ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) v4.0 for Oracle Advertising Data Management Platform (DMP) First Party Data (1p) and BlueKai Third Party Data (3p)

September 06 2022 | Version 4

PURPOSE STATEMENT

Developed by the Cloud Security Alliance, the Cloud Assessment Initiative Questionnaire (CAIQ) provides a standard template for cloud services providers to accurately describe their security practices. The CAIQ format is largely based on the Cloud Controls Matrix (CCM), which lists a set of fundamental cloud controls. The use of CAIQs 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 services 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

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

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

ORACLE CLOUD SERVICES IN SCOPE

This document applies to the following Oracle Advertising application delivered as a Software as a Service (SaaS) deployed at Oracle data centers:

- Oracle Data Services Digital Audience Services (BlueKai): https://www.oracle.com/assets/odc-digital-audiences-sd-4813206.pdf
- Oracle Marketing Cloud Data Management Platform (DMP) Service Description: https://www.oracle.com/assets/omc-dmp-service-descriptions-4308340.pdf

TABLE OF CONTENTS

CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ)

v4.0

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Audit & Assurance	**A&A-01.1**	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle internal audit policies, procedures, and standards are established and documented by Oracle Corporate functions including Business Assessment & Audit, Risk, Standards, Security & Compliance, in partnership with their Oracle Line of Business counterparts.
	A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations. Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their A&A-01.1 evidence from Oracle Corporate may update that evidence annually. Audit reports about Oracle Cloud Services are periodically published by Oracle's third-party auditors. Reports may not be available for all services or all audit types or at all times. Customer may request access to available audit reports for a particular Oracle Cloud service via Sales.
	A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Oracle maintains teams of specialized security professionals for the purpose of assessing the security strength of the company's infrastructure, products, and services. Oracle requires that external facing systems and cloud services undergo penetration testing performed by independent security teams. Global Information Security's Penetration Testing Team performs penetration tests and provides oversight to all lines of business in instances where other internal security teams or an approved third-party perform penetration testing activities. This oversight is designed to drive quality, accuracy, and consistency of penetration testing activities and their associated methodology. Oracle has formal penetration testing requirements which include test scope and environment definition, approved tools, findings classification, categories of

			exploits to attempt via automation and manual steps, and procedures for reporting results. These teams perform various levels of complementary security testing: **Operational security scanning** is performed as part of the normal systems administration of all Oracle's systems and services. This kind of assessment largely leverages tools including commercial scanning tools as well as Oracle's own products (such as Oracle Enterprise Manager). The purpose of operational security scanning is primarily to detect unauthorized and insecure security configurations. **Penetration testing** is also routinely performed to check that systems have been set up in accordance with Oracle's corporate standards and that these systems can withstand their operational threat environment and resist hostile scans that permeate the Internet. Penetration testing can take two forms: **Passive-penetration testing** is performed using commercial scanning tools and manual steps. It is usually performed via the Internet and usually with the minimum of insider knowledge. Passive testing is used to confirm the presence of known types of vulnerabilities with sufficient confidence and accuracy to create a test case that can then be used by development or cloud operations to validate the presence of the reported issue. During passive-penetration testing, no exploitation is performed on production environments, other than that minimally required to confirm the issue. For example, a SQL injection will not be exploited to exfiltrate data. **Active-penetration testing** is more intrusive than passive-penetration testing and allows for the exploitation of discovered vulnerabilities. It is also broader in scope than passive penetration testing as the security teams are typically allowed to pivot from one system to another. Obviously, active penetration testing is closely controlled so as to avoid unintentional impacts on production systems. All penetration test results and reports are reviewed by Oracle's Corporate Security teams to validate that an independent and thorough test has been performed. Before an Oracle Line of Business is allowed to bring a new system or cloud service into production, Oracle requires that the remediation of significant penetration test findings be completed. Information about penetration tests of Oracle's corporate systems and cloud services is Oracle Confidential and is not shared externally.
	A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Independent audit and assurance assessments are individually approved based on risk plans reviewed under Oracle risk policies and standards.

			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, such as employees and contractors. These policies are aligned with the ISO/IEC 27002:2013 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2013 standards and guide all areas of security within Oracle. Some Oracle products and services are certified per specific industry and government standards such as ISO/IEC 27001:2013, AICPA SSAE Number 18 (SOC), Payment Card Industry Data Security Standards (PCI DSS) and other standards.
	A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Oracle Legal closely monitors the global regulatory landscape to identify legislation applicable to Oracle, including regional and local teams monitoring changes in relevant jurisdictions. Oracle Legal partners with Corporate Security and other organizations to manage Oracle's compliance to regulatory obligations across all lines of business. For more information, see https://www.oracle.com/legal/. 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
	A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Oracle audit management processes within Oracle Lines of Business align to recognized industry associations and standards and common bodies of practice including ISO and NIST. NIST risk framework guidance is used by Corporate Security. Oracle corporate security governance is described here: https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html For Cloud see: https://www.oracle.com/corporate/contracts/cloud-services/service-descriptions.html
	A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Audit reports about Oracle Cloud Services are periodically published by Oracle's third- party auditors. Reports may not be available for all services or all audit types or at all times. Customer may request access to available audit reports for a particular Oracle Cloud service via Sales.

	A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Audit reports about Oracle Cloud Services are periodically published by Oracle's third- party auditors. Reports may not be available for all services or all audit types or at all times. Customer may request access to available audit reports for a particular Oracle Cloud service via Sales.
Additional Comments for Control Domain above:			
Application & Interface Security	**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?	Oracle has established corporate security practices around software development, supplemented by guidelines and standards for implementation that are appropriate to the unique differences between Oracles lines of business and product suites. For more information, please refer to: https://www.oracle.com/corporate/security-practices/assurance/ See also: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html and: https://www.oracle.com/corporate/security-practices/global-customer-support/
	AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their AIS-01.1 evidence from Oracle Corporate may update that evidence annually.
	AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Oracle's enterprise architecture organization defines and maintains guidance documentation and secured configurations for use within Oracle's corporate systems and in Oracle Cloud. This guidance applies across layers of Oracle environments, including hardware, storage, operating systems, databases, middleware, and applications.
	AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	The Oracle Risk Assessment Management Plan (RAMP) is focused on providing visibility into high-risk security issues within Oracle Lines of Business (LoBs). RAMP goals are: - To align risk assessment between the LoB Security and GIS teams. GIS and LoBs agree on the key risks: ▪ Use as the basis for planned security work ▪ Track security maturity and readiness over time ▪ Track the status of the reported remediation plans in quarterly Oracle Security Oversight Committee (OSOC) updates - Maintain relationships and regularly engage with LoB stakeholders to obtain visibility into Information Security risks - Use common risk language

			- Produce a risk reporting mechanism - Drive action and ownership of risk and assurance activities - Risk assessments are ongoing - Unified view of risk to improve decision making capabilities Security Readiness Assessments are included to assess security capabilities within LOBs using industry standard rating criteria. Security Readiness Assessments are reflected in a Readiness Scorecard for each LoB using the NIST categories of Identify, Protect, Detect, Respond, and Recover. Security readiness is tracked over time OSOC is a committee comprising senior management representatives from key organizations within Oracle. It provides strategic direction on security matters for Oracle and is a forum for senior management to discuss and consider security concerns from their respective organizations and the company as a whole. OSOC considers, reviews, and approves security strategy, initiatives, and policies at its biannual meetings
	AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Functional security testing is typically executed by regular product QA teams as part of normal product testing cycle. During this testing, QA engineers verify conformance of implemented security features to what had been previously agreed upon in the functional specifications during the architectural and checklist reviews process. Please refer to AIS-01.1 and AA-02.1 and references for a description of the Oracle Software Security Assurance process and the complementary Oracle Corporate Solution Security Assurance Process.
	AIS-05.1	Do the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Security assurance analysis and testing verify security qualities of Oracle products against various types of attacks. There are two broad categories of tests employed for testing Oracle products: static and dynamic analysis, which are further described in the sections below. These tests fit differently in the product development lifecycle and tend to find different categories of issues, so they are used together by Oracle product teams. Please refer to https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
	AIS-05.2	Is testing automated when applicable and possible?	Security testing of Oracle code includes both functional and non-functional activities for verification of product features and quality. Although these types of tests often target overlapping product features, they have orthogonal goals

			and are carried out by different teams. Functional and non-functional security tests complement each other to provide security coverage of Oracle products. 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 a variety of internally developed tools, to catch problems while code is being written. Products developed in programming languages and platforms (J2EE, .NET) are scanned to identify possible security issues. Please reference https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
	AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	The Oracle corporate security architect helps set internal information-security technical direction and guides Oracle's IT departments and lines of business towards deploying information security and identity management solutions that advance Oracle's Information Security goals. An example program for managing the security of Oracle's architecture is the Corporate Security Solution Assurance Process (CSSAP). CSSAP is a security review process developed by Corporate Security Architecture, Global Information Security, Global Product Security, Oracle Global IT, and Oracle's IT organizations to provide comprehensive information-security management review. CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle, so that projects are aligned with: • 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
	AIS-06.2	Is the deployment and integration of application code automated where possible?	The Oracle Advertising DevOps model employs the Continuous Integration/Continuous Deployment tool within the CSSAP-approved GitLab Enterprise Edition application.
	AIS-07.1	Are application security vulnerabilities remediated following defined processes?	In order to provide the best security posture to all Oracle customers, Oracle fixes significant security vulnerabilities based on the likely risk they posed to customers. Please refer to:

			https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html
	AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Remediation of security vulnerabilities within Oracle Advertising is automated when and where possible. The objective is to remediate security vulnerabilities based on the likely risk they pose to customers. As a result, the most severe vulnerabilities are prioritized to be remediated first. Security vulnerabilities are remediated throughout the DevOps model: a) In the development phase, the introduction of vulnerabilities is avoided through Static Application Security Testing (SAST). manual code reviews, and other mechanisms (for more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html). b) Our operational practices require periodic vulnerability scanning, with the automatic application of security patches when possible. Oracle Advertising uses the Common Vulnerability Scoring System (CVSS) to determine the relative severity of security vulnerabilities in the production environment.
Additional Comments for Control Domain above:			
Business Continuity Management & Operational Resilience	**BCR-01.1**	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	The Risk Management Resiliency Program (RMRP) objective is to establish a business- resiliency framework to help provide an efficient response to business interruption events affecting Oracle's operations. The RMRP approach is comprised of several sub-programs: Information Technology Disaster Recovery, initial emergency response to unplanned and emergent events, crisis management of serious incidents, and business-continuity management. The goal of the program is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored. Each of these sub-programs is a uniquely diverse discipline. However, by consolidating emergency response, crisis management, business continuity, and disaster recovery, they can become a robust collaborative and communicative system. Oracle's RMRP is designed to engage multiple aspects of emergency management and business continuity from the onset of an event and to

			leverage them based on the needs of the situation. The RMRP is implemented and managed locally, regionally, and globally. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
	BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations.
	BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Such criteria are based upon risk standards including NIST. Corporate business continuity policy, standards, and practices are governed by the RMRP Program Management Office (PMO) and are generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance. For more information about the centralized RMRP program and the risk management activities within geographies and lines of business, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/
	BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Lines of business are required maintain operational and technical documents and make these available to relevant personnel. Assigned executives are accountable for the strategies and oversight to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite.
	BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Oracle data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build 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), and geopolitical considerations among other criteria.
	BCR-05.1	Is relevant documentation developed, identified, and acquired to support	Oracle 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

		business continuity and operational resilience plans?	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. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.
	BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Oracle Supplier Information and Physical Security Standards requires that suppliers maintain Disaster Recovery and Business Continuity Plan (BCP) plans which encompass the scope of products and services provided to Oracle. Suppliers are required to test these plans at least annually and notify Oracle of any potential or realized business interruptions which impact services to Oracle. For more information, see https://www.oracle.com/corporate/suppliers.html
	BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Functional business continuity planning is managed by the Risk Manager within each Line of Business (LoB). The critical LoBs are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. The RMRP program requires that identified LoBs: • Review and update a Risk Assessment • Write a Business Impact Analysis that includes identification of interdependent resources and internal customers, and the determination of a Recovery Time Objective and Recovery Point Objective • Define a business continuity strategy • Review and update a Business Continuity Plan • Train employees in Business Continuity Plan execution • Conduct an exercise to test the efficacy of the plan within the LoB, as well as participate in a cross-functional annual exercise assessing the capability of multiple organizations to collaborate effectively in response to events • Implement lessons learned for plan improvement • Obtain approval attestation from the LoB's Vice President Approver In addition, all LoBs are required to: • Identify relevant business interruption scenarios, including essential people, resources, facilities, and technology

			• Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information. • Obtain approval from the LoB's executive
	BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Oracle 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 (OCI) services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise. Oracle has identified certain critical internal infrastructure systems that are backed up and can be restored. For these systems, Oracle performs the following backups as applicable: • Database: Full and incremental backups are created on physical and/or electronic media. • Archive logs: Full and incremental backups are created on physical and/or electronic media In addition, source code repository backups are performed on recurring bases that vary by environment. Oracle implements additional strategies for certain critical internal systems, such as: • Application failover • Current copy of the production database at a secondary site using solutions such as Oracle Data Guard, which manages the two databases. Oracle Data Guard provides remote archiving, managed recovery, switchover, and failover features. • Redundant middle or application server tiers consisting of a set of servers to distribute application functionality across multiple host machines. • Physical backup media such as tape is periodically relocated to a secure offsite location

	BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	The Risk Management Resiliency Program (RMRP) objective is to establish a business- resiliency framework to help provide an efficient response to business-interruption events affecting Oracle's operations. The RMRP is implemented and managed locally, regionally, and globally. The RMRP program Is comprised of four Risk Management functions: Emergency Response, managed by Facilities Environment, Health and Safety 1.Program Crisis Management, managed by Global Physical Security 2.Business Continuity Management, managed by the corporate RMRP Program 3.Management Office Disaster Recovery, managed by Global Information Technology 4.Oracle's Information Technology organization conducts an annual DR exercise designed to assess our DR plans. Lessons learned from the exercise are implemented as deemed appropriate into standard operations and DR procedures as appropriate. These reports are Oracle Confidential.
	BCR-08.1	Is cloud data periodically backed up?	Oracle Global Physical Security uses a risk-based approach to physical and environmental security. The goal is to balance prevention, detection, protection, and response, while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained.
	BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Oracle data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build 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), and geopolitical considerations among other criteria. Oracle maintains a redundant network infrastructure, including DNS servers to route between primary and secondary sites, network devices, and load balancers. Oracle 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. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.
	BCR-08.3	Can backups be restored appropriately for resiliency?	Oracle's Information Technology organization conducts an annual DR exercise designed to assess our DR plans. Lessons learned from the exercise are implemented as deemed appropriate into standard operations and DR procedures as appropriate. Oracle Cloud Hosting and Delivery Policies describe the Oracle Cloud Service Continuity Policy, Oracle Cloud Services High Availability Strategy, Oracle Cloud Services Backup Strategy and Oracle Cloud Service Level Agreement: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Please refer to BCR-06.1
	BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Functional business continuity planning is managed by the Risk Manager within each Line of Business (LoB). The critical LoBs are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes.
	BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Oracle's corporate Disaster Recovery (DR) plan focuses on the resiliency of computing infrastructure supporting Oracle's internal operations. Oracle's production data centers are geographically separated and have component and power redundancy, with backup generators in place for availability of data center resources in case of an impacting event. Oracle's DR plan leverages this separation of data centers in conjunction with other recovery strategies to both protect against disruption and enable recovery of services. This plan is Oracle Confidential. Oracle's Information Technology organization conducts an annual DR exercise
	BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	Oracle Cloud Hosting and Delivery Policies describe the Oracle Cloud Service Continuity Policy, Oracle Cloud Services High Availability Strategy, Oracle Cloud Services Backup Strategy and Oracle Cloud Service Level Agreement: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html

	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 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. Data centers housing Oracle Cloud Infrastructure (OCI) services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.
Additional Comments for Control Domain above:			
Change Control & Configuration Management	**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's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations. Oversight during development is provided by line of business functions and the corporate oversight of: https://www.oracle.com/corporate/security-practices/assurance/ As well as architectural review oversight of the system: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html Whether the asset is internal or external.
	CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Oracle policies are reviewed at least annually. Procedures are reviewed when the systems or technologies covered by the procedure change.
	CCC-02.1	Is a defined quality change control, approval, and testing process (with	Please see CCC-01.1

		established baselines, testing, and release standards) followed?	
	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)?	The Oracle corporate security architect helps set internal information-security technical direction and guides Oracle's IT departments and lines of business towards deploying information security and identity management solutions that advance Oracle's Information Security goals. The corporate security architect works with Global Information Security and Global Product Security, and the development Security Leads to develop, communicate, and implement corporate security architecture roadmaps. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
	CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted	Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. 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. Oracle policy specifies the data (or fields) which must be maintained about these information systems in the approved system inventory. The required technical and business information fall in the following categories: • Hardware details such as manufacturer, model number and serial number of the equipment, system, or device • Physical location of the data center/facility and location within that building • Software details such as the operating system and applications and associated versions • Classification of information assets • Ownership information at the organizational and individual levels
	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?	The Oracle Advertising Data Management Platform (DMP) and BlueKai do not have tenants. Oracle Advertising DMP and BlueKai are delivered as Software as a Service. This means that provisions to limit changes that directly impact CSC-owned environments are not applicable to Oracle Advertising DMP and BlueKai.
	CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Oracle requires any changes to the Oracle Advertising production environment to go through the Change Management process described in CC-01.1. This process also requires:

			• Multi-factor authentication for administrative access • Management approval for administrative access • Logging and auditing of any access to bastion and production devices
	CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	The Oracle Advertising Configuration Management, Image, and Provisioning (CIP) standard for Operating Systems and Containers enforces standardized images.
	CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Oracle Advertising has implemented procedures to manage exceptions, including emergencies, in the change and configuration process. For example, emergency change notifications are communicated across the LOB prior to release, detailing what the change is, why it is needed, and what systems will be impacted. However, a root-cause analysis is conducted to identify opportunities for improvement and lessons learned. Please reference the following: Oracle Cloud Hosting and Delivery Policies Oracle Data Services Pillar Documentation
	CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	Please see CCC-01.1
	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?	The Oracle Advertising Configuration Management, Image, and Provisioning (CIP) standard for Operating Systems and Containers enforces standardized images. This is done on a system-by-system/application-by-application basis as requirements are varied depending upon the underling infrastructure. Oracle Advertising employs snapshots during the day, daily incremental, and a weekly full. Additionally, Oracle Advertising adheres to Oracle BC/DR policy. See also: https://www.oracle.com/corporate/security-practices/corporate/resilience-management/business-continuity.html https://www.oracle.com/corporate/security-practices/corporate/resilience-management/disaster-recovery.html
Additional Comments for Control Domain above:			

Cryptography, Encryption & Key Management	**CEK-01.1**	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	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.
	CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their CEK-01.1 evidence from Oracle Corporate may update that evidence annually. Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption when data is at rest (in storage) on laptops, devices, and removable media.
	CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Solutions for managing encryption keys 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
	CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	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.
	CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Oracle Advertising offers several standard encryption technologies and options to protect data while in transit or at rest. For network transmission, secured protocols (such as Secure Shell Protocol (SSH) File Transfer Protocol (SFTP) or Hypertext Transfer Protocol Secure (HTTPS) via (Transport Layer Security (TLS) 1.2) are used to protect customer data in transit over public networks. Customer data at rest are protected on encrypted volumes (AES-256). Data in transit within the Oracle production environment traverse an encrypted tunnel (e.g., HTTPS via TLS 1.2 or greater).

			Please reference https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.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?	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.
	CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Oracle's Cryptography Review Board oversees cryptography governance: 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
	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?	Oracle's Cryptography Review Board oversees cryptography governance: 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
	CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	Oracle Advertising manages the encryption keys associated with its services. These encryption keys/secrets are stored in a secure vault. As such, Oracle Advertising operations personnel have the ability to view data in an unencrypted state.
	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?	See response to CEK-02.1.
	CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their CEK-01.1 evidence from Oracle Corporate may update that evidence at will for re-approval.

	CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Oracle implements a wide variety of technical security controls designed to protect the confidentiality, integrity, and availability of corporate information assets. These controls are guided by industry standards and are deployed across the corporate infrastructure using a risk-based approach. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
	CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Oracle policy and standards require all keys be managed securely. See: https://www.oracle.com/security/cloud-security/key-management/
	CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Oracle Advertising leverages OCI KMS for key management rotation.
	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 Advertising has a formal process for cryptographic key management and use in the Oracle Advertising production environment. There are processes and procedures for determining key size, lifecycle management, storage, access control, distribution, and logging, for example. Note that customers are solely responsible for determining legal and regulatory requirements and assessing the suitability of Oracle Advertising Product/Service in this context.
	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's Cryptography Review Board oversees cryptography governance: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html For Oracle HSMs, please see: https://docs.oracle.com/en/database/oracle/key-vault/18.1/okvhm/getting-started-hsm.html#GUID-DADA7E20-82E2-40C9-A63A-4A159EBD5F09
	CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include	See response to CEK-02.1.

		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?	See response to CEK-02.1.
	CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	See response to CEK-02.1.
	CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	See response to CEK-02.1.
	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 Advertising has 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). Additionally, data transferred within the Oracle Advertising production environment is also encrypted (e.g., currently TLS 1.2 and 1.3). Note that customers are solely responsible for determining legal and regulatory requirements and assessing the suitability of Oracle Advertising Product/Service in this context.
	CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Such criteria are based upon risk standards including NIST. Corporate business continuity policy, standards, and practices are governed by the Oracle RMRP Program Management Office (PMO) and are generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance.

	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 oversees cryptography governance: 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
Additional Comments for Control Domain above:			
Data Center Security	**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 Corporation takes guidance from NIST 800-88 for such policies and related procedures and/or Oracle Line of Business standards as appropriate. Oracle uses physical destruction and logical data erasure processes so that data doesn't persist in decommissioned hardware. Storage Media Destruction Oracle Asset Management requirements explicitly prohibit the removal of storage media that contains customer data from the data hall in which it is stored. Each data hall in a data center contains a secure media disposal bin. When a hard disk or other storage media is faulty or removed from production for disposal, it's placed in this secure bin for storage until it's degaussed and shredded. Data Erasure When a customer releases a VM instance, an API call starts the workflow to delete the instance. When a new bare metal compute instance is added to the service or is released by a customer or service, the hardware goes through the provisioning workflow before it's released to inventory for reassignment. This automated workflow discovers the physical media connected to the host. Then, the workflow initiates secure erasure by running the applicable erasure command for the media type. Hosts intended for customer use also have a network-attached disk that's used to cache the customer's storage volume. This disk is erased using the AT Attachment (ATA) security erase command. When the erasure process is complete, the workflow starts a process to flash the BIOS, update drivers, and return the hardware to a known good state. The workflow also tests the hardware for faults. If the workflow fails or detects a fault, it flags the host for further investigation. When a customer terminates a block storage volume, the key is irrevocably deleted, which renders the data permanently inaccessible. https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf

			For more information, please refer to the product documentation and security guides for the Oracle products and services.
	DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Please see DCS-01.1
	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 are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their DCS-01.1 evidence from Oracle Corporate may update that evidence annually.
	DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. Oracle's Information Systems 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. This inventory must be managed within an inventory system approved by the Oracle Security Oversight Committee (OSOC).
	DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	The Oracle Advertising Data Management Platform (DMP) and BlueKai do not have tenants. Oracle Advertising DMP and BlueKai are delivered as Software as a Service. This means that provisions to limit changes that directly impact CSC-owned environments is not applicable to Oracle Advertising DMP and BlueKai.
	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?	The Oracle Advertising Data Management Platform (DMP) and BlueKai do not have tenants. Oracle Advertising DMP and BlueKai are delivered as Software as a Service. This means that provisions to limit changes that directly impact CSC-owned environments is not applicable to Oracle Advertising DMP and BlueKai. The transfer of hardware, software, or data is not approved for this use case, as Oracle Advertising works within a cloud environment. The relocation or transfer of hardware, software, or data to an offsite premises is not a standard practice and would only be on a case-by-case basis with appropriate customer and Oracle authorization.
	DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented,	Oracle Corporate Physical Security policies are reviewed annually and updated as required: https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html

		approved, communicated, enforced, and maintained?	https://www.oracle.com/a/ocom/docs/corporate/citizenship/oracle-environment-health-safety.pdf
	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 are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their DCS-01.1 evidence from Oracle Corporate may update that evidence at will for re-approval. Oracle Global Physical Security uses a risk-based approach to physical and environmental security. The goal is to balance prevention, detection, protection, and response, while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained.
	DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Media is governed by a number of Oracle policies specifying strict requirements for encryption, labeling, sanitization, transportation and destruction of various types of media. The Oracle Media Sanitization and Disposal Policy establishes guidelines for secure erasure of information from all types of electronic media, where current usage of the media is finished. The policy is intended to protect Oracle resources and information from security threats associated with the retrieval and recovery of information on electronic media.
	DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Global Information Security is responsible for security oversight, compliance and enforcement, and conducting information-security assessments leading the development of information security policy and strategy, as well as training and awareness at the corporate level. Policies are reviewed at least annually. Procedures are reviewed when the systems or technologies covered by the procedure changes.
	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 provides guidelines for all Oracle personnel and business partners regarding information classification schemes and minimum handling requirements associated with those classifications. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
	DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Oracle has formal 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. The Oracle Information Systems Inventory Policy requires an accurate inventory of all information systems and devices holding critical and highly

			critical information assets throughout their lifecycle through an Oracle Security Oversight Committee (OSOC)-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'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. Electronic storage media include laptops, hard drives, storage devices, and removable media such as tape.
	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. The goal is to balance prevention, detection, protection, and response, while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained.
	DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Oracle Cloud data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build 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), and geopolitical considerations among other criteria. 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. 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. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.
	DCS-08.1	Is equipment identification used as a method for connection authentication?	Oracle policy requires all assets containing customer information be owned, identified, and tracked. Execution is the responsibility of the accountable Oracle executives assigned to oversee the Oracle products and services. Oracle Cloud data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build 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), and geopolitical considerations among other criteria. 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. 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. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.
	DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Oracle maintains high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business around the world. These apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Oracle requires its employees to receive training in ethics and business conduct every two years.
	DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Retention of such records is necessary for Oracle Cloud data centers to align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards. See also DCS-10.1
	DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	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. 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. Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations.

			Oracle use 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. The access logs are kept for a minimum of six months. The retention period for CCTV monitoring and recording ranges from 30-90 days minimum, depending on the facility's functions and risk level.
	DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Oracle maintains high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business around the world. These apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Oracle requires its employees to receive training in ethics and business conduct every two years. 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. 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. Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations. Oracle use 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. The access logs are kept for a minimum of six months. The retention period for CCTV monitoring and recording ranges from 30-90 days minimum, depending on the facility's functions and risk level.

	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?	Oracle Cloud data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build 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), and geopolitical considerations among other criteria. 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. 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. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.
	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?	Oracle Cloud data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build 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), and geopolitical considerations among other criteria. 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. 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. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.
	DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Oracle Cloud data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build 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), and geopolitical considerations among other criteria.

			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. 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. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.
	DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Oracle Global Physical Security uses a risk-based approach to physical and environmental security. The goal is to balance prevention, detection, protection, and response, while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained. Oracle has formal 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. The Oracle Information Systems Inventory Policy requires an accurate inventory of all information systems and devices holding critical and highly critical information assets throughout their lifecycle through an Oracle Security Oversight Committee (OSOC)-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'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. Electronic storage media include laptops, hard drives, storage devices, and removable media such as tape.
Additional Comments for Control Domain above:			
Data Security & Privacy Lifecycle	**DSP-01.1**	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data	Oracle's mandatory training instructs employees about the company's Information Protection Policy. This training also tests employee understanding of information asset classifications and handling requirements. Employees must complete this training when joining Oracle and must periodically repeat

		throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	it thereafter. Reports enable managers to track course completion for their organizations.
	DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their DSP-01.1 evidence from Oracle Corporate may update that evidence annually. Oracle's external privacy policies are reviewed and updated at least annually.
	DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Oracle has formal requirements for managing data retention. These operational policies define requirements per data type and category, including examples of records in various Oracle departments. Oracle's Media Sanitation and Disposal Policy defines requirements for the removal of information from electronic storage media (sanitization), and disposal of information, which is no longer required, either in hard copy form or on electronic storage media, such that the information is protected from security threats associated with retrieval and reconstruction of confidential data. This policy applies to all "hard copy" (paper) and electronic media. Oracle's Media Sanitation and Disposal Standards support compliance to this policy. Oracle Cloud Hosting and Deliveries Policy describes handling of customer data at termination of services: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Oracle requires Oracle Advertising to document and maintain data inventories and data flows. This documentation is for internal use only and is shared with internal audit teams.
	DSP-04.1	Is data classified according to type and sensitivity levels?	Oracle categorizes confidential information into three classes—Internal, Restricted, and Highly Restricted—with each classification requiring corresponding levels of security controls, such as encryption requirements for data classified as Restricted or Highly Restricted.
	DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	See response to DSP-03.1 and DSP-04.1.

	DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their DSP-01.1 evidence from Oracle Corporate may update that evidence at will for re-approval.
	DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Oracle has formal requirements for managing data retention. These operational policies define requirements per data type and category, including examples of records in various Oracle departments. Oracle's mandatory training instructs employees about the company's Information Protection Policy. This training also tests employee understanding of information asset classifications and handling requirements. Employees must complete this training when joining Oracle and must periodically repeat it thereafter. Reports enable managers to track course completion for their organizations.
	DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their DSP-01.1 evidence from Oracle Corporate may update that evidence at will for re-approval.
	DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Oracle's Corporate Security Program is designed to protect the confidentiality, integrity, and availability of both Oracle and customer data, such as: • The mission-critical systems that customers rely upon for cloud, technical support and other services • Oracle source code and other sensitive data against theft and malicious alteration • Personal and other sensitive information that Oracle collects in the course of its business, including customer, partner, supplier and employee data residing in Oracle's internal IT systems https://www.oracle.com/corporate/security-practices/corporate/objectives.html https://www.oracle.com/corporate/security-practices/
	DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Oracle employees are required to complete an Ethics training and Information Protection Awareness training upon hiring and on a reoccurring basis throughout the term of their employment. The Information Protection Awareness course instructs employees on their obligations under the various central Oracle privacy and security policies (such as the Information Protection Policy, Acceptable Use Policy, Security Breach Disclosure Policy and the Services Privacy Policy). The course also trains employees on data privacy principles as well as data handling practices that may apply to their jobs at

			Oracle and are required by company policy, including those related to notice, consent, use, access, integrity, sharing, retention, security and disposal of data. All Oracle employees and contractors who may have access to Customer data are subject to a written confidentiality agreement. Prior to performing services for Oracle and prior to accessing any Oracle system or resource, service providers are required to sign a Services Provider Agreement, a Network Access Agreement, and a work order defining the services to be provided. Oracle employees are required to maintain the confidentiality of Customer data. Employees are required to sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. All new products/features are subject to detailed privacy reviews with the Corporate Security Solution Assurance Process (CSSAP) prior to any development work or release to the marketplace. Oracle Legal teams perform Data Privacy Impact Assessments. Oracle Advertising performs impact assessments for all new products and feature enhancements we wish to bring to market.
	DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	See response to CCC-07.1. For more information see https://www.oracle.com/legal/privacy/advertising-privacy-policy.html
	DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations, and industry best practices?	Oracle Legal teams perform DPIAs. Oracle Advertising performs impact assessments for all new products and feature enhancements we wish to bring 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)?	Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over internal and external networks. Customer configuration information (e.g., connection strings, application settings) supplied through the management portal is protected while in transit and at rest.

	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 complies with all applicable laws and regulations and makes available to customers and consumers mechanisms to exercise applicable privacy rights. For more information see https://www-sites.oracle.com/legal/privacy/
	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)?	Oracle Advertising has implemented a robust oversight program designed to ensure lawful processing of personal information across our products and services.
	DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Oracle suppliers and partners are required to protect the data and assets Oracle entrusts to them. See sections 4, 5, and 6 of the Data Processing Agreement here: https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
	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?	Any terms and conditions related to Oracle's performance of the applicable services are specified in the customer order for services documentation.
	DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	For Oracle Advertising, our standards and procedures prohibit production data from being stored and processed in non-production environments.
	DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Information assets are classified in accordance with the Oracle Information Protection Policy. This policy identifies customer data as among Oracle's top two categories of confidential information, that have associated limits on access, distribution, and handling. Oracle will keep the information confidential in accordance with the terms of the Ordering Document and Statement of Work. Customers are solely responsible for determining the appropriate classification and levels for control of their data.

			See also https://www.oracle.com/legal/privacy/advertising-privacy-policy.html#8
	DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Please reference the following for more information about Oracle processes, procedures, and technical measures for protecting customer sensitive data: Data Protection | Oracle Technical Controls for Data Protection | Oracle Information and Assets Classification | Oracle
	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?	Please refer to Oracle Advertising's Privacy Shield Policy for details about response to these types of requests and Transparency reports: https://www.oracle.com/fr/a/ocom/docs/corporate/privacy-shield-statement-071720.pdf
	DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. 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. If Oracle determines that a confirmed security incident involving Personal 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 is Oracle Confidential and is not externally shared. Incident history is also Oracle Confidential and is not shared externally.
	DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including	See response to CEK-19.1

		locales where data is processed or backed up?	
Additional Comments for Control Domain above:			
Governance, Risk & Compliance	**GRC-01.1**	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter.
	GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations.
	GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Oracle's enterprise architecture organization defines and maintains guidance documentation and secured configurations for use within Oracle's corporate systems and in Oracle Cloud. This guidance applies across layers of Oracle environments, including hardware, storage, operating systems, databases, middleware, and Applications. The Chief Corporate Architect, who reports directly to the Executive Chairman and Chief Technology Officer (CTO), is one of the directors of the Oracle Security Oversight Committee (OSOC). The Chief Corporate Architect manages the functional departments directly responsible for identifying and implementing security controls at Oracle. These departments drive the corporate security program, define corporate security policies, assess compliance, and provide operational oversight for the multidimensional aspects of Oracle's security policies and practices: Global Information Security Global Physical Security

			Global Product Security Corporate Security Architecture
	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 required. Oracle Lines of Business that gain approval of their GRC-01.1 evidence from Oracle Corporate may update that evidence at will for re-approval.
	GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Oracle's corporate security practices are documented at https://www.oracle.com/corporate/security-practices/corporate/ Global Information Security is responsible for security oversight, compliance and enforcement, and conducting information-security assessments leading the development of information security policy and strategy, as well as training and awareness at the corporate level. This organization serves as the primary contact for security incident response, providing overall direction for incident prevention, identification, investigation, and resolution. Corporate governance teams and programs are described at https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html
	GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	The Chief Corporate Architect, who reports directly to the Executive Chairman and Chief Technology Officer (CTO), is one of the directors of the Oracle Security Oversight Committee (OSOC). Oracle's OSOC provides ongoing management and review of information security at Oracle.
	GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Oracle places a strong emphasis on personnel security. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions. Oracle promotes security awareness and educates employees through regular newsletters and ad hoc security awareness campaigns. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy. Global Information Security manages the Information Security Manager (ISM) Program.

			Information Security Managers serve as security advocates within their respective lines of business to increase awareness of and compliance with Oracle's security policies, processes, standards, and initiatives. Programs within Global Information Security are dedicated to preserving the confidentiality, integrity, and availability of Oracle information assets and the information assets entrusted to Oracle, including a focus on: • Defining global corporate technical standards to enable security, privacy, and compliance • Contributing to industry standards such as those issued by the International • Organization for Standardization (ISO) and United States National Institute of • Standards and Technology (NIST) • Assisting lines of business security organizations with fostering a culture of security across regions and functional areas.
	GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Please see GRC-06.1
	GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Oracle has formal requirements for its suppliers and partners to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle confidential information, and Oracle hardware assets placed in their custody For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
Additional Comments for Control Domain above:			
Human Resource Security	**HRS-01.1**	Are background verification policies and procedures of all new employees (including but not limited to remote	See HRS-01.3

		employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	
	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?	See HRS-01.3
	HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Th **Oracle Recruiting Privacy Policy** (**Privacy Policy**) describes the privacy and security practices that Oracle Corporation, its subsidiaries and affiliates (**Oracle, we or us**) employ when collecting, using and handling (**processing**) personal information about you in connection with our online and offline recruitment activities. It also explains the choices you have in relation to these processing activities. https://www.oracle.com/legal/privacy/recruiting-privacy-policy.html **Personal information** means all information that relates to an identified individual or to an identifiable individual. For example, your name, address, email address, educational and employment background, CV and job qualifications. Personal information is also referred to as **information about you**. This Privacy Policy was last changed on January 19, 2021. However, the Privacy Policy may change over time to comply with legal requirements or to meet our changing business needs. The most up-to-date version of the Privacy Policy can be found on this website.
	HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.
	HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their HRS-01.1 evidence from Oracle Corporate may update that evidence at will for re-approval.

		owned or managed assets reviewed and updated at least annually?	Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.
	HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy.
	HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their HRS-01.1 evidence from Oracle Corporate may update that evidence at will for re-approval. Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.
	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's Corporate Information Security Policy Review Process defines how Oracle Global Information Security (GIS) leads ongoing cross-departmental review of information security policies, so that these policies continue to be relevant and aligned with Oracle's technical, legal, governmental, and business requirements.
	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?	See HRS-01.3 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. Oracle's physical security standards and policies have been developed to align with various physical security industry initiatives, including the International Organization for Standardization (ISO), United States Customs Trade Partnership Against Terrorism (CTPAT), American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 18, and the Payment Card Industry Security Standards Council.

	HRS-05.1	Are return procedures of organizationally owned assets by terminated employees established and documented?	Oracle policy requires the use of antivirus intrusion protection and firewall software on laptops 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 process Oracle or customer information must be encrypted using approved software. Reports enable lines of business management to verify deployment of laptop encryption for their organization. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.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 with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
	HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	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. Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
	HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
	HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Oracle's information-asset classification determines corporate data-security requirements for Oracle-managed systems. Oracle policies and standards provide global guidance for appropriate controls designed to protect the confidentiality, integrity, and availability of corporate data in accordance with the data classification. Required mechanisms are designed to be commensurate with the nature of the corporate data being protected. For example, security requirements are greater for data that is sensitive or valuable, such as cloud systems, source code and employment records. 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. In addition, Oracle has formal programs to guide development of software and hardware solutions. Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products. Oracle's formal programs also focus on security requirements and operations for Oracle cloud services.
	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-11.1
	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 ad hoc security awareness campaigns. Security reviews, assessments, and audits are conducted periodically to confirm compliance with Oracle information-security policies, procedures, and practices. Employees who fail to comply with these policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy. See also: 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?	Please see HRS-11.1
Additional Comments for Control Domain above:			
Identity & Access Management	**IAM-01.1**	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
	IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their IAM-01.1 evidence from Oracle Corporate may update that evidence annually. Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
	IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Oracle policy requires strong passwords and appropriate password management processes. Implementation is the responsibility of the accountable Oracle executives assigned to oversee the products and services.

	IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their IAM-01.1 evidence from Oracle Corporate may update that evidence at will for re-approval.
	IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Oracle Corporate Security policy requires the secure management of access, which includes logging, protection of logging, and log review of system identity information. See: https://www.oracle.com/corporate/security-practices/corporate/access-control.html https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html Oracle Line of Business standards provide appropriate specific guidance. Implementation is the responsibility of the accountable Oracle executives assigned to oversee the products and services. https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Oracle enforces well-defined roles, allowing for segregation of duties among operations staff. Operations are organized into functional groups, where each function is performed by separate groups of employees. Examples of functional groups include database administrators, system administrators, and network engineers. Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval.
	IAM-05.1	Is the least privilege principle employed when implementing information system access?	Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are 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?
	IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. Metrics are considered Oracle Confidential.

	IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
	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?	Oracle Advertising employee access management covers on-boarding, internal/external transitions, and terminations. For transitions, a review is conducted to remove unnecessary access. OA performs an audit of employee access on a quarterly cadence. All terminations are processed automatically through the Oracle Human Resources Management System (HRMS). After a termination is processed, automated notifications are issued for terminations (regardless of type) based on the effective date of the termination.
	IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Oracle has implemented and maintained strong network controls to address the protection and control of customer data during its transmission from one end system to another. The Oracle Use of Network Services Policy states that computers, servers, and other data devices connected to the Oracle network must comply with well-established standards for security, configuration, and access method.
	IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Oracle has formal access controls requirements. Access control refers to the policies, procedures, and tools that govern access to and use of resources. Examples of resources include a physical server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol. • Least privilege is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties. • Default-deny is a network-oriented approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination. 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?	The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. This policy does not apply to publicly accessible, internet-facing Oracle systems or end users. Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval.
	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?	Oracle enforces strong password policies for the Oracle network, operating system, and database 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
	IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	The 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?
	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?	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? For more information about logical access control, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html

	IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.
	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?	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?
	IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Network devices must be registered and inventoried in an Oracle-approved information system per Oracle Information Systems Asset Inventory Policy. This policy requires the accurate inventory and documented ownership of all information systems processing information assets throughout their lifecycle.
	IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Please refer to: https://www.oracle.com/corporate/security-practices/corporate/access-control.html
	IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	For administration of network security and network-management devices, Oracle requires IT personnel to use secure protocols with authentication, authorization, and strong encryption. Network devices must be located in an environment protected with physical access controls and other physical security measure standards defined by Global Physical Security (GPS). Communications to and from the Oracle corporate network must pass through network security devices at the border of Oracle's internal corporate network. Remote connections to the Oracle corporate network must exclusively use virtual private networks (VPN) that have been approved via the Corporate Security Solution Assurance Process (CSSAP). Access to the Oracle corporate network by suppliers and third parties is subject to limitations and prior approval per Oracle's Third-Party Network

			Access Policy. See: https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
Additional Comments for Control Domain above:			
Interoperability & Portability	**IPY-01.1**	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Documentation about available APIs for Oracle Cloud is at https://docs.oracle.com/en/cloud/index.html
	IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	See response to CEK-19.1. Additionally, Oracle Advertising has an established process to review all new products, product features, or other new use cases that involve the use of data in new ways (Innovation Team). We assess these in advance to rule out any privacy issues, affirm data usage rights, and ensure the proposed use case aligns with Oracle's business objectives and risk profile.
	IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Oracle's Source Code Protection policy and the Oracle Software Security Assurance policies Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products and services, including the Oracle Advertising Services. The OSSA program is described at https://www.oracle.com/corporate/security-practices/assurance/ • Oracle's Source Code Protection policies maintain strong security controls over its source code. Oracle's source-code protection policies provide limits on access to source code (enforcement of the need to know), requirements for independent code review, and periodic auditing of the company's source-code repositories. Oracle Source Code Protection is described at https://www.oracle.com/corporate/security-practices/corporate/supply-chain/source-code-protection.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 Cloud Services Hosting and Delivery policies can be found here: https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf
	IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes. These policies and procedures are updated at least annually.
	IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	For more information on using the DMP APIs, see https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Developers/api_getting_started.html
	IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	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. CRB's responsibilities include: • Creating and maintaining standards for cryptography algorithms, protocols, and their parameters • Providing approved standards in multiple formats, for readability and automation • Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle • Providing practical guidance on using cryptography • Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography For more information, please see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html
	IPY-04.1	Do agreements include provisions specifying CSC data access upon	Any terms and conditions related to Oracle's performance of the applicable services shall be specified in the customer order for services documentation.

		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	
Additional Comments for Control Domain above:			
Infrastructure & Virtualization Services	**IVS-01.1**	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle Cloud largely relies on Oracle products that are subject to Oracle Security Assurance activities. Oracle-developed code used solely in the cloud, that is, code that is not used in on-premises product distributions, is also subject to Oracle Software Security Assurance.
	IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation and executive approvals for critical business operations. Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their IVS-01.1 evidence from Oracle Corporate may update that evidence annually.
	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?	System resources are monitored and reviewed to ensure adequate capacity is maintained. In many cases, our applications are built with the ability to auto scale to meet usage requirements to ensure that application performance is not degraded.
	IVS-03.1	Are communications between environments monitored?	Virtual Cloud Network (VCN) and Virtual Private Cloud (VPC) traffic flow logs are monitored by the Oracle Advertising Security Operations team. Security-related logs entries capture the following information: • Date

			• Time • Time zone • User account name • Source IP address information, software or configuration changed, identity of operation • Original value (when applicable) • New value (other than for changes such as a password change) (when applicable), and • Location of change (host name, file name, or table name)
	IVS-03.2	Are communications between environments encrypted?	Communications to and from the Oracle corporate network must pass through network-security devices at the network boundary. Access to the Oracle corporate network by third parties is subject to prior approval. Remote connections to the Oracle corporate network must exclusively use approved virtual private network (VPN) solutions. To learn more about Oracle's network management practices, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
	IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Communications between environments must be authenticated and authorized. Communications justification is established during the Corporate Security Solutions Assurance Process (CSSAP) review.
	IVS-03.4	Are network configurations reviewed at least annually?	Network configurations are reviewed at least annually.
	IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	CSSAP is a security review process developed by Corporate Security Architecture, Global Information Security, Global Product Security, Oracle Global IT, and Oracle's IT organizations to provide comprehensive information-security management review. CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle, so that projects are aligned with: • 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 See: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
	IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	The Oracle Server Security Policy requires servers (both physical and virtual) managed by Oracle or third parties on behalf of Oracle to be physically and logically secured in order to prevent unauthorized access to the servers and associated information assets.
	IVS-05.1	Are production and non-production environments separated?	See the Oracle product documentation and security guide for your Oracle product. In network security, DMZs are named after the military term "demilitarized zone." Network DMZs operate in a similar way, as a physical or logical buffer zone, providing an additional layer of security between two separate networks. DMZs ("demilitarized zones") are critical network areas providing separation between subnetworks inside Oracle corporate network and the internet. Network access control mechanisms are required to control communications in and around the DMZs so as to maintain adequate network segregation and prevent exposing sensitive IT resources. Oracle's Network Security Policy defines requirements for the use of network DMZs.
	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?	The Oracle Advertising Data Management Platform (DMP) and BlueKai do not have tenants. Oracle Advertising DMP and BlueKai are delivered as Software as a Service. This means that provisions to limit changes that directly impact CSC-owned environments is not applicable to Oracle Advertising DMP and BlueKai. However, each client is assigned a unique provider ID, and every record associated with that client is assigned to that provider ID; thereby, providing a logical separation of data. See also the response to CEK-19.1.
	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?	Oracle Advertising offers several standard encryption technologies and options to protect data while in transit or at rest. For network transmission, secured protocols (such as SFTP or HTTPS (TSL 1.2)) are used to protect customer data in transit over public networks. Customer data at rest are protected on encrypted volumes (AES-256). Data in transit within the Oracle

			production environment traverse an encrypted tunnel (e.g., HTTPS, TLS 1.2 or greater). 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. See also: Technical Controls for Data Protection | Oracle
	IVS-08.1	Are high-risk environments identified and documented?	Please see IVS-03.5
	IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Oracle employs intrusion-detection systems within the Oracle intranet to provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle utilizes a network-based monitoring approach to detect attacks on open firewall ports within Oracle's intranet. Events are analyzed using signature detection, which is a pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to Oracle's IT security for review and response to potential threats. See: https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
Additional Comments for Control Domain above:			
Logging & Monitoring	**LOG-01.1**	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	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. 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?

	LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their LOG-01.1 evidence from Oracle Corporate may update that evidence annually.
	LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security-incident management process. Access to security logs is provided on the basis of need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.
	LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten.
	LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Oracle employs intrusion detection systems within the Oracle intranet to provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle utilizes a network-based monitoring approach to detect attacks on open firewalls ports within Oracle's intranet. Events are analyzed using signature detection, which is a pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to Oracle's IT security for review and response to potential threats. See also https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
	LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security-incident management process. Access to security logs is provided on the basis of need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated

			by internet-accessible systems are relocated to systems that are not internet-accessible.
	LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security-incident management process. Access to security logs is provided on the basis of need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.
	LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Oracle reviews logs for forensic purposes and security events, and identified anomalous activities feed into the security incident management process.
	LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Network Time Protocol (NTP) is used as a common time reference across the Oracle Advertising applications.
	LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Oracle Logging and Log Analysis Policy states Oracle's Corporate-level mandates for log retention, review, and analysis. Areas covered include minimum log requirements, responsibilities for the configuration and implementation of logging, alert review, problem management, retention, security, and protection of logs, as well as compliance review.
	LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Global Information Security is responsible for security oversight, compliance, and enforcement, and conducting information-security assessments leading the development of information security policy and strategy, as well as training and awareness at the corporate level. Policies are reviewed at least annually.
	LOG-08.1	Are audit records generated, and do they contain relevant security information?	Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten.

			See https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf the Oracle product documentation and security guide for your Oracle product.
	LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security-incident management process. Access to security logs is provided on the basis of need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible. See https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf the Oracle product documentation and security guide for your Oracle product.
	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'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. 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 See https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf the Oracle product documentation and security guide for your Oracle product.
	LOG-11.1	Are key lifecycle management events logged and monitored to enable	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

		auditing and reporting on cryptographic keys' usage?	from Corporate Security and development organizations define best practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence. CRB's responsibilities include: • Creating and maintaining standards for cryptography algorithms, protocols, and their parameters • Providing approved standards in multiple formats, for readability and automation • Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle • Providing practical guidance on using cryptography • Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography See https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf the Oracle product documentation and security guide for your Oracle product.
	LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Oracle Global Physical Security regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained. See https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf the Oracle product documentation and security guide for your Oracle product.
	LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and central systems are utilized globally 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.
	LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	In the event that Oracle determines that a security incident has occurred, Oracle promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared. Incident history is Oracle Confidential and is not shared externally.
Additional Comments for Control Domain above:			

Security Incident Management, E-Discovery & Cloud Forensics	**SEF-01.1**	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Reflecting the recommended practices in prevalent security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets.
	SEF-01.2	Are policies and procedures reviewed and updated annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their SEF-01.1 evidence from Oracle Corporate may update that evidence annually. Oracle Global Information Security (GIS) organization serves as the primary contact for security incident response, as well as to provide overall direction for incident prevention, identification, investigation, and resolution. 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. 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 • Eradicating an incident • Escalating an incident
	SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle evaluates and responds to events that create suspicion of unauthorized access to or handling of customer data, whether the data is held on Oracle hardware assets or on the personal hardware assets of Oracle employees and contingent workers. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to incidents. This policy authorizes Oracle Global Information Security (GIS) organization to serve as the primary contact for security incident response, as well as to provide overall direction for incident prevention, identification, investigation, and resolution.
	SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their SEF-01.1 evidence from Oracle Corporate may update that evidence at will for re-approval.

			In the event that Oracle determines that a security incident has occurred, Oracle promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities.
	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?	Access control refers to the policies, procedures, and tools that govern access to and use of resources. Examples of resources include a physical server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol. Least privilege is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties. Default-deny is a network-oriented approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination.
	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 Corporate and Line of Business Incident Teams execute the incident response plan not less than annually. Please see: https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
	SEF-05.1	Are information security incident metrics established and monitored?	Oracle evaluates and responds to events that create suspicion of unauthorized access to or handling of customer data, whether the data is held on Oracle hardware assets or on the personal hardware assets of Oracle employees and contingent workers. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to incidents. This policy authorizes Oracle Global Information Security (GIS) organization to serve as the primary contact for security incident response, as well as to provide overall direction for incident prevention, identification, investigation, and resolution.
	SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers.
	SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Formal procedures and central systems are utilized globally to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.

	SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	In the event that Oracle determines that a security incident has occurred, Oracle promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared. Incident history is also Oracle Confidential and is not shared externally. See Oracle Cloud Hosting and Delivery Policies, Pillar Documents and Service Descriptions for specific details about incident notifications: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Oracle also has formal requirements for its suppliers and partners to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle confidential information, and • Oracle hardware assets placed in their custody Agreements required for Oracle suppliers are at: https://www.oracle.com/corporate/suppliers.html
Additional Comments for Control Domain above:			
Supply Chain Management, Transparency & Accountability	**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?	Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ Oracle suppliers and partners are required to protect the data and assets Oracle entrusts to them. These 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 and partners are responsible for compliance with these

			standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards.
	STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations.
	STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Oracle also has formal requirements for its suppliers and partners to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when: Accessing Oracle and Oracle customers' facilities, networks and/or information systems Handling Oracle confidential information, and Oracle hardware assets placed in their custody Oracle suppliers are required to sign the agreements at https://www.oracle.com/corporate/suppliers.html
	STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Oracle's Supply Chain Risk Management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services. Quality and reliability for Oracle's hardware systems are addressed through a variety of practices, including: Design, development, manufacturing and materials management processes Inspection and testing processes Requiring that hardware supply chain suppliers have quality control processes and measurement systems Requiring that hardware supply chain suppliers comply with applicable Oracle requirements and specifications
	STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Oracle has functional responsibility for control implementation, as Oracle Advertising does not have customer tenancies.

	STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	The Oracle corporate security architect helps set internal information-security technical direction and guides Oracle's IT departments and lines of business towards deploying information security and identity management solutions that advance Oracle's Information Security goals. The corporate security architect works with Global Information Security and Global Product Security, and the development Security Leads to develop, communicate, and implement corporate security architecture roadmaps. Corporate Security architecture manages a variety of programs and leverages multiple methods of engaging with leadership and operational security teams responsible for Oracle operations, services, cloud, and all other lines of business.
	STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Corporate Security Architecture manages a cross-organization working group focused on security architecture, with the goal of collaboratively guiding security for Oracle cloud services. Participation includes members from Oracle cloud service development, operations, and governance teams.
	STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	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. 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. 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.
	STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Supply availability and 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
	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	Oracle suppliers and partners are required to protect the data and assets Oracle entrusts to them. These 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 and partners are responsible for compliance with these standards, including

		• 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	ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards. These standards cover a wide range of requirements in the following critical areas: • Personnel/human resources security • Business continuity and disaster recovery • Information security organization, policy, and procedures • Compliance and assessments • Security incident management and reporting • IT security standards • Baseline physical and environmental security
	STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	See STA-13.1
	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?	Quality and reliability for Oracle's hardware systems are addressed through a variety of practices, including: • Design, development, manufacturing, and materials management processes • Inspection and testing processes • Requiring that hardware supply chain suppliers have quality control processes and measurement systems • Requiring that hardware supply chain suppliers comply with applicable Oracle requirements and specifications See: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
	STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	See STA-13.1
	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 which utilize third party providers to maintain a program which manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual review, where appropriate per the risk to data confidentiality, availability or integrity

			introduced by the way each particular supplier's goods or services are leveraged.
	STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Oracle's Supplier Security Management Policy requires all lines of business which utilize third party providers to maintain a program which manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each particular supplier's goods or services are leveraged.
Additional Comments for Control Domain above:			
Threat & Vulnerability Management	**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?	See https://www.oracle.com/corporate/security-practices/assurance/vulnerability/ Oracle uses the Common Vulnerability Scoring System (CVSS) to report the relative severity of security vulnerabilities. CVSS information is provided in the risk matrices published in Critical Patch Update and Security Alert Advisories as individual metrics which cover the technical aspects of the vulnerabilities, such as the preconditions required for successful exploitation. CVSS uses a formula to turn the metrics into a Base Score between 0.0 and 10.0, where 10.0 represents the greatest severity. Oracle orders the risk matrices using this Base Score, with the most severe vulnerability at the top of each risk matrix. Oracle provides additional information for each vulnerability to help customers make better informed patching decisions. Oracle adopted CVSS in 2006 and has adopted newer versions of the standard as they are released. CVSS version 3.1, the version used in current advisories and alerts, was adopted in July 2020. Use of Common Vulnerability Scoring System (CVSS) by Oracle provides a detailed explanation on how the CVSS ratings are applied in Oracle's risk advisories. Common Vulnerabilities and Exposures (CVE) numbers are used by Oracle to identify the vulnerabilities listed in the risk matrices in Critical Patch Update and Security Alert advisories. CVE numbers are unique, common identifiers for publicly known information about security vulnerabilities. The CVE program is co-sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security and is managed by MITRE corporation. Oracle is a CVE Numbering Authority (CNA), that is the company can issue CVE numbers for vulnerabilities in its products. Note that the ordering of CVE

			numbers in Oracle's security advisories does not necessarily correspond to dates of discovery of the vulnerabilities they reference. In other words, CVE numbers are not assigned in order of the discovery dates of vulnerabilities whose fixes will be delivered in those distributions. This is because CVE Numbering Authorities (CNAs) like Oracle periodically get sets of CVE numbers from MITRE so a separate request for a new CVE does not need to be made every time a vulnerability is discovered. CVE numbers are assigned to vulnerabilities sequentially by Oracle from the pool of CVE number assigned by the CVE organization about 3 to 4 weeks before the scheduled distribution of the fix through the Critical Patch Update program.
	TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their TVM-01.1 evidence from Oracle Corporate may update that evidence annually.
	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. See https://www.oracle.com/corporate/security-practices/assurance/vulnerability/
	TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies are reviewed annually and updated as required. Oracle Lines of Business that gain approval of their TVM-01.1 evidence from Oracle Corporate may update that evidence at will for re-approval.
	TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Oracle may issue a Security Alert in the case of a unique or dangerous threat to our customers. In this event, customers will be notified of the Security Alert by email notification through My Oracle Support and Oracle Technology Network. The fix included in the Security Alert will also be included in the subsequent Critical Patch Update. See https://www.oracle.com/corporate/security-practices/assurance/vulnerability/
	TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update	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

		detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	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.
	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 requires security reviews for any third-party components embedded in Oracle products and cloud services. The development teams must use current and actively maintained versions of third-party software. Teams must verify that third-party components are free of publicly reported vulnerabilities at the time of their inclusion in an Oracle product distribution or use by a cloud service. They must also verify that there is active maintenance for any third-party component selected and must confirm that component maintenance (either by the component source, by a fourth party, or by Oracle) extends throughout the support life of the embedding product. Development teams are required to compile binaries for third party open-source components from source code. This ensures that the binaries used in Oracle products derive from known source code, which improves Oracle's ability to support that code if needed and reduces the risk of malicious functionality being embedded in third party binaries. Under Oracle Software Security Assurance, development teams are required to monitor third-party components in use for reports of new security vulnerabilities. Software Composition Analysis (SCA) tools are integrated into DevOps processes to scan Oracle software. These tools can help identify newly reported vulnerabilities in third party components. Oracle requires third-party components to be updated and patched in a timely fashion.
	TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Oracle regularly performs penetration testing and security assessments against Oracle Cloud infrastructure, platforms, and applications in order to validate and improve the overall security of Oracle Cloud Services.
	TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	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. A fixed CPU schedule takes the guesswork out of patch management. The schedule is also designed to avoid typical blackout dates during which customers cannot typically alter their production environments. Patch updates are cumulative for many Oracle products. This provides customers the ability to catch up quickly to the current security release level, since the application of the latest cumulative CPU resolves all previously addressed vulnerabilities.
	TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Vulnerabilities are remediated by Oracle in order of the risk they pose to users. This process is designed to patch the security holes with the greatest associated risk first in the Critical Patch Update, resulting in optimizing the security posture of all Oracle customers. As much as possible, Oracle tries to make Critical Patch Updates cumulative; that is, each Critical Patch Update contains the security fixes from all previous Critical Patch Updates. In practical terms, for those products that receive cumulative fixes, the latest Critical Patch Update is the only one that needs to be applied when solely using these products, as it contains all required fixes. Fixes for the other products that do not receive cumulative fixes are released as one-off patches. It is necessary for these products to refer to previous Critical Patch Update advisories to find all the patches that may need to be applied. See: https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html
	TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Audit reports about Oracle Cloud Services are periodically published by Oracle's third-party auditors. Reports may not be available for all services or all audit types or at all times. Customer may request access to available audit reports for a particular Oracle Cloud service via Sales. 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. See also: https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html
	TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Oracle may provide information which summarizes that point-in-time penetration testing and environment vulnerability scans are performed regularly, with a summary of findings. Oracle does not provide the details of identified weaknesses because sharing that information would put all customers using that product or service at risk. Please see the Oracle Cloud

			Security Testing Policy for information about customer testing of Oracle Cloud services: https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security-testing-policy.htm
Additional Comments for Control Domain above:			
Universal Endpoint Management	**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. 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 descriptions of Oracle Corporate Endpoint controls, see: https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
	UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations.
	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. 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. Any Oracle employee who is discovered violating this standard may be subject to disciplinary action up to and including termination of employment.

	UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	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.
	UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. 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. Oracle policy specifies the data (or fields) which must be maintained about these information systems in the approved system inventory. The required technical and business information fall in the following categories: • Hardware details such as manufacturer, model number and serial number of the equipment, system, or device • Physical location of the data center/facility and location within that building • Software details such as the operating system and applications and associated versions • Classification of information assets • Ownership information at the organizational and individual levels
	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?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice. 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.

	UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	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.
	UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	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: 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. 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 released products on customers. Oracle has adopted transparent security vulnerability disclosure and remediation policies. The company is committed to treating all customers equally and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs. See also: https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html
	UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage 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.

	UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Antivirus software must be scheduled to perform daily threat definition updates and virus scans. The Oracle Information Technology (OIT) organization keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. OIT is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. OIT provides automation to verify antivirus configuration.
	UEM-10.1	Are software firewalls configured on managed endpoints?	Oracle policy requires the use of antivirus, intrusion protection and firewall software on laptops 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. While desktops and laptops do not process customer data within Oracle Advertising, they are encrypted using approved software. Reports enable lines of business management to verify deployment of laptop encryption for their organization. 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?	Data Loss Prevention or DLP-type technologies are in place for workstations with access to scoped data and servers containing scoped data. Internet proxies are deployed. Additionally, bastion hosts are used to access production servers.
	UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Oracle Advertising does not allow the use of mobile devices to access the production network. There is a guest VLAN mobile devices may use to access the Internet. Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile device operating systems and platforms. Enterprise Engineering and corporate security organizations regularly promote awareness of mobile device security and good practice.
	UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable	Oracle has policies governing remote access to systems transmitting, processing, and storing scoped data. These policies are management-approved and communicated to applicable employees.

		remote company data deletion on managed endpoint devices?	Remote access for Oracle personnel requires connection to the restricted-access Oracle network from a non-Oracle location to use either an IPsec or TLS encrypted VPN with two-factor authentication. Additionally, access to the Oracle Advertising production environment requires multi-factor authentication over a VPN. The OCNA VPN that is used by Oracle staff to connect to Oracle's infrastructure uses both machine certificates and other identifiers to validate that the device is Oracle owned and provisioned before allowing access to Oracle resources.
	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?	Personal devices are not allowed to connect to the Oracle Advertising internal network. We provide guest and mobile VLANs to access the Internet.
Additional Comments for Control Domain above:			

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

Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Advertising DMP 1p and BlueKai 3p