ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) v4.0 for Oracle Hospitality OPERA Cloud

April 2025 | Version 1.0

PURPOSE STATEMENT

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

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

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

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

DISCLAIMER

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

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

ORACLE CLOUD SERVICES IN SCOPE

Oracle Hospitality OPERA Cloud
Oracle Hospitality Integration Platform
Oracle Hospitality Reporting & Analytics Cloud Service
Oracle Hospitality Distribution Cloud Service
Oracle Hospitality Identity & Access Management
Oracle Hospitality OPERA Payment Interface Cloud Service
Oracle Hospitality Nor1 Cloud Service
Oracle Hospitality Token Proxy Service

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. The audit rights of customers for whom Oracle processes data are described in your agreement. For more information, see https://www.oracle.com/contracts/cloud-services/. The audit rights of customers of Oracle services are described in the Oracle Services Privacy Policy. For more information, see https://www.oracle.com/legal/privacy/services-privacy-policy.html
		Oracle Hospitality OPERA Cloud line of business follows Oracle policies, OCI standards, and Global Industry Unit (GIU) Security standards with regards to audit and assurance.
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Oracle Hospitality OPERA Cloud follows Global Industry Unit (GIU) Security standards.
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 Hospitality OPERA Cloud are conducted on an annual basis. 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 assessments performed according to risk-based plans and policies?	See A&A-01.1. Oracle's Business Assessment & Audit (BA&A) is independent. Its operational activities and procedures are conducted in alignment with Institute of Internal Auditors (IIA).
		Independent external audits and assessments of Oracle Hospitality OPERA Cloud are approved based on risk plans. 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 Hospitality OPERA Cloud engages with external assessment entities and independent auditors to verify that Oracle Hospitality OPERA Cloud have a control environment that includes policies, processes and security controls for the delivery of application services. These efforts align with ISO/IEC 27001 standards. 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 Hospitality OPERA Cloud and also checked by independent assessors during annual PCI DSS and SOC audits.
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 Hospitality OPERA Cloud follow a defined process for remediation following a risk-based approach.
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 Hospitality OPERA Cloud'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. Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at: **Reducing the incidence of security weaknesses in all Oracle products.**

		Oracle Software Security Assurance key programs include Oracle's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups, and the use of automated analysis and testing tools. **Reducing the impact of security weaknesses in Oracle products and services** Oracle has mature security vulnerability disclosure and remediation practices. The company is committed to treating all customers equally and delivering the best possible security maintenance experience through the Critical Patch Update and Security Alert programs. **Fostering security innovations.** Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help enable organizations to implement and manage consistent security policies across the hybrid cloud data center: database security and identity management, and security monitoring and analytics. For more information, see https://www.oracle.com/corporate/security-practices/assurance/
		Oracle Hospitality OPERA Cloud is audited for PCI DSS and therefore has additional SLDC requirements that govern it including annual secure code training for all development staff.
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Oracle Hospitality OPERA Cloud security 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 Hospitality OPERA Cloud undertakes baseline security requirements which are documented in accordance with the published Payment Card Industry-Data System Security (PCI-DSS) and are audited against those standards. Secure cloud configurations begin with the software design phase and continue through to pre-deployment testing in environments that are identical to our production environments.
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Oracle Hospitality OPERA Cloud teams maintain a set of defined technical and operational metrics to monitor adherence to business objectives, security requirements and compliance obligations.
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and	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

	operation per organizationally designed security requirements?	best practices as well as lessons learned from ongoing vulnerability testing by Oracle's internal product assessment teams. The Secure Coding Standards are a key component of Oracle Software Security Assurance and adherence to the Standards is assessed throughout the supported life of all Oracle products.
		Oracle Hospitality OPERA Cloud follows the OSSA Standards as well as the PCI-DSS.
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Security assurance analysis and testing assess security qualities of Oracle products against various types of attacks. There are two broad categories of tests: static and dynamic analysis. **Static security analysis** of source code is the initial line of defense used during the product development cycle. Oracle uses a commercial static code analyzer as well as a variety of internally developed tools, to catch problems while code is being written. Typically, analysis of these scan reports involves senior engineers from the product teams who are well-familiar with the product code sorting out false positives from real issues and reducing the number of false positives. **Dynamic analysis** activity takes place during latter phases of product development because it requires that the product or component be able to run. Dynamic analysis is aimed at externally visible product interfaces and APIs, and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing within Oracle. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
		Oracle Hospitality OPERA Cloud has defined testing strategies as part of our Development Security Operations principles. We validate application upgrades through a defined vulnerability testing process. Oracle regularly performs authenticated penetration and vulnerability testing and security assessments against the Oracle Hospitality OPERA Cloud application and underlying platform and infrastructure. These tests are intended to validate and improve the overall security posture of Oracle Hospitality OPERA Cloud.
AIS-05.2	Is testing automated when applicable and possible?	Oracle Hospitality OPERA Cloud application deployment follows an automated pipeline process which includes application regression testing. OPERA Cloud is deployed as a Cloud Native application on Oracle Cloud Infrastructure using the concepts of Continuous Integration & Continuous Deployment (CI/CD).
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Cloud services are deployed in a specific configuration, or a small number of configurations. Testing must be performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment. Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/configuration.html

		Oracle Hospitality OPERA Cloud Code 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?	Oracle Hospitality OPERA Cloud is deployed using an automated, provisioning pipeline.

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

		Oracle Hospitality OPERA Cloud follows a clearly defined process for regularly testing, assessing, evaluating, and maintaining the effectiveness of the technical and organizational security measures. Regular scans are conducted, Oracle Hospitality OPERA Cloud developers use static and dynamic analysis tools to detect security defects in Oracle Hospitality OPERA Cloud code prior to deploying to production. Identified issues are evaluated and addressed in order of priority and severity. Oracle Hospitality OPERA Cloud 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 Hospitality OPERA cloud security vulnerabilities are detected through the build and release pipeline remediation of vulnerabilities are automated where applicable.

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,	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/

	communicated, applied, evaluated, and maintained?	The RMRP is comprised of several sub-programs: emergency response to unplanned and emergent events, crisis management of serious incidents, technology disaster recovery and business continuity management. The program goal is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored. The RMRP is implemented and managed locally, regionally, and globally. The RMRP program management office provides executive scorecard reporting on program activities, planning and plan testing status within the LOBs.
		Oracle Hospitality OPERA Cloud has a Business Continuity / Disaster Recovery (BCDR) Program which is designed to meet the published Application SLA (https://www.oracle.com/contracts/cloud-services/). The details of the program is covered under the Risk Management resiliency Program (RMRP). 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 in accordance with Oracle policy. For additional information, see: https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	The RMRP policy mandates an annual operational cycle for (LoB) planning, evaluation, training, validation, and executive approvals for critical business operations. Oracle's Risk Management Resiliency Program defines requirements and standards for all Oracle LOBs regarding plans for and response to potential business disruption events. It also specifies the functional LOB roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across geographies. A centralized RMRP Program Management Office (PMO) has oversight responsibilities for the LoB compliance to the program. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
		Oracle Hospitality OPERA Cloud's Risk Assessment is aligned with Oracle Risk Management Resiliency Policy and Business Impact Analysis and Business Continuity Plans are reviewed annually and updated as needed
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	The RMRP Program is generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance. For more information about the program and requirements for Oracle Lines of Business, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
		Criteria used for Oracle Hospitality OPERA Cloud business continuity and operational resilience is aligned with the Oracle RMRP program. . For additional information, see: https://www.oracle.com/corporate/contracts/cloud-services/service-descriptions.html

BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	The RMRP PMO develops guidance as aids to LoB Risk Managers in managing their LoB's business continuity plans, testing and training procedures. The RMRP program requires all LoBs to: • Identify relevant business interruption scenarios, including essential people, resources, facilities and technology • Define business continuity plans and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Obtain approval of the plans from the LoB's executive For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	See BCR-03.1
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and 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: • Conduct a Business Impact Analysis that specifies a Recovery Time Objective and Recovery Point Objective (if appropriate to the function) and identifies the organization's business continuity contingencies strategy • Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Revise business continuity plans based on changes to operations, business requirements, and risks For more information, see: https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
		Oracle Hospitality OPERA Cloud 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 made available to authorized stakeholders, for example, auditors as part of SOC and PCI-DSS audits.

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 Hospitality OPERA Cloud reviews its business continuity documentation at least Annually in accordance with Oracle Corporate policy and updates 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 Hospitality OPERA Cloud) 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 Hospitality OPERA 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 Hospitality OPERA Cloud have a detailed SaaS Business Continuity / Disaster Recovery (BCDR) Program. The details of the SaaS Cloud Services BCDR program is covered under the Risk Management resiliency Program (RMRP). The procedures establish a communication plan for stakeholders and participants. See: https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
BCR-08.1	Is cloud data periodically backed up?	Oracle Hospitality OPERA Cloud 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 Hospitality OPERA Cloud undertakes backups in accordance with PCI DSS Requirement 3 and as published in the "Oracle Hosting and Delivery Policy": https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
BCR-08.3	Can backups be restored appropriately for resiliency?	Oracle Hospitality OPERA Cloud does not undertake restoration of data on behalf of customers. Customer data should be exported directly via the Oracle Hospitality OPERA Cloud SaaS application.
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Oracle's corporate Disaster Recovery (DR) plan focuses on the resiliency of computing infrastructure supporting Oracle's internal operations and cloud services. Oracle's production data centers are geographically separated and have component and power redundancy, with backup generators in place for availability of data center resources in case of a disaster, whether natural or man-made. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/disaster-recovery.html.
		Oracle Hospitality OPERA Cloud 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 Hospitality OPERA Cloud 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 Hospitality OPERA Cloud 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 Hospitality OPERA Cloud is deployed in Oracle Cloud Infrastructure which is designed to maintain service availability and continuity in the case of an incident affecting the services. Oracle Hospitality OPERA Cloud is deployed in geographically redundant Oracle Cloud datacenters in accordance with applicable industry standards. 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 Hospitality OPERA Cloud 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 Hospitality OPERA Cloud procedures are reviewed annually

CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Oracle Hospitality OPERA Cloud are deployed using a strict baseline deployment which helps implement consistent deployment standards against each version release.
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Oracle Corporate Security Solution Assurance Process (CSSAP) is a security review process developed by Corporate Security Architecture, Global Information Security, Global Product Security, Oracle Global IT, and Oracle's IT organizations to provide comprehensive information-security management review whether asset management occurs internally or externally. CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle: • Pre-review: the risk management teams in each line of business must perform a pre-assessment of each project using the approved template • CSSAP review: the security architecture team reviews the submitted plans and performs a technical security design review • Security assessment review: based on risk level, systems and applications undergo security verification testing before production use Reviews ensure that projects are aligned with: • Oracle Corporate Security Architecture strategy and direction • Oracle Corporate security, privacy and legal policies, procedures and standards For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
		All Oracle Hospitality OPERA Cloud are required to meet OSSA and be reviewed and approved by the Oracle Corporate Security Solution Assurance Process (CSSAP).
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted	Oracle's Network Security Policy establishes requirements for network management, network access and network device management, including authentication and authorization requirements for both physical devices and software-based systems. For more information, https://www.oracle.com/corporate/security-practices/corporate/access-control.html Oracle's Information Systems Asset Inventory Policy requires that an accurate and current inventory be maintained for all information systems holding critical and highly critical information assets in Oracle Corporate and cloud infrastructures, including the physical location. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html

		Oracle Hospitality OPERA Cloud follow the Oracle Corporate policies and standards that are in place outlining restrictions for adding, removing, and updating Oracle assets. Additionally, technical restrictions are in place where possible. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	Oracle Cloud Hosting and Delivery Policies does include provision within the SLA for changes which may impact Oracle Hospitality OPERA Cloud application availability, end user authorization for such change is part of the approval chain prior to the change process implementation. For more information, see: Oracle Cloud Hosting and Delivery Policies. https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf
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 Hospitality OPERA Cloud assets.
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Detection measures are implemented with proactive notification for changes that deviate from established baseline configurations. Oracle Hospitality OPERA Cloud use a centralized system for managing the access and integrity of device configurations. Change controls are in place to ensure only approved changes are applied. These systems are actively monitored to verify compliance with security and operational procedures. Also, internal weekly scans are performed on OCI.
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Oracle Hospitality OPERA Cloud 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 Hospitality OPERA Cloud 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 Hospitality OPERA Cloud 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, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/
		Oracle Hospitality OPERA Cloud follows documented standards supporting Oracle corporate encryption and key management policies.
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address cryptography, encryption, and key management) are reviewed annually and updated as needed.
		Oracle Hospitality OPERA Cloud reviews encryption and key management procedures at least annually and updates these as needed.
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services. The group is primarily responsible for making technical decisions and authoring internal standards to address government and industry requirements. Representatives from Corporate Security and development organizations define best practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence, and including roles and responsibilities. CRB's responsibilities include: • Creating and maintaining standards for cryptography algorithms, protocols, and their parameters • Providing approved standards in multiple formats, for readability and automation • Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle • Providing practical guidance on using cryptography • Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography
		Oracle Hospitality OPERA Cloud services review cryptography roles and responsibilities For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Solutions for managing encryption keys and cryptographic libraries at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). Oracle Global IT defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include:

		• Locations and technologies for storing encryption keys • Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures • Changing default encryption keys • Replacement schedule for various types of encryption keys For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
		Oracle Hospitality OPERA Cloud encrypts data at-rest and in following Oracle corporate policy and PCI DSS requirements.
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to only use up-to-date versions of approved security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
		Appropriate data protection encryption algorithms are used based on data classification, associated risks, and encryption technology usability for Oracle Hospitality OPERA Cloud. All Customer data is classified as "Confidential – Internal Only" or higher. Oracle Hospitality OPERA Cloud encrypts all data at rest using full schema level encryption (Oracle Transparent Data Encryption). For more information, see: https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
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: • Locations and technologies for storing encryption keys • Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures • Changing default encryption keys • Replacement schedule for various types of encryption keys For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html

		Oracle Hospitality OPERA Cloud change management processes includes tokenization and cryptography. Oracle Hospitality OPERA Cloud follows PCI-DSS guidelines with regards to encryption technologies.
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Representatives from Corporate Security and development organizations define recommended practices related to using and implementing cryptography in Oracle products, derived from frequent reviews of existing industry practices and current threat intelligence. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html
		Oracle Hospitality OPERA Cloud services follow OSSA and must be approved per the Corporate Security Solution Assurance Process (CSSAP).
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Representatives from Corporate Security and development organizations define recommended practices related to using and implementing cryptography in Oracle products, derived from frequent reviews of existing industry practices and current threat intelligence. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html
		In accordance with the Cloud Compliance Standard for Risk Management, risk assessments are performed annually across Oracle Hospitality OPERA Cloud applications to identify threats and risks that could impact the security, confidentiality, or availability of the system.Risks rated critical and high are reviewed, assigned an owner, and remediated in line with the Oracle Hospitality OPERA Cloud's risk management assessment program
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	Oracle Hospitality OPERA Cloud 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 Hospitality OPERA Cloud 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)?	Oracle Hospitality OPERA Cloud 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 Hospitality OPERA Cloud 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. 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 Hospitality OPERA Cloud keys are provisioned for a unique purpose and are stored in a Hardware Security Module (HSM).
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	For Oracle Hospitality OPERA Cloud, cryptographic key rotation occurs based on regulation, certification, or for 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 Hospitality OPERA Cloud Service cryptographic keys are revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions.
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 Hospitality OPERA 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,	Oracle Hospitality OPERA Cloud services follow Oracle Software Security Assurance for all key management practices. Processes, procedures, and technical measures are in place to create keys in a pre-activated state. Keys are not created prior to authorization to use.

	implemented, and evaluated to include legal and regulatory requirement provisions?	
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 Hospitality OPERA Cloud services follow Oracle Software Security Assurance for all key management practices. Processes, procedures, and technical measures are in place to monitor, review and approve key transitions. Oracle Hospitality OPERA Cloud services leverages key management software that allows for the approval and change of state for all key change of state transitions.
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Oracle Hospitality OPERA Cloud services follow Oracle Software Security Assurance for all key management practices. Processes, procedures, and technical measures are in place to deactivate keys as required. Oracle Hospitality OPERA Cloud services leverages key management software that allows for the deactivation and key change of state.
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Oracle Hospitality OPERA Cloud services follow Oracle Software Security Assurance for all key management practices. Processes, procedures, and technical measures are in place to manage archived keys in a secure repository.
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 Hospitality OPERA 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,	Oracle Hospitality OPERA Cloud services have processes, procedures, and technical measures to assess operational continuity risks are defined, implemented and evaluated to include legal and regulatory requirement provisions.

	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 regulatory requirements provisions?	Oracle 's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services, including legal and regulatory requirements. Oracle Hospitality OPERA 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 See also: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html

Control Domain: Data Center Security

Question ID	Consensus Assessment Question	Oracle Response
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Oracle's Media Sanitization Policy specifies requirements including secure disposal of equipment and media used for data storage. This policy is established, documented, approved, communicated, and maintained.
		Oracle Hospitality OPERA Cloud have processes and procedures that follow Oracle's Media Sanitization and Disposable Policy and Enterprise Engineering Media Sanitization and Disposal Standard. I
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Oracle's Media Sanitation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. For more information, https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
		Oracle Hospitality OPERA Cloud processes and procedures follow Oracle's Media Sanitization and Disposal Policy and PCI DSS Requirement 3.2.1 which requires that data is securely deleted.
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.
		Oracle Hospitality OPERA Cloud services processes and procedures are reviewed annually.
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware,	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,

	software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	documented, approved, communicated, and maintained. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
		Oracle Hospitality OPERA Cloud maintains 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 Hospitality OPERA Cloud does require manager approval for the relocation of all datacenter assets in accordance with published corporate policy. For further information please also refer to the published Change Management Policy Section 4.1: https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address the relocation or transfer of hardware, software, or data/information to any location) are reviewed annually and updated as needed.
		Oracle Hospitality OPERA Cloud services follow the Oracle Corporate Security policies, including the polices that address secure disposal of equipment outside the organization's premises.
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html
		Oracle Hospitality OPERA Cloud services relies on Oracle Global Physical Security to manage all aspects of physical security.
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address safe and secure working environments) are reviewed annually and updated as needed.
		Oracle Hospitality OPERA Cloud services relies on Oracle Global Physical Security to manage all aspects of physical security
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Oracle Hospitality OPERA Cloud services relies on Oracle Global Physical Security policies and procedures for the secure transportation of physical media, 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 Hospitality OPERA Cloud 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 Hospitality OPERA Cloud 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 Hospitality OPERA Cloud 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/communications-operations-management.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 Hospitality OPERA Cloud services relies on Oracle Global Physical Security to manage all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets.
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	The goal is to balance prevention, detection, protection, and response, while maintaining a work environment that fosters collaboration among Oracle employees.
		Oracle Hospitality OPERA 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. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
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 Hospitality OPERA Cloud uses machine certificates and other identifiers to validate that the device is Oracle owned and provisioned before allowing access to resources. Oracle Hospitality OPERA Cloud 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	Oracle has implemented the following protocols: • Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors. • Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises.

	physical access control mechanisms?	For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html Oracle Hospitality OPERA 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-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors. Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises. Visitors are required to sign a visitor's register, be escorted and/or observed when they are on Oracle premises, and/or be bound by the terms of a confidentiality agreement with Oracle. Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving Oracle's employment must return keys/cards and key/cards are deactivated upon termination. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html Oracle Hospitality OPERA 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-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Oracle uses a mixture of 24/7 onsite security officers or patrol officers, depending on the risk/protection level of the facility. In all cases officers are responsible for patrols, alarm response, and recording of security incidents. Oracle has implemented centrally managed electronic access control systems with integrated intruder alarm capability and CCTV monitoring and recording. The access control system logs and CCTV recordings are retained for a period of 30-90 days as defined in Oracle's Record Retention Policy which are based on the facility's function, risk level and local laws. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html Oracle Hospitality OPERA 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-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 Oracle Hospitality OPERA 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-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Data centers hosting Oracle cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria. Oracle cloud service data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Personnel are trained in procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html Oracle Hospitality OPERA 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-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 Hospitality OPERA Cloud follow the Oracle's Information Protection Policy. The policy provides GlU guidance and determines appropriate controls to protect data that follow the Oracle data classification and handling of data throughout its lifecycle.
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 Hospitality OPERA Cloud security and privacy procedures are reviewed annually and updated as needed.
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Industry accepted methods are applied for secure data disposal from storage media. Oracle's Media Sanitation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/
		Oracle Hospitality OPERA Cloud follows Oracle's Media Sanitization and Disposal Policy and the requirements of PCI DSS Requirement 3.2.1
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Oracle Hospitality OPERA 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 Hospitality OPERA Cloud. This documentation is for internal use only. For more information, 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?	Oracle Hospitality OEPRA Cloud Data Flow documentation is reviewed at least annually, or after any architectural change, and updated as needed.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Oracle's Information Systems Asset Inventory Policy requires that an accurate and current inventory (including data owners and data stewards) be maintained for all information systems holding critical and highly critical information assets in Oracle Corporate and cloud infrastructures.
		Oracle Hospitality OEPRA Cloud has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Information designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. The customer is the controller of their data.
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Oracle Hospitality OPERA Cloud follow Oracle's Information Protection Policy that requires Ownership and stewardship of all relevant personal and sensitive data to be documented. 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?	Oracle Hospitality OPERA Cloud 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.
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Oracle Hospitality OPERA Cloud system, products, and business practices are based on privacy principles by design and per industry best practices. Oracle's privacy policies and practices cover the management of privacy for both Oracle's internal operations and the services Oracle provides to its customers, and

		apply to all Oracle personnel, such as employees and contractors. These policies are aligned with ISO 27018 and SSAE18 SOC1 / SOC2.
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html
		Privacy settings for Oracle Hospitality OPERA Cloud services are controlled by the customer.
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations, and industry best practices?	Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html
		Oracle Hospitality OPERA Cloud performs impact assessments for all new products and feature enhancements being brought to market.
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Oracle Hospitality OPERA Cloud processes, procedures, and technical measures are in place to help ensure that transfer of sensitive data is protected from unauthorized access and is follows data transfer laws and regulations. Oracle has Business Continuity Policies/Practices in place as well as an approved Data Protection Agreement (DPA). See the following links for additional information: https://www.oracle.com/ie/corporate/contracts/cloud-services/contracts.htmlhttps://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 Hospitality OPERA 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 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
		Where applicable, Oracle Hospitality OPERA Cloud services follows applicable laws and regulations for protecting personal data For more detail, please refer to: https://www.oracle.com/security/gdpr/ 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,	Please see the Oracle privacy policies at https://www.oracle.com/legal/privacy/

	implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Oracle Hospitality OPERA Cloud services have processes, procedures, and technical measures in place for the transfer and sub-processing of personal data within the service supply chain. Oracle and Oracle Affiliates employees, as well as any Third-Party sub-processors that Process Personal Information, are subject to appropriate written confidentiality arrangements, including regular training on information protection, and compliance with Oracle policies concerning protection of confidential information.
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Process, procedures, and technical measures are defined, implemented, and evaluated as part of Oracle Privacy policies. Please see the following for additional information. https://www.oracle.com/legal/privacy/ Oracle Hospitality OPERA 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. These sub-processor lists are distributed to customers via the Oracle Cloud Customer Support Portal. 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 at Oracle. 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 Hospitality OPERA 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 Hospitality OPERA 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's customers are responsible for the proper handling of any data they choose to collect, store, or process, and to ensure that handling complies with all applicable law and regulation. Oracle makes available Data privacy and Data processing agreements for CSC review; these can be found at: https://www.oracle.com/contracts/cloud-services/ Customers typically have direct access to their data stored in their services environments. Oracle therefore believes that customers are generally in a better position to identify and access their own data

		in response to a legal access request. However, If Oracle receives a Disclosure Request it will first assess the legality thereof whether it remains within the powers granted to the requesting authority. Oracle will challenge Disclosure Requests that it considers unlawful under the laws of the Third Country, applicable obligations under international law, or principles of international comity, and under the same conditions shall pursue possibilities to appeal. When challenging a Disclosure Request, Oracle shall seek interim measures with a view to suspending the effects of the Disclosure Request until the requesting authority has decided on its merits. Oracle shall not disclose the Personal Information requested until required to do so under the applicable procedural rules and will only provide the Personal Information that is strictly necessary when complying with a Disclosure Request, based on a reasonable interpretation thereof. Oracle will document this assessment and provide it to the Data Exporter and, upon request, to the Competent SA. Subject to this paragraph, Oracle shall inform the Customer and the Lead SA, and cooperate with the Customer to inform the Customer's SA, of a Disclosure Request. Oracle will also request that the requesting authority delay the Disclosure Request in order to enable the Lead SA and/or the Customer's SA to issue an opinion on the validity of the relevant disclosure. Notifications of a Disclosure Request shall include information about the data requested, the requesting body, and the legal basis for the disclosure. If notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, Oracle will request the relevant authority to waive this prohibition and will document that it has made this request, which documentation will be provided to the Lead SA upon request. If, despite its efforts, Oracle does not obtain a waiver, Oracle will on an annual basis provide to the Lead SA general information on the number and type of Disclosure Requests it received in the preceding 12 month period, to the fullest extent permitted by Applicable Law. In any event, any transfers by Oracle of Personal Information in response to a Disclosure Request will not be massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society. This Article does not apply to requests received by Oracle from other government agencies in the normal course of its activities, which Oracle can continue to provide in accordance with Applicable Law, as far as the request is necessary and proportionate in a democratic society to 13 protect one of the objectives listed in article 23(1) of the GDPR. Please also refer to: Oracle Cloud Service Agreement - https://www.oracle.com/corporate/contracts/cloudservices/contracts.html#ct07tabcontent1 Please review the Oracle Data Processing Agreement and BCR Oracle's Binding Corporate Rules for Processors (Oracle Processor Code); https://www.oracle.com/corporate/contracts/cloudservices/contracts.html#ct07tabcontent1 SaaS Services are delivered in accordance with the oracle services privacy policy: https://www.oracle.com/au/legal/privacy/services-privacy-policy.html
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition	Oracle will promptly inform You (Customer) of requests to provide access to Personal Information unless otherwise required by law. Please see: Oracle's Binding Corporate Rules for Processors (Oracle Processor Code)

	under criminal law to preserve confidentiality of a law enforcement investigation?	
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Oracle Hospitality OPERA Cloud services has processes, procedures, and technical measures implemented to specify and document physical data locations, including locations where data is processed or backed up.

Control Domain: Governance, Risk & Compliance

Question ID	Consensus Assessment Question	Oracle Response
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Global Information Security (GIS) defines policies for the Line of Business management of information security across Oracle. Additionally, GIS sets direction and provides advice to help protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners, and employees. GIS also coordinates the reporting of information security risk to senior leadership such as the Oracle Security Oversight Committee and Board of Directors. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html
		Oracle Hospitality OPERA Cloud has an information governance program policies and procedures sponsored by Oracle Global Information Security (GIS) established, documented, approved, communicated, applied, evaluated, and maintained. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle. For more information, see https://www.oracle.com/corporate/securitypractices/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 Hospitality OPERA Cloud GIU 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	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

	management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	departments drive the corporate security programs, define corporate security policies, and provide security assurance oversight of Lines of Business. Corporate Security Architecture manages a cross-organization working group focused on security architecture of corporate and cloud systems. Participation includes members from cloud service development, operations, and governance teams. Each Line of Business is responsible implementing associated procedures. Oracle Privacy & Security Legal manages the cross-organization oversight of privacy risks. For more information, see https://www.oracle.com/legal/privacy/
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Oracle Corporate Security policies are reviewed annually and updated as needed. Oracle Hospitality OPERA Cloud GIU has procedures (including those that address cloud security and privacy risks) are reviewed annually and updated as needed.
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Global Information Security (GIS) manages a security exception program which oversees LoB exception and exception management activity. Oracle Hospitality OPERA Cloud follows Oracle Corporate Policies including the 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 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. See: https://www.oracle.com/corporate/security-practices/corporate/governance.html Oracle Hospitality OPERA Cloud maintains PCI DSS validation and issues SOC 1 and SOC 2 reports annually. These are available for customer review upon request. See https://www.oracle.com/corporate/cloud-compliance/
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	See GRC-05.1
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	All relevant standards, regulations, legal/contractual, and statutory requirements applicable to Oracle are identified and documented. Oracle Legal monitors the global regulatory landscape to identify legislation applicable to Oracle, including regional and local teams monitoring changes in relevant jurisdictions.. In addition, Oracle Global Trade Compliance (GTC) is responsible for import and export oversight, guidance, and enforcement to enable worldwide trade compliant processes across Oracle. For more information,

		see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-trade-compliance.html. Customer remains solely responsible for its regulatory compliance in its use of any Oracle Cloud services. 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 Hospitality OPERA Cloud maintains a relationship with PCI SSC Cloud Computing special interest group. Please see link below for additional information. https://listings.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf

Control Domain: Human Resource Security

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

	assets established, documented, approved, communicated, applied, evaluated, and maintained?	services. For more information, see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
		Oracle Hospitality OPERA Cloud services relies on Oracle Corporate Security and Corporate HR policies (including policies that address Acceptable Use). See: https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Oracle Corporate Security policies (including the Acceptable Use Policy) are reviewed annually and updated as needed. Oracle has formal "acceptable use of asset" policy requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, internet access, and other company resources available to Oracle employees, contractors and visitors. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html
		Oracle Hospitality OPERA Cloud follows the acceptable use policy for use of organizationally owned 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 data reviewed and updated at least annually?	Oracle Hospitality OPERA Cloud requires annual information protection awareness training. Additional security and confidentiality training for developers.
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 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 Hospitality OPERA 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. For more information, 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 Hospitality OPERA 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 regularly reviews network and operating system accounts regarding the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Please see HRS-02.1
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Please see HRS-02.1
HRS-09.1	Are employee roles and responsibilities relating to	Oracle's information asset classification determines corporate data-security requirements for Oracle managed systems. Oracle policies and standards provide global guidance for appropriate controls

	information assets and security documented and communicated?	designed to protect the confidentiality, integrity, and availability of corporate data in accordance with the data classification. Required mechanisms are designed to be commensurate with the nature of the corporate data being protected. For example, security requirements are greater for data that is sensitive or valuable, such as cloud systems, source code and employment records. Oracle's corporate security controls can be grouped into three categories: administrative, physical, and technical security controls. • Administrative controls, including logical access control and human resource processes • Physical controls designed to prevent unauthorized physical access to servers and data processing environments • Technical controls, including secure configurations and encryption for data at rest and in transit The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/
		Customers are responsible for the management of identity and access to their data in their use of Oracle Hospitality OPERA Cloud. IAM 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 operational details identified, documented, and reviewed at planned intervals?	Please see HRS-02.1
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Employees who fail to comply with these policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment. Each employee is required to complete information-protection awareness training upon hiring and every two years. The course instructs employees on their obligations under Oracle policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs and are required by company policy. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html

HRS-11.2	Are regular security awareness training updates provided?	Please see HRS-11.1
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Please see HRS-11.1
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Please see HRS-11.1
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	See HRS-11.1

Control Domain: Identity & Access Management

Question ID	Consensus Assessment Question	Oracle Response
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. Oracle Hospitality OPERA Cloud publishes its identity and access procedures for customers at the following location: https://docs.oracle.com/en/industries/hospitality/hotels.html under the sub-section OPERA Cloud Identity Management. With role manager documentation detailed at https://docs.oracle.com/en/industries/hospitality/identity-management/24.3/ocimy/t_responsibilities.htm

IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including policies applicable to identity and access management) are reviewed annually and updated as needed.
		Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. Oracle Hospitality Opera Cloud customer guidance is reviewed with each product release.
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
		Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. Oracle Hospitality OPERA Cloud follows Oracle corporate policies and complies with PCI DSS requirements for strong passwords.
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 primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. Oracle Hospitality OPERA Cloud password requirements are reviewed at least annually.
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
		Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. Oracle Hospitality OPERA Cloud provides tools and guidance to customer for identity management within OPERA. Related documentation can be found below: https://docs.oracle.com/en/industries/hospitality/identity-management/24.3/index.html
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. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest?
		Customers are responsible for ensuring separation of duties in their use of Oracle cloud services. Oracle Hospitality OPERA Cloud 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: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest? • Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose? For more information, see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		Customers are responsible for user access provisioning and role assignment when connecting to Oracle Hospitality OPERA Cloud. Opera Cloud supports Role Based Access in adherence to the principle of least privilege and segregation of duty within the integrated role management included with the product. OPERA Cloud users need to be assigned roles by Customer administrators before access to the application is enabled.
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: https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. Oracle Hospitality OPERA Cloud user access and provisioning is documented: https://docs.oracle.com/en/industries/hospitality/identity-management/24.3/index.html
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or	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

	system identity changes, to effectively adopt and communicate identity and access management policies?	access. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		Customers are responsible for user access de-provisioning in their use of Oracle Hospitality OPERA Cloud. Oracle does not have access to customer Data. Support user access is strictly controlled and granted only for the time period specified by the customer. At the set end date application access will be automatically revoked.
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 their corporate user access for least privilege and separation of duty to their SaaS instance of Oracle Hospitality OPERA Cloud. Oracle Hospitality OPERA Cloud 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?	Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. Oracle Hospitality OPERA Cloud services follows the documented 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?	Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. Oracle Hospitality OPERA Cloud services access processes are defined and implemented. Privileged Access roles and rights have processes to help ensure they are reviewed on a quarterly basis. Privileged Account passwords expire on a shortened cycle. For more information see: https://www.oracle.com/corporate/security-practices/corporate/access-control.html
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services.
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented, and evaluated?	Customers are responsible for review and revalidation of user access de-provisioning in their use of Oracle cloud services. Oracle Hospitality OPERA Cloud services document their customer Identity and access for privileged administrative accounts https://docs.oracle.com/en/industries/hospitality/identity-management/24.3/ocimy/t_responsibilities.htm

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 Hospitality OPERA 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 with user identification usage) defined, implemented, and evaluated?	Customers are responsible for the management of identity and access to their data in their use of Oracle Hospitality OPERA Cloud. For Oracle Hospitality OPERA Cloud, the processes, procedures, and technical measures that help ensure users are identifiable through unique identification (or can associate individuals with user identification usage) are defined, implemented, and evaluated. Each user is assigned a unique identifier/account through IAM.
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?	Processes, procedures, and technical measures are in place for authenticating access to systems, applications and data assets including multifactor authentication for a least-privileged user and sensitive data access. The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. 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 based on the following principles: • Need to know: Does the user require this access for his job function • Segregation of duties: Will the access result in a conflict of interest? • Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose. Oracle does not control the roles and groups assigned to Customer users of their products. Oracle Hospitality OPERA Cloud is provisioned with the ability for the user to manage Identity and Access rights together with the assignment of additional factors during the initial login, Customers are responsible for administering the user privilege and data access rights.
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Oracle Hospitality OPERA Cloud services rely 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. 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 Hospitality OPERA Cloud. IAM processes, procedures, and technical measures are in place for the secure management of passwords. These are documented here: https://docs.oracle.com/en/industries/hospitality/identity-management/24.3/ocimy/t_responsibilities.htm
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 Hospitality OPERA Cloud. These responsibilities are documented here. https://docs.oracle.com/en/industries/hospitality/identity-management/24.3/ocimy/t_responsibilities.htm For administration of network security and network-management devices, Oracle Hospitality OPERA 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/securitypractices/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 Hospitality OPERA Cloud has a dedicated integration platform and approved interfaces to allow data transfer into and out of Opera Cloud. Documentation detailing how these interfaces can be used is detailed at: https://www.oracle.com/industries/hospitality/integration-platform/
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Oracle Hospitality OPERA Cloud has a dedicated integration platform and approved interfaces to allow data transfer into and out of Opera Cloud. Documentation detailing how these interfaces can be used is detailed at: https://www.oracle.com/industries/hospitality/integration-platform/

IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Oracle Hospitality OPERA Cloud has a dedicated integration platform to help enable user custom development across different user platforms this is documented at: https://docs.oracle.com/en/industries/hospitality/hotels.html
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Oracle Hospitality OPERA Cloud is a SaaS product which is deployed in accordance with Oracle Corporate Security policy, Oracle corporate policies are published online at: https://www.oracle.com/corporate/security-practices/ Oracle Hospitality OPERA Cloud is deployed only on Oracle Cloud Infrastructure (OCI). Users wishing to import/export data must follow the published API specifications which can be viewed here: https://docs.oracle.com/en/industries/hospitality/hotels.html
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Oracle Hospitality OPERA Cloud procedures (including interoperability and portability policies) are reviewed annually and updated as needed.
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Some Oracle Hospitality OPERA 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?	All data in transit for Oracle Hospitality OPERA Cloud including data import or export is encrypted in accordance with the Oracle Hosting and Delivery Polices. See Section 1.5: https://www.oracle.com/contracts/cloud-services/
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Oracles Cloud Hosting and Delivery policies include provisions for CSC data access upon contract termination. For a period of 60 days upon termination of the Oracle Cloud Services, Oracle will make available, via secure protocols and in a structured, machine-readable format, Customer Content residing in the production Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by Customer. Any terms and conditions related to Oracle 's performance of the applicable services shall be specified in the customer order for services documentation. Please refer to: https://www.oracle.com/contracts/cloud-services/

Control Domain: Infrastructure & Virtualization Services

Question ID	Consensus Assessment Question	Oracle Response

IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle Hospitality OPERA Cloud is deployed on OCI . See: https://www.oracle.com/corporate/security-practices/corporate/
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Oracle Hospitality OPERA Cloud relies on the OCI Host Hardening standard addresses infrastructure and virtualization and follows Oracle policies See: https://www.oracle.com/corporate/security-practices/corporate/
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Oracle Hospitality OPERA Cloud is deployed on OCI with managed capacity management and monitoring to help ensure service availability uptime and performance is in accordance with its published guidelines. OCI collects and monitors capacity and utilization data. This data is used to plan for adequate capacity to help meeting current, projected, and anticipated needs and customer service level agreements. See: https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf within section 3.2 Service Availability
IVS-03.1	Are communications between environments monitored?	Oracle Cloud Infrastructure monitors, encrypts, and restricts communications between environments to only authenticated and authorized connections, as justified by the business.
IVS-03.2	Are communications between environments encrypted?	Oracle Cloud Infrastructure monitors, encrypts, and restricts communications between environments to only authenticated and authorized connections, as justified by the business. Furthermore, connections to the customer administration console, currently 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 during transport across public networks.
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	As defined in the Oracle Network Security Policy, Oracle Hospitality OPERA Cloud restricts communication between environments to only authenticated and authorized connections. please see: https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
IVS-03.4	Are network configurations reviewed at least annually?	Oracle Hospitality OPERA Cloud network configurations are reviewed at least annually and updated as needed.
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Oracle Hospitality OPERA Cloud follows the defined process Corporate Security Solution Assurance Process (CSSAP). This process ensures justification and approval of the proposed configuration change has taken place. 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	OCI employs standardized system hardening practices across Oracle Hospitality OPERA Cloud instances. This includes alignment monitoring with base images and/or baselines, restricting protocol access,

	supported by technical controls as part of a security baseline?	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 Hospitality OPERA Cloud production and non-production platforms are logically separated.
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Oracle Hospitality OPERA Cloud 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 and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Your access to Oracle Hospitality OPERA Cloud is through a secure communication protocol. Staging networks are segregated from production-level networks and utilized when migrating production data to virtual servers. Physical servers, applications, and virtual machines are not moved. New environments are provisioned using a hardened master image with customer data migrated once the provisioning process is complete. Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Customer configuration information (e.g., connection strings, application settings) supplied through the management portal is protected while in transit and at rest.
IVS-08.1	Are high-risk environments identified and documented?	Oracle 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 Hospitality OPERA Cloud implements application layer security combined with OCI network layer security framework to help detect and protect from network-based attacks. OCI employs intrusion-detection systems to provide continuous surveillance for intercepting and responding to security events as they are identified. OCI utilizes a network-based monitoring approach to detect attacks on open firewall ports within Oracle's Cloud Infrastructure. Events are analyzed using signature detection, which involves pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to Oracle's security personnel for review and response to potential threats. For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html .

Control Domain: Logging & Monitoring

Question ID	Consensus Assessment Question	Oracle Response
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Logging and monitoring policies are established, documented, approved, communicated, evaluated, and maintained by Oracle Corporate Security. Oracle Lines of Business (LoBs) are required to capture and store logs for certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html
		Oracle Hospitality OPERA Cloud employs processes to capture and store logs for certain security-related activities on operating systems, applications, databases, and network devices to support Oracle Logging and Monitoring polices. For more information, see the 'Monitoring ' section of the Oracle Cloud Hosting and Delivery Policies document: https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address logging and monitoring) are reviewed annually and updated as needed.
		Oracle Hospitality OPERA Cloud services has a defined GBU Security Logging Standard. This standard supports the Oracle Logging and Log Analysis Policy.
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Processes, procedures, and technical measures are in place to help ensure audit log security and retention. Oracle centrally logs certain security-related activities, such as events and activities from operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Log files are protected by strong cryptography, multi-factor authentication, and secure architectures. Oracle adheres to least privilege practices, and access to audit logs is monitored. The information management and records retention policy outline the required retention of audit logs, security events, and any protentional investigative reports. The retention of these records also adheres to any applicable government and compliance programs. Oracle Hospitality OPERA Cloud has a defined GBU Security Logging Standard. This standard supports the Oracle Logging and Log Analysis Policy. The following are defined in the standard: 1. Information included in the log collection record 2. Events to be logged 3. Log Storage 4. Retention period and classification 5. Frequency of Analysis of Logs
LOG-03.1	Are security-related events identified and monitored within	Oracle Hospitality OPERA Cloud logs application security events to the SEIM. Infrastructure security related events (application logs, system events, firewall logs, network flows, etc.) from Oracle Hospitality

	applications and the underlying infrastructure?	OPERA Cloud and its underlying OCI based infrastructure are logged into a Security Information and Event Management (SIEM) solution to correlate information and alert on any potential security event.
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Oracle Hospitality OPERA Cloud services is deployed on OCI, where a system is defined and implemented to generate alerts and notify responsible stakeholders. Oracle Cloud Infrastructure has deployed a security information and event monitoring (SIEM) solution in each region which ingests and stores security-related logs and alerts from networking devices, hosts, and other components within the infrastructure. Access to logs is controlled in a permissions system and is restricted to authorized personnel. Oracle Cloud Infrastructure's Detection and Response team (DART) monitors the SIEM for event correlations and other relevant detection scenarios on a 24x7 basis to help defend and protect\ against unauthorized intrusions and activity in the production environment.
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	The GBU Logging and Log Analysis Standard defines security and parameters (including retention) for Oracle Hospitality OPERA 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 Hospitality OPERA Cloud is deployed on OCI. Oracle Hospitality OPERA Cloud logs application security events to the SEIM. The SIEM has detections to monitor anomalous activities. Oracle has dedicated detection and response teams that focus on designing and implementing solutions to help identify Tactics, Techniques, and Procedures (TTPs) of threat actors.
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Oracle Hospitality OPERA Cloud services has defined procedures and processes to help 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 Hospitality OPERA Cloud 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 Hospitality OPERA 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 Hospitality OPERA 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 Hospitality OPERA 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 Hospitality OPERA Cloud log files are protected by strong cryptography in addition to role-based access controls, truncation, masking, and encryption of sensitive data, . Access to these logs is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Oracle monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. There are logs generated and mechanisms in place to review/respond to activity.
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Oracle monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. Logs are generated and mechanisms have been put in place to review activity.
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	For datacenters hosting Oracle Hospitality OPERA Cloud physical access to the facilities is limited and all access is logged. For more information, see: 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?	OCI 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 Hospitality OPERA Cloud leverages a Security Information and Event Management (SIEM) solution to correlate information such as system events, firewall logs, WAF logs, network flows from the environment and to alert on any potential security event. Oracle Security Operations Center (SOC) monitor the SIEM 24x7x365 and have defined processes to escalate events as needed. This process includes reporting and notification requirements to system owners and Oracle leadership.

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

Question ID	Consensus Assessment Question	Oracle Response

SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Policies and procedures for security incident management, e-discovery, and cloud forensics are established, documented, approved, communicated, applied, evaluated, and maintained with the oversight of Oracle Global Information Security. Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed data has been unproperly handled or accessed. Note that cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available logs and other tooling. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to security events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for security event and incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). GIS defines roles and responsibilities for the incident response teams embedded within the Lines of Business (LoBs). All LoBs must comply with GIS incident response guidance about detecting events and timely corrective actions. Upon discovery of an incident, Oracle defines an incident response plan for rapid and effective incident investigation, response, and recovery. Formal procedures and systems are utilized within the Lines of Business (LoBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
		All Security related events (system events, firewall logs, network flows, etc.) from Oracle Hospitality OPERA 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 Hospitality OPERA Cloud procedures are reviewed annually and updated as needed.
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Please see SEF-01.1
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Oracle Corporate Security policies and procedures that address timely management of security incidents are reviewed annually and updated as needed.
		Oracle Hospitality OPERA Cloud services security procedures, that follow Oracle Corporate Security policies that address timely management of security incidents,are reviewed annually and updated as needed.

SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). Corporate requirements for LoB incident-response programs and operational teams are defined per incident type: • Validating that an incident has occurred • Communicating with relevant parties and notifications • Preserving evidence • Documenting an incident itself and related response activities • Containing an incident • Addressing the root cause of an incident • Escalating an incident For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Oracle Hospitality OPERA 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) as per applicable SLAs, laws, and regulations?	Please see SEF-01.1 For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html

SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Oracle maintains points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

Control Domain: Supply Chain Management, Transparency & Accountability

Question ID	Consensus Assessment Question	Oracle Response
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, 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/ Oracle has policies designed to help protecting 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 help mitigating the risks associated with the malicious alteration of products before installation by customers. Oracle suppliers are required to comply with the Supplier Information and Physical Security Standards of mandatory security controls. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ Oracle's Supplier Management Security Policy defines requirements for Lines of Business supplier management programs, to guide selection and management of suppliers each LOB utilizes.
		As part of the GIU Supplier Management program, a central repository of GIU suppliers is maintained. The suppliers are assigned a Risk Category which is used to schedule security assessments. The suppliers are assessed regularly to help ensure GIU suppliers are following supplier requirements (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?	Oracle Hospitality Opera Cloud undergoes PCI-DSS assessments and provides customers with a PCI-DSS shared responsibility matrix. . The GIU Supplier Management program procedures are updated and reviewed annually. 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 Hospitality OPERA Cloud. 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?	Quality and reliability for Oracle Hospitality OPERA Cloud 's Applications' hardware systems are addressed through a variety of practices, including design, development, manufacturing, and materials management processes. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	The Oracle Cloud Hosting and Delivery Policies describe the customer (tenant) security obligations. Also, the Oracle Data Processing Agreement includes the responsibilities of the data controller (tenant/customer) versus data processor (Oracle). Please see the Oracle Hosting and Delivery Policies located at https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html and the Oracle Data Processing Agreement at https://www.oracle.com/contracts/cloud-services/
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Oracle Hospitality OPERA 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 Hospitality OPERA 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 Hospitality OPERA Cloud services, maintains 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. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Oracle's Supply Chain Risk Management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services. Supply availability, continuity and resiliency in Oracle's hardware supply chain are addressed through a variety of practices, including: • Multi-supplier and/or multi-location sourcing strategies where possible and reasonable. • Review of supplier financial and business conditions. • Requiring suppliers to meet minimum purchase periods and provide end-of-life (EOL)/end-of-support-life (EOSL) notice. • Requesting advance notification of product changes from suppliers so that Oracle can assess and address any potential impact. • Managing inventory availability due to changes in market conditions and due to natural disasters.

		For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ Additionally, Oracle Hospitality OPERA Cloud follows guidelines to review any third-party tools and libraries to help ensure they are updated with every major release and contain no reported vulnerabilities. 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? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Oracle makes available its Oracle Cloud Services contracts for download from the following location: https://www.oracle.com/contracts/cloud-services/ Note, you will need to select your specific region and the 'Hospitality' product. The documentation is grouped according to policy area: Cloud Services Agreement – this covers contractual terms which cover the SaaS Service offered including fees, rights/restrictions, 3rd parties and term. Cloud Service Descriptions – details the specific service description and SLA for the SaaS service you are using. Professional Services and Support Services Service Descriptions – covers any professional services which are required for the service delivery. Delivery Policies – this includes detail about how Oracle will deliver your content detailing the Security Policy, Continuation policy, Service Level Agreement, Change Management Policy, logging and monitoring and Support. Oracle Corporate Security Policy: which outlines the security governance process for the Oracle Corporation. Privacy Documents – this includes the data processing Agreement for oracle services, including right to audit, incident management, and service termination. Oracle Corporate Security policy details how oracle develops and maintains Enterprise cloud services.
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Oracle Hospitality OPERA Cloud reviews and manages supply chain agreements as needed, but at least annually.
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Oracle Hospitality OPERA Cloud has 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,	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

	personnel policy, and service level requirements and standards implemented?	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/s
		Oracle Hospitality OPERA Cloud services security procedures are reviewed and updated as needed. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	See STA-13.1

Control Domain: Threat & Vulnerability Management

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

		Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Customers and security researchers can report suspected security vulnerabilities to Oracle: How to Report Security Vulnerabilities to Oracle or by submitting a Service Request in their support system. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html and https://www.oracle.com/corporate/security-practices/assurance/vulnerability/
		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 Hospitality OPERA Cloud procedures (including policies and procedures that address 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
		Oracle Hospitality OPERA Cloud has procedures in place to help protecting against malware on managed assets.
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 Hospitality OPERA Cloud Security Standards (including standards that address asset management and malware protection) are reviewed annually and updated as needed.
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability	Oracle Hospitality OPERA Cloud processes, procedures, and technical measures are defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk.) Oracle Hospitality OPERA 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

	identifications (based on the identified risk)?	Scoring System (CVSS) Base Score, and remediation timelines are based upon the assigned severity and possible business impact. Please see: https://www.oracle.com/security-alerts/ 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 Oracle Hospitality OPERA 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 Hospitality OPERA Cloud services processes, procedures and technical measures are defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries. During the Development cycle, development teams are required to vet and get Corporate Architecture approval for any third-party software that may be embedded in Oracle products. The Oracle Hospitality OPERA Cloud services development has patching and release cycles that require that third-party components be evaluated or reevaluated for any vulnerabilities found in testing or through notifications of vulnerabilities. The severity of vulnerabilities is determined using a Common Vulnerability Scoring System (CVSS) Base Score, and remediation timelines are based upon the assigned severity and possible business impact
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Processes, procedures, and technical measures are in place for independent third-party penetration testing. In accordance with PCI requirement 11 Oracle Hospitality OPERA Cloud is required to undertake regular vulnerability and 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?	Processes procedures, and technical measures are in place for vulnerability detection on Oracle Hospitality OPERA Cloud managed assets at least monthly.
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 Hospitality OPERA Cloud Service Applications' vulnerability remediation is prioritized using a risk-based model from an industry recognized framework. The remediation process ensures all testing or reported vulnerabilities are evaluated and patches are deployed across all Oracle Hospitality OPERA Cloud products based on criticality. The severity of vulnerabilities is determined using the Common Vulnerability Scoring System (CVSS) Base Score.
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	See TVM-01.1. Oracle Hospitality OPERA Cloud follows Oracle policy having 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 Hospitality OPERA Cloud participates in OCI system for notifications to 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 Oracle Hospitality OPERA Cloud follows Oracle policy having 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 Hospitality OPERA Cloud participates in OCI system for notifications to 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. 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 Hospitality OPERA Cloud services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Hospitality OPERA 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 Hospitality Cloud Services 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. Oracle maintains a repository of approved software for all Oracle managed endpoint devices.
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	Please see UEM-01.1. This list is approved by Oracle Corporate Architecture and maintained by Oracle Information Technology.
		Oracle Hospitality OPERA Cloud relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for all cloud endpoints. Oracle Hospitality OPERA Cloud endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP).
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 Hospitality OPERA Cloud endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP). Where CSSAP or SOC audits requires it, penetration testing is scheduled and performed.
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Oracle's Information Systems Asset Inventory Policy requires that Line of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware and software.
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, 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. To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full disk encryption software on their laptops and desktops, except where approved for justifiable business purposes. Data on the disk can only be accessed through the use of a private key stored as a password-protected file on the disk. A preboot login manager allows authorized users to login to unlock the key, boot the operating system, and access the data. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
		Oracle Hospitality OPERA Cloud endpoint management processes and procedures follow Oracle Corporate policy.
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 Hospitality OPERA Cloud services.

		Oracle Hospitality OPERA Cloud SaaS enforces an unattended automatic lock screen as a default setting in accordance with PCI that is enforced by the application.
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	The Oracle Information Technology keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. OIT is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. OIT provides automation to verify antivirus configuration. Oracle employees are required to comply with email instructions from OIT and are responsible for promptly reporting to the Oracle employee helpdesk any virus or suspected virus infection that cannot be resolved by antivirus software. Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
		Oracle Hospitality OPERA Cloud services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for endpoints. Oracle Hospitality OPERA Cloud Service endpoints are reviewed and approved via the Corporate Security Solution Assurance Process (CSSAP).
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 Hospitality OPERA Cloud services relies on Oracle Corporate Security and Oracle Cloud infrastructure (OCI) provided processes, procedures, and technical measures for endpoints. Oracle Corporate Security policy requires the use of antivirus, intrusion protection and firewall software on laptops and mobile devices. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Oracle Hospitality OPERA Cloud relies on OCI for managed endpoint configuration. OCI has dynamic access policies configured to validate the following items on endpoints before granting access to the infrastructure supporting OCI services: • Devices are running up-to-date software including anti-malware software and compliance monitoring tools that validate endpoint encryption. • A local firewall is installed. • The Oracle Cloud Network Access (OCNA) VPN is configured to time out after 24 hours of connectivity.

		• Devices that support Windows and Mac operating systems are configured to lock automatically after 15 minutes of inactivity. • Oracle managed endpoints are tracked centrally in inventory systems. • Business-critical software installed on the endpoints is checked regularly, and software update alerts are issued to users to meet compliance requirements according to Oracle policies and standards. When an endpoint is out of compliance, an email notification is sent to the user and management to make the necessary updates. The Security Information and Event Monitoring (SIEM) tool is configured to review the telemetry against predefined rules including detections related to data loss prevention. Security events detected generate an automated ticket with a severity rating and are tracked to resolution by the OCI Detection and Response Team (DART).
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?	Endpoint devices utilized to manage the Oracle Hospitality OPERA Cloud application and its related source code employ Oracle's secure desktop, and mobile device management software which has 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: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle confidential information, and Oracle hardware assets placed in their custody In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
		Third party endpoints are not allowed in Oracle Hospitality OPERA 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>