ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle CTMS Cloud Service

August 2023 | Version 1.0

TABLE OF CONTENTS

PURPOSE STATEMENT

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

The answers contained in this CAIQ version 3.1 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

Oracle Life Sciences services provide pharmaceutical, biotechnology, medical device, and healthcare organizations with innovative products that optimize clinical research and development, improve patient outcomes, and accelerate value-based care. For more information, see https://docs.oracle.com/en/industries/health-sciences/index.html

The scope for this questionnaire includes the following Oracle Life Sciences CTMS Cloud Service and associated components hosted in Oracle Cloud Infrastructure (OCI):

- Siebel Clinical Trial Management https://docs.oracle.com/en/industries/health-sciences/siebel-clinical/index.html

CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ)

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Application & Interface Security: Application Security	AIS-01.1	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	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. To ensure that Oracle products are developed with consistently high security assurance, and to help developers avoid common coding mistakes, Oracle employs formal secure coding standards. For more information, see https://www.oracle.com/corporate/security-practices/assurance/
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	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 comprehensive 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 static code analyzer from Fortify Software, an HP company, as well a variety of internally developed tools, to catch problems while code is being written. Products developed in most modern programming languages (such as C/C++, Java, C#) and platforms (J2EE, .NET) are scanned to identify possible security issues. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	Oracle Developers use static and dynamic analysis tools to detect security defects in Oracle code prior to production. Identified issues are evaluated and addressed in order of priority and severity. Oracle management tracks metrics regarding issue identification and resolution. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for	Oracle Software Security Assurance (OSSA) policies require that third-party components (e.g., open-source components used in the Oracle Clouds or distributed in traditional Oracle product distributions) be appropriately assessed for security purposes. Additionally, Oracle has formal policies and procedures which define

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		Systems/Software Development Lifecycle (SDLC) security?	requirements for managing the safety of its supply chain, including 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	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. An example program for managing the security of Oracle's architecture is the Corporate Security Solution Assurance Process (CSSAP). 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
Application & Interface Security: Customer Access Requirements	AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	See Oracle Cloud Hosting and Delivery Policies and Pillar documents to understand how Oracle will deliver Cloud Services: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html Before deploying Oracle cloud services, Oracle strongly recommends that cloud customers formally analyze their cloud strategy to determine the suitability of using the applicable Oracle cloud services in light of their own legal and regulatory compliance obligations. Making this determination remains solely the responsibility of customers. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
	AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	Before deploying Oracle cloud services, Oracle strongly recommends that cloud customers formally analyze their cloud strategy to determine the suitability of using the applicable Oracle cloud services in light of their own legal and regulatory compliance obligations. Making this determination remains solely the responsibility of customers.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
Application & Interface Security: Data Integrity	AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?	Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. They discuss general security knowledge areas such as design principles, cryptography and communications security, common vulnerabilities, etc. The Standards provide specific guidance on topics such as data validation, CGI, user management, and more. All Oracle developers must be familiar with these standards and apply them when designing and building products. The coding standards have been developed over a number of years and incorporate best practices as well as lessons learned from continued vulnerability testing by Oracle's internal product assessment team. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/
	AIS-03.2	Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Data input and output validation occurs on form fields to sanitize unsafe and unpermitted characters and commands. CTMS Cloud Service is tested throughout the application's development phases to help ensure these validation techniques are applied. For more information, see Oracle's Secure Coding Practices: https://www.oracle.com/corporate/security-practices/assurance/development https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
Application & Interface Security: Data Security / Integrity	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• 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
Additional Comments for Control Domain above: N/A			
Audit Assurance & Compliance: Audit Planning	AAC-01.1	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources, etc.) for reviewing the efficiency and effectiveness of implemented security controls?	Oracle develops and maintains an agreed upon audit plan with third party auditors for reviewing the efficiency and effectiveness of implemented security controls for the infrastructure. Oracle conducts internal security reviews, assessments, and audits to confirm CTMS Cloud Service complies with Oracle information security policies, procedures, and practices.
	AAC-01.2	Does your audit program take into account effectiveness of implementation of security operations?	Oracle leverages third-party audits, which cover effectiveness of implementation of security operations. Oracle conducts internal security reviews, assessments, and audits to confirm CTMS Cloud Service complies with Oracle information security policies, procedures, and practices.
Audit Assurance & Compliance: Independent Audits	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	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. CTMS Cloud Service currently has ISO 27001 and 27018 certifications. It is also assessed annually for HIPAA compliance by Oracle's third-party auditors. Customers may request access to these reports and certifications through their sales representative. Before deploying Oracle cloud services, Oracle strongly recommends that cloud customers formally analyze their cloud strategy to determine the suitability of using the applicable Oracle cloud services in light of their own legal and regulatory compliance obligations. Making this determination remains solely the responsibility of customers. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure 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. 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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• **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.
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	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. 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 a 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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	AAC-02.4	Do you conduct internal audits at least annually?	Internal audits are performed annually to confirm compliance with security and operational procedures.
	AAC-02.5	Do you conduct independent audits at least 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. CTMS Cloud Service currently has ISO 27001 and 27018 certifications. It is also assessed annually for HIPAA compliance by Oracle's third-party auditors. Customers may request access to these reports and certifications through their sales representative.
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	Penetration test summary reports for the cloud service are available to customers upon request under NDA. Customers should inquire with their account representatives.
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	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. Customers may request access to these reports and certifications via Sales.
Audit Assurance & Compliance: Information System Regulatory Mapping	AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	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 Before deploying Oracle cloud services, Oracle strongly recommends that cloud customers formally analyze their cloud strategy to determine the suitability of using the applicable Oracle cloud services in light of their own legal and regulatory compliance obligations. Making this determination remains solely the responsibility of customers. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
Additional Comments for Control Domain above: N/A			
Business Continuity Management & Operational Resilience:	BCR-01.1	Does your organization have a plan or framework for business	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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Business Continuity Planning		continuity management or disaster recovery management?	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	Do you have more than one provider for each service you depend on?	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.
	BCR-01.3	Do you provide a disaster recovery capability?	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. Service-specific Pillar documents provide additional information about specific cloud services: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	BCR-01.4	Do you monitor service continuity with upstream providers in the event of provider failure?	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	BCR-01.5	Do you provide access to operational redundancy reports, including the services you rely on?	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: 1. Emergency Response, managed by Facilities Environment, Health and Safety Program 2. Crisis Management, managed by Global Physical Security 3. Business Continuity Management, managed by the corporate RMRP Program Management Office 4. Disaster Recovery, managed by Global Information Technology 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-01.6	Do you provide a tenant-triggered failover option?	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-01.7	Do you share your business continuity and redundancy plans with your tenants?	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 designed to assess our DR plans. Lessons learned from the exercise are implemented as deemed appropriate into standard operations and DR procedures as appropriate.
Business Continuity Management & Operational Resilience:	BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental	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:

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Business Continuity Testing		changes to ensure continuing effectiveness?	• 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
Business Continuity Management & Operational Resilience: Power / Telecommunications	BCR-03.1	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	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-03.2	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	Oracle data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Potential 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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			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.
Business Continuity Management & Operational Resilience: Documentation	BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Lines of business are required to maintain operational and technical documents and make these available to relevant personnel.
Business Continuity Management & Operational Resilience: Environmental Risks	BCR-05.1	Is physical damage anticipated and are countermeasures included in the design of physical protections?	Oracle data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Potential 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.
Business Continuity Management & Operational Resilience: Equipment Location	BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	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.
Business Continuity Management & Operational Resilience: Equipment Maintenance	BCR-07.1	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• 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-07.2	Do you have an equipment and datacenter maintenance routine or plan?	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.
Business Continuity Management & Operational Resilience: Equipment Power Failures	BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• 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
Business Continuity Management & Operational Resilience: Impact Analysis	BCR-09.1	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc)?	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.
	BCR-09.2	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	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.
Business Continuity Management & Operational Resilience: Policy	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	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.
Business Continuity Management & Operational Resilience: Retention Policy	BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	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-11.2	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	Customers are generally responsible for managing retention of data during their use of Oracle Cloud services.
	BCR-11.3	Have you implemented backup or recovery mechanisms to ensure	Oracle Cloud Hosting and Delivery Policies describe the Oracle Cloud Service Continuity Policy, Oracle Cloud Services High Availability Strategy, Oracle Cloud

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		compliance with regulatory, statutory, contractual or business requirements?	Services Backup Strategy and Oracle Cloud Service Level Agreement: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	BCR-11.4	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	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
	BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	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-11.6	Does your cloud solution include software/provider independent restore and recovery capabilities?	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-11.7	Do you test your backup or redundancy mechanisms at least annually?	Oracle's Information Technology organization conducts an annual Disaster Recovery 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.
Additional Comments for Control Domain above: N/A			
Change Control & Configuration Management: New Development / Acquisition	CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	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-02.1	Are policies and procedures for change management, release, and	Oracle has formal requirements for its suppliers and partners to confirm they protect Oracle and third-party data and assets entrusted to them. The Supplier Information

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Change Control & Configuration Management: Outsourced Development		testing adequately communicated to external business partners?	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 See requirements for Oracle suppliers: https://www.oracle.com/corporate/suppliers.html
	CCC-02.2	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	Oracle's Supplier Security Management Policy requires all lines of business which utilize third party providers to maintain a program that manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities, such as an annual review, where appropriate per the risk to data confidentiality, availability or integrity introduced by how each particular supplier's goods or services are leveraged.
Change Control & Configuration Management: Quality Testing	CCC-03.1	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	CTMS Cloud Service uses a formal change management and testing process designed for the purpose to help ensure availability, confidentiality, and integrity. For more information, see the "Secure Development" tab on the Software Security Assurance page: https://www.oracle.com/corporate/security-practices/assurance
	CCC-03.2	Is documentation describing known issues with certain products/services available?	Known issues that are not security vulnerabilities are published in the Release Notes for each service release. See the specific Trial Management and Monitoring Cloud Service Release Notes for the appropriate release: https://docs.oracle.com/en/industries/health-sciences/siebel-clinical/index.html (for issues addressed in the specific release).
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Oracle has formal practices to identify, analyze, and remediate security vulnerabilities that may affect CTMS Cloud Service. The Oracle security and development teams monitor relevant vendor and industry bulletins, including Oracle's security advisories, to identify and assess relevant security patches. Additionally, various security testing activities are performed by the CTMS Cloud Service teams throughout the development cycle to identify potential issues. These activities include the use of static and dynamic analysis tools, as well as vulnerability assessment tools. Customers and security researchers can report security vulnerabilities to Oracle per the process documented at Oracle.com: How to Report Security Vulnerabilities to Oracle or by submitting a Service Request in their designated support system (for example, My Oracle Support (MOS) or Support Cloud).

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			Oracle's strategic priority for the handling of vulnerabilities is to remediate these issues according to their severity and the risk they pose in the context of the use of CTMS Cloud Service. The Common Vulnerability Scoring System (CVSS) Base Score is one of the criteria used in assessing the relative severity of vulnerabilities. All vulnerabilities identified are tracked in a defect tracking system. All fixes are thoroughly tested to avoid issues in production. Prior to each major release of CTMS Cloud Service, Oracle performs security testing and uses formal security criteria before bringing the new release into production. Vulnerability scanning is performed daily for CTMS Cloud Service. Penetration testing in the production environment is performed periodically and prior to each new major release. Oracle's goal is to perform remediation actions, including testing, customer notification, implementation, and updates, within maintenance windows. If emergency maintenance is required due the assessed severity, the process outlined in Section 4 of the Oracle Cloud Hosting and Delivery Policies is followed.
	CCC-03.4	Do you have controls in place to ensure that standards of quality are being met for all software development?	Quality is part of the CTMS Cloud Service development process. Multiple methodologies and tools are used to ensure quality standards are met.
	CCC-03.5	Do you have controls in place to detect source code security defects for any outsourced software development activities?	Not applicable – LSSGBU does not outsource software development activities.
	CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	Oracle Secure Operations Standard requires compliance with Oracle Secure Configuration rules, which mandates, among other things that debugging and test code elements be removed from released software. For more information about Oracle Software Security Assurance, see https://www.oracle.com/corporate/security-practices/assurance/
Change Control & Configuration Management: Quality Testing	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Oracle requires any changes to the CTMS Cloud Service production environment to go through the Change Management process described in CCC-01.1. Additionally, the GBUs maintain a list of unauthorized potentially unwanted programs (PUP), which are explicitly prohibited from being installed on the systems through automated processes. Any program that is executed on SaaS systems is subsequently validated against reputation sources and alerts are generated for investigation if any suspicious program is executed.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Change Control & Configuration Management: Production Changes	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	Oracle Cloud Change Management Policy, including roles and responsibilities, is detailed in the Oracle Cloud Hosting and Deliveries Policy: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	CCC-05.2	Do you have policies and procedures established for managing risks with respect to change management in production environments?	CTMS Cloud Service Operations has policies and procedures established for managing risks with respect to change management in production environments. Oracle requires CTMS Cloud Service to follow formal change management procedures to review, test, and approve changes before the application is deployed in the Oracle Cloud production environment. Changes made through change management procedures include: • System and service maintenance activities • Management of application updates • Coordination of customer specific changes, where required Oracle works to design cloud services to minimize service interruption during the implementation of changes. For more information, see the 'Oracle Cloud Change Management Policy' section of the Oracle Cloud Hosting and Delivery Policies document: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	CCC-0.5.3	Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	CTMS Cloud Service has technical measures in place within the change management process designed to ensure that changes in production environments adhere to Service Level Agreements (SLA).
Additional Comments for Control Domain above: N/A			
Data Security & Information Lifecycle Management: Classification	DSI-01.1	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transportin g data in the wrong country)?	CTMS Cloud Service customers cannot identify virtual machines using policy tags or metadata. Customers do not have access to operating system functions.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	DSI-01.2	Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	CTMS Cloud Service customers cannot identify hardware via policy tags/metadata/hardware tags. Customers do not have access to operating system functions.
Data Security & Information Lifecycle Management: Data Inventory / Flows	DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	Oracle requires CTMS Cloud Service to document and maintain data inventories and data flows. This documentation is for internal use only and is shared with appropriate internal audit teams.
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	A customer's order specifies the Data Center Region in which the services environment will reside. Oracle provides production and test environments in the Data Center Region stated in the order. In the event of a disaster, the production service will be restored in the Data Center Region stated in the order. Oracle and its affiliates may perform certain aspects of operating cloud services, such as service administration and support, as well as other Services, including Professional Services, from locations and/or through use of subcontractors, worldwide. For more information, see the Global Business Unit Cloud Services Pillar Document under the Oracle Cloud Hosting and Delivery Policies: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
Data Security & Information Lifecycle Management: E-commerce Transactions	DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	CTMS Cloud Service supports the protection of customer data in transit over the network using a variety of standards-based, secure protocols such as Transport Layer Security (TLS) 1.2 or a successor and Internet Protocol Security (IPsec). For more information, see the Oracle Cloud Hosting and Delivery Policies: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Encryption is the process of rendering data unreadable without the specific key to decrypt the data. 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. 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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms.
Data Security & Information Lifecycle Management: Handling / Labeling / Security Policy	DSI-04.1	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?	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
	DSI-04.2	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	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.
	DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	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.
Data Security & Information Lifecycle Management: Nonproduction Data	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	CTMS Cloud Service is designed and architected to help avoid production data being moved or replicated outside of the production environment. The following controls have been implemented: • Physical and/or logical network boundaries with strictly enforced change control policies • Segregation of duties requiring a business need to access an environment • Highly restricted physical and/or logical access to an environment • Strict controls that define coding practices, quality testing and code promotion • Ongoing security, privacy, and secure coding practice awareness training • Logging and audit of system access • Regular compliance audits to verify control effectiveness
Data Security & Information Lifecycle Management: Ownership / Stewardship	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Data Security & Information Lifecycle Management: Secure Disposal	DSI-07.1	Do you support the secure deletion (e.g., degaussing/ cryptographic wiping) of archived and backed-up data?	Oracle's Media Sanitation and Dispoal 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.
	DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Oracle Cloud Hosting and Delivery Policy describes handling of customer data at termination of services: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
Additional Comments for Control Domain above: N/A			
Datacenter Security: Asset Management	DCS-01.1	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	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.
	DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	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).
Datacenter Security: Controlled Access Points	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	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. Potential 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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			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.
Datacenter Security: Equipment Identification	DCS-03.1	Do you have a capability to use system geographic location as an authentication factor?	CTMS Cloud Service does not provide geolocation restrictions for customer access; however, customers can federate with a Security Assertion Markup Language (SAML) provider of their choice to leverage geographic location as an authentication control via the SAML identity provider if needed.
	DCS-03.2	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	CTMS Cloud Service does not provide this feature to validate connection authentication.
Datacenter Security: Offsite Authorization	DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	The relocation or transfer of hardware, software, or data to an offsite premises is not a standard practice and would require appropriate authorization.
Datacenter Security: Offsite Equipment	DCS-05.1	Can you provide tenants with your asset management policies and procedures?	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.
Datacenter Security: Policy	DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		working environment in offices, rooms, facilities, and secure areas?	assessments to confirm that the correct and effective mitigation controls are in place and maintained.
	DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	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.
Datacenter Security: Secure Area Authorization	DCS-07.1	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	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. Furthermore, the retention period for CCTV monitoring and recording ranges from 30-90 days minimum, depending on the facility's functions and risk level.
Datacenter Security: Unauthorized Persons Entry	DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• 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. Furthermore, the retention period for CCTV monitoring and recording ranges from 30-90 days minimum, depending on the facility's functions and risk level.
Datacenter Security: User Access	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	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.
Additional Comments for Control Domain above: N/A			
Encryption & Key Management: Entitlement	EKM-01.1	Do you have key management policies binding keys to identifiable owners?	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. 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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Encryption & Key Management: Key Generation	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	CTMS Cloud Service does not provide this functionality.
	EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	CTMS Cloud Service is single-tenant and Oracle manages all tenant's keys. Oracle manages keys for the overall environment and does not allow tenants to manage the key.
	EKM-02.3	Do you maintain key management procedures?	Solutions for managing encryption keys at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). Oracle 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
	EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	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.
	EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	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.
Encryption & Key Management: Encryption	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	For CTMS Cloud Service, tenant data at rest is stored using Oracle Transparent Data Encryption (TDE). TDE uses AES 256 for Master Key encryption and AES 128 for Tablespace key encryption. For more information, see https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/frequently-asked-questions-about-transparent-data-encryption.html#GUID-BBA0097F-258B-44C5-A83F-2DE625A34EC1
	EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across	Encryption is employed to protect data and virtual machine images during transport across public networks. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		and between networks and hypervisor instances?	
	EKM-03.3	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	Oracle has formal policies and procedures governing the use of encryption. Additionally, Oracle's Cryptography Review Board (CRB) defines and promotes cryptography-related technical standards for Oracle products and services. The group is primarily responsible for making technical decisions and authoring internal standards to address government and industry requirements. Representatives from Corporate Security and development organizations define best practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence. CRB's responsibilities include: • Creating and maintaining standards for cryptography algorithms, protocols, and their parameters • Providing approved standards in multiple formats, for readability and automation • Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle • Providing practical guidance on using cryptography • Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography For more information, please see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html
Encryption & Key Management: Storage and Access	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	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
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	Oracle maintains the encryption keys associated with the CTMS Cloud Service.
	EKM-04.3	Do you store encryption keys in the cloud?	For CTMS Cloud Service subscriptions, master encryption keys are stored in a proprietary software management system built and used by Oracle.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	EKM-04.4	Do you have separate key management and key usage duties?	CTMS Cloud Service has established and implemented procedures to enforce segregation of key management and key usage duties. Key management encompasses the entire life cycle of cryptographic keys and has identified a method for establishing and managing keys in each management phase from generation, installation, storage, rotation, and destruction.
Additional Comments for Control Domain above: N/A			
Governance and Risk Management: Baseline Requirements	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	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.
	GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Oracle employs standardized system hardening practices across the CTMS Cloud Service. This includes alignment with base images and/or baselines, restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management and logging.
Governance and Risk Management: Risk Assessments	GRM-02.1	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	Oracle's risk assessment methodology and process are aligned with ISO 27001 and 27018 standards. Oracle's security and privacy risk assessment processes account for data residency, legal and statutory requirements for retention periods and data protection and classification and are modeled after information security and privacy frameworks, standards, and regulations, such as ISO 27001 and 27018 and General Data Protection Regulation (GDPR). Customers are responsible for their legal statutory and residency requirements for their data. Before deploying CTMS Cloud Service, Oracle strongly recommends that cloud customers formally analyze their cloud strategy to determine the suitability of use in light of their own legal and regulatory compliance obligations. Making this determination remains solely the responsibility of customers. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing, and if additional controls are required and mutually agreed upon, additional charges may apply.
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	Oracle conducts internal security reviews, assessments, and audits annually to confirm compliance with Oracle information security policies, procedures, and practices.
Governance and Risk Management:	GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and	Oracle places a strong emphasis on personnel security. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud,

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Management Oversight		compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions. 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.
Governance and Risk Management: Management Program	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	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
	GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	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.
Governance and Risk Management: Management Support / Involvement	GRM-05.1	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	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)

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			• Assisting lines of business security organizations with fostering a culture of security across regions and functional areas.
Governance and Risk Management: Policy	GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	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.
	GRM-06.2	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	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
	GRM-06.3	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	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/
	GRM-06.4	Can you provide evidence of due diligence mapping of your controls, architecture, and	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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		processes to regulations and/or standards?	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
	GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	CTMS Cloud Service currently has ISO 27001 and 27018 certifications. It is also assessed annually for HIPAA compliance by Oracle's third-party auditors. Customers may request access to these reports and certifications through their sales representative. CTMS Cloud Service regulatory compliance assessments are available for customers at My Oracle Support (https://support.oracle.com) (Doc ID 1470961.1).
Governance and Risk Management: Policy Enforcement	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	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.
	GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	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.
Governance and Risk Management: Policy Reviews	GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	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.
Governance and Risk Management: Policy Reviews	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Customers can subscribe to Oracle Cloud Hosting and Delivery Policy updates: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	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.
Governance and Risk Management: Assessments	GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/objectives.html
	GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	The risk assessment process begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and identifying controls and safeguards intended to reduce the impact of the risk to an acceptable level. Measures, recommendations, and controls are put in place to mitigate risks.
Governance and Risk Management: Program	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	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
	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	Corporate governance teams and programs are described at https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html 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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Additional Comments for Control Domain above: N/A			
Human Resources: Asset Returns	HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned 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-01.2	Do you have asset return procedures outlining how assets should be returned within an established period?	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.
Human Resources: Background Screening	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	In the United States, Oracle uses an external screening agency to perform pre-employment background investigations for newly hired U.S. personnel. Personnel screening in other countries varies according to local laws, employment regulations, and local Oracle policy.
Human Resources: Employment Agreements	HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	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-03.2	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	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.
Human Resources: Employment Termination	HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	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.
Human Resources: Portable / Mobile Devices	HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	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
Human Resources: Non-Disclosure Agreements	HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	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.
Human Resources: Roles / Responsibilities	HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	See Getting Started tasks and managing the CTMS Cloud Service documentation at https://docs.oracle.com/en/industries/health-sciences/siebel-clinical/index.html
Human Resources: Acceptable Use	HRS-08.1	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	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. Antivirus software must be scheduled to perform daily threat-definition updates and virus scans.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			Oracle's Global Desktop Strategy (GDS) organization keeps anti-virus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. GDS is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. GDS provides automation to verify anti-virus configuration.
	HRS-08.2	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	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.
Human Resources: Training / Awareness	HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	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.
	HRS-09.2	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	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-09.3	Do you document employee acknowledgment of training they have completed?	Training completion is tracked within the Oracle Global Training tool per Oracle policy.
	HRS-09.4	Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	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. Management is notified of incomplete employee training plans.
	HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	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-

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy.
	HRS-09.6	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	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.
Human Resources: User Responsibility	HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	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-10.2	Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	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.
	HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	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.
Human Resources: Workspace	HRS-11.1	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	Oracle personnel are required to utilize the Oracle's Global Desktop Strategy (GDS) solutions for Windows Server Update Services (WSUS), virus definitions, security updates and tools which automatically lock the screen.
	HRS-11.2	Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	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.
Additional Comments for Control Domain above: N/A			

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Identity & Access Management: Audit Tools Access	IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	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?
	IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	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.
Identity & Access Management: User Access Policy	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	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-02.2	Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	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-02.3	Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	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-02.4	Do you have procedures and technical measures in place for	Not applicable. CTMS Cloud Service is single-tenant.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		data access segmentation in multi-tenant system architectures?	
	IAM-02.5	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	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-02.6	Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	Oracle's Logical Access Controls Policy describes logical access control requirements for all Oracle systems, including authentication, authorization, access approval, provisioning and revocation for employees and any other Oracle-defined users with access to Oracle systems which are not internet-facing, publicly accessible systems. The Logical Access Controls Policy sets forth the requirements for information owners to define, document, and enforce logical access controls for the information systems for which they have responsibility, and which process confidential – Oracle internal, restricted and highly restricted information, including information held on behalf of customers, partners and other third parties. CTMS Cloud Service has (optional) support for Single Sign-on (SSO) authentication. CTMS Cloud Service versions 22.1 and onwards support multifactor authentication (MFA) for customer access using Oracle Identity Cloud Services (IDCS).
	IAM-02.7	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	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.
Identity & Access Management: Diagnostic / Configuration Ports Access	IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	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.
	IAM-04.1	Do you manage and store the identity of all personnel who have	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Identity & Access Management: Policies and Procedures		access to the IT infrastructure, including their level of access?	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-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of 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.
Identity & Access Management: Segregation of Duties	IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	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
Identity & Access Management: Source Code Access Restriction	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	Oracle maintains 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's objectives with protecting its source code are twofold: • Protect the company's intellectual property while fostering innovation • Protect Oracle and its customers against malicious attempts to alter Oracle's source code or exploit security vulnerabilities
	IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Identity & Access Management: Third Party Access	IAM-07.1	Does your organization conduct third-party unauthorized access risk assessments?	CTMS Cloud Service access is reviewed as part of standard internal and third-party audits and assessments. Administrative access to cloud services is restricted behind a secured network and bastion hosts. The bastion hosts have keystroke logging enabled for auditing purposes. Each access point goes through multiple levels of approvals. Access logs are reviewed regularly, as are employee access entitlements to help ensure only authorized access is enabled. Customer access to the CTMS application is managed by the customer using the CTMS Oracle Identity Manager (IDM), or for versions 22.1 and onwards, using Oracle Identity Cloud Service (IDCS).
	IAM-07.2	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropraite access?	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
Identity & Access Management: User Access Restriction / Authorization	IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	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-08.2	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	IAM-08.3	Do you limit identities' replication only to users explicitly defined as business necessary?	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.
Identity & Access Management: User Access Authorization	IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	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? Customer access to the CTMS application is managed by the customer using the CTMS Oracle Identity Manager (IDM), or for versions 22.1 and onwards, using Oracle Identity Cloud Service (IDCS).
	IAM-09.2	Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	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? Customer access to the CTMS application is managed by the customer using the CTMS Oracle Identity Manager (IDM), or for versions 22.1 and onwards, using Oracle Identity Cloud Service (IDCS).
Identity & Access Management: User Access Reviews	IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege,	Oracle regularly reviews network, operating system and CTMS application 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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		by business leadership or other accountable business role or function?	
	IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	Oracle requires that remediation and certification actions be recorded and retained.
	IAM-10.3	Do you ensure that remediation actions for access violations follow user access policies?	Remediation and certification actions are implemented, recorded and retained as per Oracle policy.
	IAM-10.4	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	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.
Identity & Access Management: User Access Revocation	IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	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. Customer access to the CTMS application is managed by the customer using the CTMS Oracle Identity Manager (IDM), or for versions 22.1 and onwards, using Oracle Identity Cloud Service (IDCS).
	IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Oracle regularly reviews network, operating system and CTMS application 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-12.1	Do you support use of, or integration with, existing	CTMS Cloud Service has (optional) support for federated SSO authentication.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Identity & Access Management: User ID Credentials		customer-based Single Sign On (SSO) solutions to your service?	
	IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	CTMS Cloud Service has (optional) support for the Security Assertion Markup Language (SAML) 2.0 open standard.
	IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	CTMS Cloud Service has (optional) support for the Security Assertion Markup Language (SAML) 2.0 open standard.
	IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	CTMS Cloud Service does not provide this functionality.
	IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	CTMS Cloud Service does not provide this functionality.
	IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	CTMS has (optional) support for SSO authentication and customers can federate with the Security Assertion Markup Language (SAML) provider of their choosing to support MFA. CTMS Cloud Service versions 22.1 and onwards provide (optional) multifactor authentication (MFA) for customer access using Oracle Identity Cloud Service (IDCS).
	IAM-12.7	Do you allow tenants to use third-party identity assurance services?	CTMS Cloud Service does not directly support identity assurance; but if federated SSO is implemented, a customer can implement identity assurance outside of CTMS using the customer's SAML identity provider. See product-specific information for CTMS Cloud Service https://docs.oracle.com/en/industries/health-sciences/siebel-clinical/index.html
	IAM-12.8	Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	CTMS Cloud Service supports password requirements for minimum length, re-use attempts, and failed login attempts. CTMS Cloud Service also supports account lockout policy enforcement. Customers using federated SSO must check with their respective SSO implementation provider.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	CTMS Cloud Service does not allow tenants to define password and account lockout policies from the default values defined by the service.
	IAM-12.10	Do you support the ability to force password changes upon first logon?	CTMS Cloud Service supports this feature.
	IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	CTMS Cloud Service customer system administrators can manually unlock accounts. CTMS Cloud Service versions 22.1 and onwards support self-service password reset using IDCS, which also unlocks the account on success.
Identity & Access Management: Utility Programs Access	IAM-13.1	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	Access to CTMS Cloud Service systems, including access to service accounts that manage utility programs, is controlled by restricting access to authorized personnel. Security events are logged and monitored through a Security Information Event Management (SIEM) system.
Additional Comments for Control Domain above: Customer access to the CTMS application is managed by the customer using the CTMS Oracle Identity Manager (IDM), or for versions 22.1 and onwards, using Oracle Identity Cloud Service (IDCS). See product-specific information at https://docs.oracle.com/en/industries/health-sciences/siebel-cloud-clinical/22.1/			
Infrastructure & Virtualization Security: Audit Logging / Intrusion Detection	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	CTMS Cloud Service utilizes host-based and Network-based Intrusion Detection Systems (IDS) to protect the environment. IDS sensors are deployed to monitor suspicious network traffic. IDS alerts are routed to a centralized monitoring system that is managed by the security operations teams 24x7x365.
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	Oracle Global Business Units operates under policies which are aligned with the ISO/IEC 27002 Code of Practice for information security controls. Oracle Global Business Units' internal controls are mapped to applicable regulations and standards and subject to internal control reviews and testing by independent third-party audit organizations.
	IVS-01.4	Are audit logs centrally stored and retained?	Security logs are stored within the Security Information and Event Management system (SIEM) (or equivalent system) in a native, unaltered format and retained in accordance with Oracle's internal policies. Such logs are retained online for a minimum of 1 year, or as otherwise required by an applicable regulatory framework. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Access logs are periodically reviewed for unauthorized access attempts, use, security incidents, forensic purposes, and identified anomalous activities. A SIEM system is used to correlate logs and alert on security events for Intrusion Detection System events, firewall logs, and network flows.
Infrastructure & Virtualization Security: Change Detection	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	Oracle logs certain security-related activities on operating systems, applications, databases, virtual machines, 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.
	IVS-02.2	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	For CTMS Cloud Service, change controls are in place to ensure only approved changes are applied. Regular audits are also performed to confirm compliance with security and operational procedures.
	IVS-02.3	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	CTMS Cloud Service virtual machines are not moved. There is a new environment provisioned using the hardened master image with customer data migrated once the provisioning process is complete.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Infrastructure & Virtualization Security: Capacity / Resource Planning	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Network Time Protocol (NTP) is used for common time reference across the CTMS Cloud Service.
Infrastructure & Virtualization Security: Capacity / Resource Planning	IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Not Applicable. Oracle does not allow oversubscription of CTMS Cloud Service.
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	Not Applicable. Oracle does not allow oversubscription of CTMS Cloud Service.
	IVS-04.3	Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	Oracle collects and monitors capacity and utilization data. This data is used to plan for adequate capacity to meet current, projected, and anticipated needs and customer service level agreements.
	IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	During development, CTMS Cloud Service leverages a dedicated performance test team to conduct benchmarking, load testing, and defining the scalability requirements of the service. Oracle also uses a variety of software tools to monitor both the availability and performance of all customer environments, stage as well as production, and the operation of infrastructure and network components. These are used to ensure CTMS Cloud Service meets regulatory, contractual, and business requirements for all the systems used to provide services to customers. Before deploying Oracle cloud services, Oracle strongly recommends that cloud customers formally analyze their cloud strategy to determine the suitability of using the applicable Oracle cloud services in light of their own legal and regulatory compliance obligations. Making this determination remains solely the responsibility of customers. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
Infrastructure & Virtualization Security:	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization	Vulnerability assessment tools accommodate virtualization technologies.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Management - Vulnerability Management		technologies being used (e.g., virtualization aware)?	
Infrastructure & Virtualization Security: Network Security	IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	Not applicable for CTMS Cloud Service.
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	System and network changes go through change management, as well as security review. The network architecture diagrams are updated as needed when changes occur.
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	Firewall and other rulesets are reviewed regularly and updated as needed.
	IVS-06.4	Are all firewall access control lists documented with business justification?	System and network changes go through change management and a security review. Any updates to Access Control Lists would need business justification before being approved and implemented.
Infrastructure & Virtualization Security: OS Hardening and Base Controls	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	Oracle employs standardized system hardening practices for master images across CTMS Cloud Service devices. This includes restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, logging, antivirus, etc. Also, Oracle used hardened master images for provisioning services. This is a standard process for images deployed for CTMS Cloud Service.
Infrastructure & Virtualization Security: Production / Non-Production Environments	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	To customers upon request.
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on	Not applicable for CTMS Cloud Service.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		how to create suitable production and test environments?	
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	Production and non-production environments are logically and physically segregated. Additionally, procedures are in place to ensure production data is not used in nonproduction environments.
Infrastructure & Virtualization Security: Segmentation	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	CTMS Cloud Service operations teams access customer environments through a segregated network connection, which is dedicated to environment access control and isolated from Oracle's internal corporate network traffic. The dedicated network functions as a secure access gateway between support systems and target application and database servers. Both end-user/customer and operational traffic is managed, protected, and/or restricted with the service firewalls. These include the load balancers and edge routers.
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	Firewall access policies are implemented between: • Oracle Cloud networks and the public Internet • Oracle Cloud networks and Oracle Corporate networks. • Oracle Cloud production networks and Oracle Cloud development networks
	IVS-09.3	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	Not applicable for CTMS Cloud Service. Tenants do not have access to infrastructure or network components.
	IVS-09.4	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	CTMS Cloud Service is single-tenant and Oracle manages tenant's keys thereby allowing logically segmentations at the tenancy level.
	IVS-09.5	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	Firewall access policies are implemented between: • Oracle Cloud networks and the public Internet • Oracle Cloud networks and Oracle Corporate networks • Oracle Cloud production networks and Oracle Cloud development networks

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			In addition, all network traffic is denied unless explicitly permitted by a firewall rule (default deny practice).
Infrastructure & Virtualization Security: VM Security - Data Protection	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Customer configuration information (e.g., connection strings, application settings) supplied through the management portal is protected while in transit and at rest.
	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	Staging networks are segregated from production-level networks and utilized when migrating production data to virtual servers. Physical servers, applications, and virtual machines are not moved. There is a new environment provisioned using the hardened master image with customer data migrated once the provisioning process is complete.
Infrastructure & Virtualization Security: VMM Security - Hypervisor Hardening	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	Access to management functions is performed using a bastion server. Access is managed through a centralized program with multiple approvals based on role and function. VPN and two-factor authentication are used to access the bastion server. The bastion server has limited tools installed and the support personnel cannot add additional tools. Access and activity on the bastion server are logged and monitored, per Oracle policy.
Infrastructure & Virtualization Security: Wireless Security	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	The Oracle Wireless Network Policy guides the provision and use of wireless networks and connectivity to access the Oracle corporate network. Oracle IT manages wireless networks and monitors for unauthorized wireless networks. Network devices must be registered in an Oracle-approved information systems inventory per Oracle Information Systems Inventory Policy. This policy requires the inventory and documented ownership of all information systems processing critical and highly critical information assets throughout their lifecycle by means of an approved inventory system. For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	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).
	IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	The Oracle Wireless Network Policy guides the provision and use of wireless networks and connectivity to access the Oracle corporate network. Oracle IT manages wireless networks and monitors for unauthorized wireless networks.
Infrastructure & Virtualization Security: Network Architecture	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	Network architecture diagrams reflect network segments with additional compliance considerations.
	IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
Additional Comments for Control Domain above: N/A			
Interoperability & Portability:	IPY-01.1	Do you publish a list of all APIs available in the service and	Documentation about available APIs for Oracle CTMS Cloud Service is available at https://docs.oracle.com/en/industries/health-sciences/siebel-clinical/index.html

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
APIs		indicate which are standard and which are customized?	
Interoperability & Portability: Data Request	IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	CTMS Cloud Service allows users with appropriate privileges the ability to export and attach data in industry-standard formats.
Interoperability & Portability: Policy & Legal	IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	Cloud Services Hosting and Delivery Policies are available at https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	Not applicable for CTMS Cloud Service. Tenants do not have access to infrastructure or network components.
	IPY-03.3	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Cloud Services Hosting and Delivery Policies are available at https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
Interoperability & Portability: Standardized Network Protocols	IPY-04.1	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	Secure file transfer functionality is built on commonly used network access storage platforms and uses secured protocols for transfer, such as HTTPS, sFTP and Oracle approved versions of TLS. The functionality can be used to upload files to a secured location, most commonly for data import/export on the Oracle Cloud hosted service or downloading files at service termination.
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Customers are provided the network protocol information necessary to use the CTMS Cloud Service.
Interoperability & Portability:	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats	Not applicable. CTMS Cloud Service is a SaaS service.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Virtualization		(e.g., OVF) to help ensure interoperability?	
	IPY-05.2	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	Not applicable. CTMS Cloud Service is a SaaS service.
	IPY-05.3	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	Not applicable. CTMS Cloud Service is a SaaS service.
Additional Comments for Control Domain above: N/A			
Mobile Security: Anti-Malware	MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	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.
Mobile Security: Application Stores	MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	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.
Mobile Security: Approved Applications	MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	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.
Mobile Security	MOS-04.1	Does your BYOD policy and training clearly state which applications and applications	Oracle's Global Desktop Strategy (GDS) organization keeps anti-virus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. GDS is responsible for notifying internal Oracle system users of both any

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Approved Software for BYOD		stores are approved for use on BYOD devices?	credible virus threats and when security updates are available. GDS provides automation to verify anti-virus configuration. Oracle employees are required to comply with email instructions from the GDS organization 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.
	MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	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.
Mobile Security: Cloud Based Services	MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	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. An example program for managing the security of Oracle's architecture is the Corporate Security Solution Assurance Process (CSSAP). 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
Mobile Security: Compatibility	MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?	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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Mobile Security: Device Eligibility	MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full-disk encryption software on their laptops, except where approved for 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.
Mobile Security: Device Inventory	MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	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.
Mobile Security: Device Management	MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company 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.
Mobile Security: Encryption	MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full-disk encryption software on their laptops, except where approved for 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.
Mobile Security: Jailbreaking and Rooting	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	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.
	MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	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.
Mobile Security:	MOS-13.1	Does your BYOD policy clearly define the expectation of privacy,	Oracle policy requires the use of antivirus intrusion protection and firewall software on laptops and mobile devices. Additionally, all computers running a Windows

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Legal		requirements for litigation, e-discovery, and legal holds?	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.
	MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?	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.
Mobile Security: Lockout Screen	MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	Oracle's Global Desktop Strategy (GDS) organization keeps anti-virus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. GDS is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. GDS provides automation to verify anti-virus configuration. Oracle employees are required to comply with email instructions from the GDS organization and are responsible for promptly reporting to the Oracle employee helpdesk any virus or suspected virus infection that cannot be resolved by antivirus software.
Mobile Security: Operating Systems	MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	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.
Mobile Security: Passwords	MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	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. When Oracle compliance organizations determine that a password is not in compliance with strong password standards, they work with the applicable employee and line of business to bring the password into compliance with the standards.
	MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?	The use of passwords is addressed in the Oracle Password Policy. Oracle employees are obligated to follow rules for password length and complexity, and to keep their passwords confidential and secured at all times. Passwords may not be disclosed to unauthorized persons.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	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.
Mobile Security: Policy	MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	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.
	MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	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.
	MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	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.
Mobile Security: Remote Wipe	MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	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.
	MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	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.
Mobile Security: Security Patches	MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	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.
Mobile Security: Users	MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	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.
	MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	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.
Additional Comments for Control Domain above: N/A			
Security Incident Management, E-Discovery, & Cloud Forensics: Contact / Authority Maintenance	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	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.
Security Incident Management, E-Discovery, & Cloud Forensics: Incident Management	SEF-02.1	Do you have a documented security incident response plan?	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.
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	The Oracle Data Processing Agreement describes Oracle's obligations in the event of a personal information breach. Individual tenant service agreements may describe additional responsibilities during a security event. https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing
	SEF-02.4	Have you tested your security incident response plans in the last year?	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
Security Incident Management, E-Discovery, & Cloud Forensics: Incident Reporting	SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	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-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	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.
Security Incident Management, E-	SEF-04.1	Does your incident response plan comply with industry standards for	Reflecting the recommended practices in prevalent security standards issued by the International Organization for Standardization (ISO), the United States National

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Discovery, & Cloud Forensics: Incident Response Legal Preparation		legally admissible chain-of-custody management processes and controls?	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-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	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-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	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-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	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.
Security Incident Management, E-Discovery, & Cloud Forensics: Incident Response Metrics	SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	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-05.2	Will you share statistical information for security incident data with your tenants upon request?	Incident history is Oracle Confidential and is not shared externally.
Additional Comments for Control Domain above: N/A			
Supply Chain Management, Transparency, and Accountability:	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Data Quality and Integrity			associated with the malicious alteration of these products before purchase and installation by customers.
	STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	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.
Supply Chain Management, Transparency, and Accountability: Incident Reporting	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	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
Supply Chain Management, Transparency, and Accountability: Network / Infrastructure Services	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	See Oracle Cloud Hosting and Delivery Policies and Pillar documents: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	STA-03.2	Do you provide tenants with capacity planning and use reports?	Capacity planning information is Oracle Confidential and is not shared externally.
Supply Chain Management, Transparency, and Accountability: Provider Internal Assessments	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	See the pdf Oracle Supplier Information and Physical Security Standards PART D: COMPLIANCE AND ASSESSMENTS located on this page https://www.oracle.com/corporate/security-practices/corporate/supply-chain/suppliers-partners.html
Supply Chain Management, Transparency, and Accountability:	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is	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:

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Third Party Agreements		processed, stored, and transmitted?	• 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
	STA-05.2	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	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-05.3	Does legal counsel review all third-party agreements?	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-05.4	Do third-party agreements include provision for the security and protection of information and assets?	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.
	STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	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. Service-specific Pillar documents provide additional information about specific cloud services: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	A customer's order specifies the Data Center Region in which the services environment and storage of customer data will reside. Oracle provides production and test environments in the Data Center Region stated in the order. In the event of a disaster, the production service will be restored in the Data Center Region stated in the order.
	STA-05.7	Can you provide the physical location/geography of storage of a tenant's data upon request?	Customers can request the city and country for their cloud service instances.
	STA-05.8	Can you provide the physical location/geography of storage of a tenant's data in advance?	Customers should discuss available choices for locations of their cloud service instances with their account representative.
	STA-05.9	Do you allow tenants to define acceptable geographical locations	A customer's order specifies the Data Center Region in which the services environment and storage of customer data will reside. Oracle provides production and

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
		for data routing or resource instantiation?	test environments in the Data Center Region stated in the order. In the event of a disaster, the production service will be restored in the Data Center Region stated in the order.
	STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Oracle Privacy Policies are available at https://www.oracle.com/legal/privacy/ 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.
	STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	See Oracle Cloud Hosting and Delivery Policies and Pillar documents: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	STA-05.12	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	Lists of subprocessors for Oracle Cloud services are available in My Oracle Support (https://support.oracle.com) "Oracle General Data Protection Regulation (GDPR) Resource Center", article ID # 111.2. Agreements with subprocesors are Oracle Confidential.
Supply Chain Management, Transparency, and Accountability: Supply Chain Governance Reviews	STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Supply Chain Management, Transparency, and Accountability: Supply Chain Metrics	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	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-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	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-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	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-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Supplier SLA reporting is Oracle Confidential.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Oracle makes equivalent information available periodically in the form of various third-party audit and testing reports. These include, but are not limited to SOC 1, SOC 2, ISO, and third-party assessment/penetration test summaries when available.
	STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?	Customers can request SLA performance via their account representative. This may be a Services Project Manager or Customer Success Manager.
	STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?	CTMS Cloud Service tenants are responsible for data management policies and service level conflicts of interest in their environment.
	STA-07.8	Do you review all service level agreements at least annually?	Third-party supplier agreements, policies and processes are reviewed no less than annually.
Supply Chain Management, Transparency, and Accountability: Third Party Assessment	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	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. 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-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	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.
Supply Chain Management,	STA-09.1	Do you mandate annual information security reviews and	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Transparency, and Accountability: Third Party Audits		audits of your third party providers to ensure that all agreed upon security requirements are met?	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-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Oracle personnel conduct vulnerablity scans. In addition to vulnerability scans, Oracle personnel perform penetration tests of the production infrastructure. Only approved third-party vendors under Oracle oversight are utilized when additional resources are required.
Additional Comments for Control Domain above: N/A			
Threat and Vulnerability Management: Antivirus / Malicious Software	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	Oracle deploys anti-virus/anti-malware software on systems that are used by CTMS Cloud Service. CTMS Cloud Service Support and operations staff, along with all Oracle employees and contractors who provide Cloud Support, are required to use company approved laptop or desktop computers that have been equipped with additional controls that include antivirus and malware protection, disk encryption, VPN software, asset inventory management software, and logging software to reduce threat vectors and data privacy risks. All bastion hosts are configured to meet the Windows Server Security & Hardening Guide and the Enterprise Linux Security Standard and Hardening Guide (internal to Oracle). Hardening includes but is not limited to: ▪ Updating the OS with the latest approved security patches ▪ Disabling unnecessary services and policies ▪ Installing antivirus software ▪ Editing registry settings ▪ Disabling copy/paste and over 20 other functions to reduce data loss ▪ Setting inactivity timeouts ▪ Restricting the number of Remote Desktop sessions per user to 1
	TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	Security detection systems, including the Network Intrustion Detection System (NIDS), Anti-malware, and Distributed Denial of Service (DDoS) system are configured to auto-update at least every 24 hours.
Threat and Vulnerability Management:	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as	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 CTMS Cloud Service.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Vulnerability / Patch Management		prescribed by industry best practices?	
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Application-layer vulnerability scans are performed. CTMS Cloud Service code is reviewed and tested throughout the product development lifecycle. For more regarding the Oracle Software Security Assurance Program please see the following link: https://www.oracle.com/corporate/security-practices/assurance/
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Operating Systems-level vulnerability scans are performed at least monthly.
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	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
	TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	CTMS Cloud Service have a robust patch management solution designed to ensure that vulnerabilities are evaluated, and that corresponding patches are deployed across the environment computing devices, applications and systems. CTMS Cloud Service vulnerability severity is assessed based upon Common Vulnerability Scoring System (CVSS) scoring, and remediation timelines are based upon the assigned severity and possible business impact.
	TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	The Oracle Cloud Hosting and Delivery Policies describe the customer (tenant) security obligations. Also, the Oracle Data Processing Agreement includes the responsibilities of the data controller (tenant/customer) versus data processor (Oracle). Please see the Oracle Hosting and Delivery Policies located at https://www.oracle.com/contracts/cloud-services/ Please also see the Oracle Data Processing Agreement at https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Threat and Vulnerability Management: Mobile Code	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	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.
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	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.
Additional Comments for Control Domain above: N/A			

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