations reviewed at least annually? | Oracle Health Insurance Cloud Services' network configurations are reviewed 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 Health Insurance Cloud Services follows the defined process required by Corporate Security Solution Assurance Process (CSSAP). This process ensures justification and approval of the new configuration has occurred. For more information see: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html |
| **IVS-04.1** | Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline? | Oracle Health Insurance Cloud Services employs standardized system hardening practices across Oracle Health Insurance Cloud Services instances. This includes alignment monitoring with base images and/or baselines, restricting protocol access, removing, or disabling unnecessary software and services, removing unnecessary user accounts patch management and logging. |
| **IVS-05.1** | Are production and non-production environments separated? | Oracle Health Insurance Cloud Services production and non-production platforms are logically separated. |
| **IVS-06.1** | Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants? | Customers are responsible for the management of identity and access to their data in their use of Oracle Health Insurance Cloud Services. Oracle Health Insurance Cloud Services deployments are logically separated and secured so that tenants have a restricted view of their data only. |
| **IVS-07.1** | Are secure and encrypted communication channels including only up-to-date | Your access to Oracle Health Insurance Cloud Services is through a secure communication protocol provided by Oracle. Staging networks are segregated from production-level networks and utilized when migrating production data to virtual servers. Physical servers, applications, and virtual machines are not moved. New environments are provisioned using a hardened master image with customer data migrated once the provisioning process is complete. Communication |

| | | |
|---|---|---|
| | and approved protocols used when migrating servers, services, applications, or data to cloud environments? | 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 Cloud Infrastructure utilizes network architecture diagrams reflect network segments with additional compliance considerations, as appropriate. These Security Zones help protect resources in Oracle Cloud Infrastructure, including Compute, Networking, Object Storage, and Database resources, comply with Oracle security principles. For more information see: https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html |
| **IVS-09.1** | Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks? | Processes, procedures, and defense-in-depth techniques are defined and implemented. Oracle Health Insurance Cloud Application's defense-in-depth security framework helps detect and protect from network-based attacks. Specifically, OCI intrusion-detection systems within the Oracle Cloud Infrastructure provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle utilizes a network-based monitoring approach to detect attacks on open firewall ports within Oracle's Cloud Infrastructure. Events are analyzed using signature detection, which involves pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to Oracle's security personnel for review and response to potential threats. For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html. |

## Control Domain: Logging & Monitoring

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **LOG-01.1** | Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained? | Logging and monitoring policies are established, documented, approved, communicated, evaluated, and maintained by Oracle Corporate Security.<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 Health Insurance Cloud Services capture and store logs for certain security-related activities on operating systems, applications, databases, and network devices following Oracle Logging and Monitoring polices. For more information, see the 'Monitoring' section of the Oracle Cloud Hosting and Delivery Policies document: https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf |
| **LOG-01.2** | Are policies and procedures reviewed and | Oracle Corporate Security policies (including polices that address logging and monitoring) are reviewed annually and updated as needed. |

| | | |
|---|---|---|
| | updated at least annually? | Oracle Health Insurance Cloud Services has a defined GBU Security Logging Standard, and is reviewed annually. |
| **LOG-02.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention? | Oracle Health Insurance Cloud Services has a defined GBU Security Logging Standard. This standard supports the Oracle Logging and Log Analysis Policy. The following are defined in the standard:<br>• Information included in the log collection record<br>• Events to be logged<br>• Log Storage<br>• Retention period and classification<br>• Frequency of Analysis of Logs |
| **LOG-03.1** | Are security-related events identified and monitored within applications and the underlying infrastructure? | All security-related events (system events, firewall logs, network flows, etc.) from Oracle Health Insurance Cloud Services and its underlying OCI infrastructure are logged into a OCI managed Security Information and Event Management (SIEM) solution to correlate information and alert on any potential security event. Oracle security personnel monitor these events 24x7x365 and have defined processes to enable the incident response process. |
| **LOG-03.2** | Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics? | All Security-related events (system events, firewall logs, network flows, etc.) from Oracle Health Insurance Cloud Services and its underlying OCI infrastructure are logged into a OCI managed Security Information and Event Management. The OCI managed (SIEM) solution to correlate information and alert on any potential security event. A system is defined and implemented to generate alerts and notify responsible stakeholders. |
| **LOG-04.1** | Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability? | The GIU Logging and Log Analysis Standard defines security and parameters (including retention) for Oracle Health Insurance Cloud Application logs. These logs are restricted and provided on a need-to-know basis. Record of audit log access are maintained to provide unique access accountability. |
| **LOG-05.1** | Are security audit logs monitored to detect activity outside of typical or expected patterns? | Oracle Health Insurance Cloud application logs are sent to the OCI managed SIEM along with infrastructure logs from OCI. The Security Operations Center monitors these logs via dedicated detection and response teams that focus on designing and implementing solutions to help identify Tactics, Techniques, and Procedures (TTPs) of threat actors. |
| **LOG-05.2** | Is a process established and followed to review and take appropriate and timely actions on detected anomalies? | Oracle Health Insurance Cloud Services has defined procedures and processes to ensure appropriate and timely actions are taken on detected anomalies. |

| | | |
|---|---|---|
| **LOG-06.1** | Is a reliable time source being used across all relevant information processing systems? | Oracle Health Insurance Cloud Services utilizes Network Time Protocol (NTP) to synchronize systems for a common time reference across the environment. |
| **LOG-07.1** | Are logging requirements for information meta/data system events established, documented, and implemented? | Oracle Health Insurance Cloud Services follows the Oracle Cloud Services Logging and Log Analysis Standard which defines the standards for log generation, storage, retention, analysis, and log archived retention periods. |
| **LOG-07.2** | Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment? | Oracle Health Insurance Cloud Applications logging requirements and the threat landscape are continually reviewed. Logging requirement updates are made as necessary to include changing threats. The scope is reviewed annually and updated as needed. If necessary, the scope may be reviewed more frequently. |
| **LOG-08.1** | Are audit records generated, and do they contain relevant security information? | Oracle Health Insurance Cloud Services logs contain information on security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. |
| **LOG-09.1** | Does the information system protect audit records from unauthorized access, modification, and deletion? | Where possible, Oracle Health Insurance Cloud Services log files are protected by strong cryptography. . Access to these logs granted using role-based access controls and is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible. |
| **LOG-10.1** | Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls? | Oracle Health Insurance Cloud Applications monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. There are logs generated and mechanisms in place to review/respond to activity. |
| **LOG-11.1** | Are key lifecycle management events logged and monitored to | Oracle Health Insurance Cloud Applications monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. Logs are generated and mechanisms have been put in place to review activity. |

| | | |
|---|---|---|
| | enable auditing and reporting on cryptographic keys' usage? | |
| **LOG-12.1** | Is physical access logged and monitored using an auditable access control system? | For Oracle and third-party datacenters used by OCI, physical access is monitored and logged. https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html |
| **LOG-13.1** | Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated? | Oracle Health Insurance Cloud Services uses a variety of software tools to monitor the availability and performance of the Oracle Cloud Services and the operation of infrastructure and network components. Processes and measures for reporting and monitoring system anomalies and failures are in place. |
| **LOG-13.2** | Are accountable parties immediately notified about anomalies and failures? | Accountable parties are immediately notified about anomalies and failures. Oracle Health Insurance Cloud Services leverages a Security Information and Event Management (SIEM) solution to correlate information such as system events, firewall logs, WAF logs, network flows from the environment and to alert on any potential security event. Oracle Cloud Infrastructure 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. |

| | | |
|---|---|---|
| | | Upon discovery of an incident, Oracle defines an incident response plan for rapid and effective incident investigation, response, and recovery. Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |
| | | All Security related events (system events, firewall logs, network flows, etc.) from Oracle Health Insurance Cloud Services and its underlying infrastructure are logged into a Security Information and Event Management (SIEM) solution to correlate information and alert on any potential security event. A system is defined and implemented to generate alerts and notify responsible stakeholders. |
| **SEF-01.2** | Are policies and procedures reviewed 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. |
| | | Oracle Health Insurance Cloud Services security procedures follows the Oracle Corporate Security policies that address timely management of security events and are reviewed annually and updated as needed. |
| **SEF-02.1** | Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained? | Please see SEF-01.1 |
| **SEF-02.2** | Are policies and procedures for timely management of security incidents reviewed and updated at least annually? | Oracle Corporate Security policies and procedures that address timely management of security incidents are reviewed annually and updated as needed. |
| | | Oracle Health Insurance Cloud Services security procedures follows the Oracle Corporate Security policies that address timely management of security events and are reviewed annually and updated as needed. |
| **SEF-03.1** | Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, | 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 |

| | | |
|---|---|---|
| | communicated, applied, evaluated, and maintained? | • 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? | Oracle Health Insurance Cloud Services security incident response plans are tested and updated as needed. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |
| **SEF-05.1** | Are information security incident 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? | See SEF-01.1 |
| **SEF-07.1** | Are processes, procedures, and technical measures for security breach notifications defined and implemented? | In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents and incident history are not shared externally. |
| **SEF-07.2** | Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) | Please see SEF-01.1<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html |

| | | |
|---|---|---|
| | as per applicable SLAs, laws, and regulations? | |
| **SEF-08.1** | Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities? | Oracle maintains points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. |

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

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **STA-01.1** | Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained? | Managing security and privacy in the cloud is a shared responsibility between the customer and the service provider. The distribution of responsibilities varies based on the nature of the cloud service (IaaS, PaaS, SaaS). Oracle strongly recommends that customers determine the suitability of using cloud services considering their own legal and regulatory compliance obligations. Making this determination is solely the customer's responsibility. For information, see https://www.oracle.com/cloud/compliance/<br><br>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. |
| | | As part of the GIU Supplier Management program, a central repository of GIU suppliers is maintained. The suppliers are assigned a Risk Category which is used to schedule security assessments. The suppliers are assessed regularly to help ensure GIU suppliers are following corporate policy and standards, but understand their obligations to protect Oracle information assets, including customer data and intellectual property. |

| | | |
|---|---|---|
| **STA-01.2** | Are the policies and procedures that apply the SSRM reviewed and updated annually? | The GIU Supplier Management program procedures are updated and reviewed annually.<br><br>See STA-01.1 |
| **STA-02.1** | Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering? | The Security Shared Responsibility Model (SSRM) is applied, documented, implemented, and managed throughout the supply chain for the Oracle Health Insurance Cloud Services. For more information see: https://www.oracle.com/corporate/suppliers.html |
| **STA-03.1** | Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain? | Oracle's Supply Chain Risk Management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services. Quality and reliability for Oracle Health Insurance Cloud Services' Applications' hardware systems are addressed through a variety of practices, including design, development, manufacturing, and materials management processes. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ |
| **STA-04.1** | Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering? | The Oracle Cloud Hosting and Delivery Policies describe customer (tenant) security obligations. Also, the Oracle Data Processing Agreement includes the responsibilities of the data controller (tenant/customer) versus data processor (Oracle). Please see the Oracle Hosting and Delivery Policies located at https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html and the Oracle Data Processing Agreement at https://www.oracle.com/contracts/cloud-services/ |
| **STA-05.1** | Is SSRM documentation for all cloud services the organization uses reviewed and validated? | Oracle Health Insurance Cloud Services reviews and validates SSRM Documentation annually. |
| **STA-06.1** | Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed? | All portions of the SSRM Oracle Health Insurance Cloud Services is responsible for is implemented, operated, audited, and assessed. |
| **STA-07.1** | Is an inventory of all supply chain relationships developed and maintained? | For Oracle Health Insurance Cloud Services, an inventory of all supply chain relationships is developed and maintained. These agreements define agreed upon security, privacy, and compliance controls prior to the onset of services. Oracle Cloud Infrastructure (OCI) currently maintains contracts with third-party vendors for co-location facilities (for certain services), transportation and storage of encrypted customer backup tapes to off-site storage facilities (for certain services) and various data center functions such as physical security guards, systems maintenance and facility building operations/ maintenance. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ |

| | | |
|---|---|---|
| **STA-08.1** | Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs? | Oracle's Supply Chain Risk Management focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services. Supply availability, continuity and resiliency in Oracle's hardware supply chain are addressed through a variety of practices, including:<br>• Multi-supplier and/or multi-location sourcing strategies where possible and reasonable.<br>• Review of supplier financial and business conditions.<br>• Requiring suppliers to meet minimum purchase periods and provide end-of-life (EOL)/end-of-support-life (EOSL) notice.<br>• Requesting advance notification of product changes from suppliers so that Oracle can assess and address any potential impact.<br>• Managing inventory availability due to changes in market conditions and due to natural disasters.<br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/<br>Additionally, Oracle Health Insurance Cloud Services follows guidelines to review any third-party tools and libraries to help ensure they are updated with every major release. Oracle Hospitality OPERA Cloud follows OSSA guidelines to build all third-party libraries from source to reduce the possibility of supply chain attacks. |
| **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 | Service agreements between CSPs and CSCs incorporate these provisions and/or terms, see the following Oracle documents: Hosting and Delivery Policy, Services Pillar Document, Data Processing Agreement https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.htmlhttps://www.oracle.com/be/corporate/contracts/cloud-services/contracts.htmlhttps://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf |

| | | |
|---|---|---|
| | portability requirements<br>• Data privacy | |
| **STA-10.1** | Are supply chain agreements between CSPs and CSCs reviewed at least annually? | Oracle Health Insurance Cloud Services does not have any direct third-party agreements. Datacenter agreements are managed and reviewed by OCI. |
| **STA-11.1** | Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities? | Oracle Health Insurance Cloud Services have processes for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities. |
| **STA-12.1** | Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented? | Oracle Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when accessing Oracle or Oracle customer facilities, networks and/or information systems, handling Oracle confidential information, or controlling custody of Oracle hardware assets. Suppliers are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/suppliers.html |
| **STA-13.1** | Are supply chain partner IT governance policies and procedures reviewed periodically? | Oracle's Supplier Security Management Policy requires all lines of business to maintain a program which manages risk for their suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual supplier review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each supplier's goods or services are leveraged. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ |
| | | Oracle Health Insurance Cloud Services Security are reviewed and updated as needed. see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ |
| **STA-14.1** | Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented? | See STA-13.1 |

## Control Domain: Threat & Vulnerability Management

| Question ID | Consensus Assessment Question | Oracle Response |
|---|---|---|
| **TVM-01.1** | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation? | Oracle has formal practices designed to identify, analyze, and remediate technical security vulnerabilities that may affect our enterprise systems and Oracle Cloud environments.<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.<br><br>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/ |
| | | The Oracle Cloud operations and security teams regularly evaluate Oracle's Critical Patch Updates and Security Alerts as well as relevant third-party security updates as they become available and apply the relevant patches in accordance with applicable change management processes. |
| | | |
| **TVM-01.2** | Are threat and vulnerability management policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including polices that address threat and vulnerability management) are reviewed annually and updated as needed. |
| | | Oracle Health Insurance Cloud Services procedures (including policies and procedures related to vulnerability management) are reviewed annually and updated as needed. |

| | | |
|---|---|---|
| **TVM-02.1** | Are policies and procedures to protect against malware on managed assets established, documented, approved, 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.<br><br>For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html |
| | | Oracle Health Insurance Cloud Services Security Standards includes procedures that address asset management and malware protection. |
| **TVM-02.2** | Are asset management and malware protection policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including polices that address asset management and malware protection) are reviewed annually and updated as needed. |
| | | Oracle Health Insurance Cloud Services Security Standards (including standards that address asset management and malware protection) are reviewed annually and updated as needed. |
| **TVM-03.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)? | Oracle Health Insurance Cloud Services processes, procedures, and technical measures are defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk.)<br><br>Oracle Health Insurance Cloud Services act on the detection or notification of a threat or risk once it has been confirmed that, both, a valid risk exists and that the recommended changes are applicable to Services environments. The severity of vulnerabilities is determined using a Common Vulnerability Scoring System (CVSS) Base Score, and remediation timelines are based upon the assigned severity and possible business impact.<br><br>Please see: https://www.oracle.com/security-alerts/<br><br>Also, see section: Order of Fixing Security Vulnerabilities https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html |
| **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? | Please see TVM-01.1<br><br>Oracle Health Insurance Cloud Services 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. 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 Health Insurance Cloud Services follow processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries following the Oracle Software Security Assurance standards. |
| **TVM-06.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing? | Oracle Health Insurance Cloud Services have processes, procedures, and technical measures are in place for independent third-party penetration testing. |
| **TVM-07.1** | Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly? | Oracle Health Insurance Cloud Services relies on OCI for continuous vulnerability detection on managed assets. |
| **TVM-08.1** | Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework? | Oracle uses the Common Vulnerability Scoring System (CVSS) to report the relative severity of security vulnerabilities when it discloses them. CVSS Base Score information is provided in the risk matrices published in Critical Patch Update and Security Alert Advisories. Oracle uses Common Vulnerabilities and Exposures (CVE) numbers to identify the vulnerabilities listed in the risk matrices in Critical Patch Update and Security Alert advisories. For more information, see https://www.oracle.com/corporate/security-practices/assurance/vulnerability/ |
| | | Oracle Health Insurance Cloud Services vulnerability remediation is prioritized using a risk-based model from an industry recognized framework. The remediation process ensures all testing or reported vulnerabilities are evaluated and patches are deployed across all Oracle Health Insurance Cloud Services products based on criticality. The severity of vulnerabilities is determined using the Common Vulnerability Scoring System (CVSS) Base Score. |
| **TVM-09.1** | Is a process defined and implemented to track and report vulnerability identification and | See TVM-01.1.<br>Oracle Health Insurance Cloud Services have a defined process for tracking and reporting vulnerabilities and remediation activities. This process includes the identification of vulnerabilities, assessment of their impact, and the implementation of remediation measures. Oracle Health Insurance Cloud Services participates in Oracle's system for |

| | | |
|---|---|---|
| | remediation activities that include stakeholder notification? | notifications to the responsible stakeholders about the discovered vulnerabilities, their impact, and the remediation plan. |
| **TVM-10.1** | Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals? | See TVM-01.1<br><br>Oracle Health Insurance Cloud Services have a defined process for tracking and reporting vulnerabilities and remediation activities. This process includes the identification of vulnerabilities, assessment of their impact, and the implementation of remediation measures. Oracle Health Insurance Cloud Services participates in Oracle's system for notifications to the responsible stakeholders about the discovered vulnerabilities, their impact, and the remediation plan. |

## 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 Health Insurance Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Health Insurance Cloud Services endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP)..For more information about CSSAP, see Corporate Security Solution Assurance Process: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html |
| **UEM-01.2** | Are universal endpoint management policies and procedures reviewed and updated at least annually? | Oracle Corporate Security policies (including polices that address universal endpoint management) are reviewed annually and updated as needed. |
| | | Oracle Health Insurance Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. |
| **UEM-02.1** | Is there a defined, documented, applicable | Please see UEM-01.1. This list is approved by Oracle Corporate Architecture and maintained by Oracle Information Technology. |

| | | |
|---|---|---|
| | 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? | Oracle Health Insurance Cloud Service relies on the Oracle Acceptable Use Policy for Systems and Resources is designed to help Oracle protect the security and integrity of information and Oracle systems and resources and provides guidance to employees, suppliers, contractors, and partners on how they may, and may not, use systems and resources while performing their job.<br><br>Oracle maintains a repository of approved software for all Oracle managed endpoint devices. |
| **UEM-03.1** | Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications? | Please see UEM-01.1. Endpoint validation is performed by automation approved by Oracle Corporate Architecture and maintained by Oracle Information Technology. |
| | | Oracle Health Insurance Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Health Insurance Cloud Services endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP). |
| **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 were 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 Health Insurance Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Health Insurance Cloud Services endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP)..For more information about CSSAP, see Corporate Security Solution Assurance Process: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html |
| **UEM-06.1** | Are all relevant interactive-use endpoints configured to require an automatic lock screen? | Interactive-used endpoints are configured to require an automatic lock screen. Oracle computers have secure desktop management software installed that lock screens automatically after a defined period of inactivity. This includes computers used to manage Oracle Health Insurance Cloud Services. Oracle Health Insurance Cloud Services enforces an automatic lock screen as a default setting that cannot be changed. |

| | | |
|---|---|---|
| **UEM-07.1** | Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process? | The Oracle Information Technology keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. OIT is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. OIT provides automation to verify antivirus configuration.<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 Health Insurance Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for endpoints. |
| **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 Health Insurance Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Corporate Security policy requires the use of antivirus, intrusion protection and firewall software on laptops and mobile devices. see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html |
| **UEM-11.1** | Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment? | Dynamic access policies are configured to validate the following items on endpoints before granting access to the Oracle Cloud Infrastructure hosting Oracle Health Insurance Cloud Services:<br>• Devices are running up-to-date software including anti-malware software and compliance monitoring tools that validate endpoint encryption.<br>• A local firewall is installed.<br>• The Oracle Cloud Network Access (OCNA) VPN is configured to time out after 24 hours of connectivity.<br>• Devices that support Windows and Mac operating systems are configured to lock automatically after 15 minutes of inactivity. |

| | | |
|---|---|---|
| | | • Oracle managed endpoints are tracked centrally in inventory systems. Business-critical software installed on the endpoints is checked regularly, and software update alerts are issued to users to meet compliance requirements according to Oracle policies and standards.<br>• When an endpoint is out of compliance, an email notification is sent to the user and management to make the necessary updates.<br>• The Security Information and Event Monitoring (SIEM) tool is configured to review the telemetry against predefined rules including detections related to data loss prevention.<br>• Security events detected generate an automated ticket with a severity rating and are tracked to resolution by the OCI Detection and Response Team (DART). |
| **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 Health Insurance Cloud Services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints Processes, procedures, and technical measures are defined and implemented to enable remote company data deletion on managed endpoint devices. Endpoint devices used by Oracle Health Insurance Cloud Services are subject to Oracle's secure desktop, and mobile device management software have remote wipe capabilities. |
| **UEM-14.1** | Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets? | Oracle has formal requirements for its suppliers to confirm they protect Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when:<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 follow the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ |
| | | Third party endpoints are not allowed in Oracle Health Insurance Cloud Services environments. |

## CONNECT WITH US

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

| | | |
|---|---|---|
| blogs.oracle.com | facebook.com/oracle | twitter.com/oracle |



CAIQ for <Product ZZZZ>