ORACLE

Artifical Intelligence Consensus Assessment Initiative Questionnaire (AI-CAIQ) v1 for Oracle SaaS Cloud Applications

January 2026 | Version 1.0

PURPOSE STATEMENT

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

The answers contained in this AI-CAIQ version 1.0 are related to specific Oracle cloud offerings as listed in the "Oracle cloud services in Scope" section below.

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

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

DISCLAIMER

The AI Cloud Assessment Initiative Questionnaire (AI-CAIQ) for Oracle SaaS Cloud Applications, 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 SaaS Cloud Applications. 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. Responses to the CAIQ are based on available information as of the date of submission.

ORACLE CLOUD SERVICES IN SCOPE

This document applies to the following Oracle SaaS Cloud Applications delivered as SaaS service deployed on OCI at Oracle data centers or third-party data centers retained by Oracle.

- Oracle Cloud Applications
  - Oracle Fusion Cloud Applications Suite
    - Enterprise Resource Planning (ERP) including Oracle Enterprise Performance Management (EPM)
    - Supply Chain & Manufacturing (SCM)
    - Human Capital Management (HCM)
  - Sales
  - Service
  - Marketing

AI CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (AI-CAIQ) VERSION 1

Control Domain: Audit & Assurance

Question ID	Consensus Assessment Question	Oracle Response
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle's Business Assessment & Audit (BA&A) is an independent global team that reviews key business risk management and compliance with Oracle policies, standards, and select laws across Oracle's Lines of Business. These policies extend to AI and ML. Risks or control gaps identified are confidential, tracked for remediation, and shared with executive leadership and the Board. Customer audit rights related to data processing are outlined in your agreement. Oracle SaaS Cloud Compliance oversees a SaaS Compliance Program with annual internal and external audits of SaaS Cloud Applications, which includes AI and ML systems, testing against industry standards like ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, PCI-DSS, and SOC reports. More information is available at https://www.oracle.com/corporate/cloud-compliance/
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually or upon significant changes?	Oracle SaaS Cloud Compliance control-related audit and assurance policies, procedures, and standards are reviewed at least annually. These reviews also include emerging AI and ML threats, regulatory changes, and new technology implementation.
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Oracle's Business Assessment & Audit (BA&A) is independent. Its operational activities and procedures are conducted at least annually in alignment with Institute of Internal Auditors (IIA) Standards. Oracle SaaS Compliance conducts audits and governance framework assurance assessments in accordance with SaaS Cloud Security Organization Standards for the professional practice of internal auditing. Also see A&A-01.1.
A&A-03.1	Are independent audit and assurance assessments performed in response to significant changes or emerging risks and according to risk-based plans and policies?	See A&A-01.1. Oracle's Business Assessment & Audit (BA&A) is independent. Its operational activities and procedures are conducted in alignment with Institute of Internal Auditors (IIA). Oracle SaaS Compliance conducts audits and governance framework assurance assessments to address risk-based audit plans on identifying, assessing, and prioritizing the highest risk areas within SaaS Cloud Applications. Risks are identified, rated, and discussed in accordance with the risks identified in the risk assessment report and mitigation activities are considered. For more information, see: https://www.oracle.com/corporate/cloud-compliance/

A&A-04.1	Is compliance verified with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Oracle SaaS Compliance identifies key audit compliance objectives relevant to SaaS Cloud Application standards, regulations, legal/contractual and statutory requirements, in addition any new controls introduced during the audit review period findings. SaaS Compliance Audit plans incorporate consistency to verify compliance to requirements including applicable standards and regulations governing AI and ML (e.g., EU AI Act, NIST AI Risk Management Framework (AI RMF))
A&A-05.1	Are Audit Management processes aligned with global auditing standards, defined and implemented to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, review of past reports and supporting evidence?	Oracle SaaS Compliance executes a standardization and management process that is defined and implemented to support and approve the Audit program development and strategy for SaaS Cloud Applications including AI-specific artifacts (data lineage, model cards, audit trails for LLM output where applicable).
A&A-06.1	Is a risk-based corrective action plan established, documented, approved, communicated, applied, evaluated, and maintained to remediate audit findings, regularly review, and report remediation status to relevant stakeholders?	Any key risks or control gaps (including AI/ML risk and controls gaps) identified by Oracle's Business Assessment & Audit (BA&A) during these reviews are tracked through remediation. Risk-based action plans to address audit findings are established, documented, and communicated to BA&A for approval by Oracle's Lines of Business with evaluation by BA&A.

Control Domain: Application & Interface Security

Question ID	Consensus Assessment Question	Oracle Response
AIS-01.1	Are policies and procedures for application security established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle Software Security Assurance (OSSA) is Oracle's comprehensive approach to integrating security throughout every stage of the product development lifecycle—including design, development, testing, and ongoing maintenance. This methodology applies to all Oracle products, whether deployed on customer premises or delivered via Oracle Cloud. The purpose of OSSA is to ensure that Oracle solutions help customers fulfill their security objectives while also offering a cost-effective ownership experience. For further details, please visit https://www.oracle.com/corporate/security-practices/assurance/ Oracle SaaS Cloud Applications follow the OSSA methodology and incorporate the Standards Secure Software Development Lifecycle (SSDLC). Additionally, the Oracle Corporate Security Solution Assurance Process (CSSAP) offers a

		centralized process for reviewing and approving compliance with security policies.
AIS-01.2	Are the policies and procedures for application security reviewed and updated at least annually or upon significant system changes?	Oracle SaaS Cloud Security standards and procedures follow the Oracle Corporate Security policies and are reviewed annually and updated as needed. AI-related application security controls are included in this review process.
AIS-02.1	Are baseline requirements for securing applications established, documented, and maintained?	Oracle requires Oracle Cloud services be deployed in a specific configuration, or a small number of configurations. The security of cloud configurations are planned from the design phase by the development team. The developers implementing the service need to be aware of the planned configuration. Testing is required to be performed on the product in this configuration, with predeployment tests performed in an environment identical to the production environment. Additionally, cloud development teams are required to deliver the service to cloud operations teams in a secured configuration. Use of containers, such as Docker and automated deployment pipelines, can help development teams satisfy this requirement. Baseline requirements for SaaS Cloud Applications including AI and ML modules are documented and maintained and extend to data security, model integrity and abuse resistance. Secure configurations are evaluated during security reviews, and security scans and testing is performed to check secure configurations of the services deployed.
AIS-03.1	Are technical and operational metrics defined and implemented in alignment with business objectives, security requirements, and compliance obligations?	Oracle SaaS Cloud maintains a set of technical and operational metrics to help meet business objectives, security requirements, and compliance obligations to define what should be implemented and when, including security compliance requirements.
AIS-04.1	Is a secure software development lifecycle (SDLC) process defined and implemented for application requirements analysis, planning, design, development, testing, deployment, and operation in accordance with security requirements defined by the organization?	Oracle products are developed with consistently high security assurance. To help developers avoid common coding mistakes, Oracle employs formal Secure Coding Standards. Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. All Oracle developers are required to be familiar with these standards and apply them when designing and building products. The coding standards have been developed over a number of years and incorporate best practices as well as lessons learned from ongoing vulnerability testing by Oracle's internal product assessment teams. The Secure Coding Standards are a key component of Oracle Software Security Assurance and following the requirements of the Standards is assessed throughout the supported life of all Oracle products. Oracle SaaS Cloud teams follow an SSDLC process and are required to take OSSA training which covers Oracle Secure Coding Standards. Compliance with Secure Coding Standards is being checked through various mechanisms during

		the SSDLC including security reviews, code reviews, and static code analysis and testing.
AIS-05.1	Is a testing strategy implemented, including criteria for acceptance of new information systems, upgrades, and new versions, to provide application security assurance, maintain compliance, and meet organizational delivery goals?	Security assurance analysis and testing assess security qualities of Oracle products against various types of attacks. There are two broad categories of tests: static and dynamic analysis. Static security analysis of source code is the initial line of defense used during the product development cycle. Oracle uses a commercial static code analyzer as well as a variety of internally developed tools, to catch problems while code is being written. Typically, analysis of these scan reports involves senior engineers from the product teams who are familiar with the product code, sorting out false positives from real issues and reducing the number of false positives. Dynamic analysis activity takes place during latter phases of product development because it requires that the product or component be able to run. Dynamic analysis is aimed at externally visible product interfaces and APIs and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing within Oracle. For more information, see https://www.oracle.com/corporate/securitypractices/assurance/development/analysis-testing.html. Oracle SaaS Cloud Security executes various security testing scenarios, using both static code and dynamic analysis tools as part of the manual and automated testing process, including security penetration tests on Oracle SaaS Cloud Applications.
AIS-05.2	Is automation applied where applicable and possible?	SaaS Cloud Security testing for SaaS applications including AI and ML use cases is automated wherever possible.
AIS-06.1	Are strategies and capabilities established and implemented for secure, standardized, and compliant application deployment?	Strategies and capabilities are defined and implemented to deploy new code for SaaS applications in a secure manner. Testing must be performed on the product with pre-deployment tests performed in an environment identical to the production environment. Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances.
AIS-07.1	Are processes defined and implemented to remediate application security vulnerabilities, automating remediation when possible?	Oracle SaaS Cloud Applications has defined metrics to monitor vulnerabilities as they are identified through remediation. The process which includes AI and ML vulnerabilities (e.g, poisoning, extraction) follows the Security Health Review and Vulnerability Management Advocacy Program to monitor all vulnerabilities through remediation. Security vulnerabilities are remediated through the build and release pipeline. All SaaS Cloud Application security updates are delivered through security patches, and this process is fully automated once a fix is available.
AIS-08.1	Is the input against adversarial patterns, failure patterns and unwanted behaviour, validated,	The Oracle Cloud and Fusion AI development teams identify and approve the specific data required for each feature, following data minimization principles. Only the data essential for training machine learning models is ingested, and

	filtered, modified, or blocked as necessary, according to organisational policies, applicable laws and regulations?	data is preapproved through the Oracle Corporate Security Solution Assurance Process (CSSAP). An initial bulk data ingestion occurs during setup, followed by incremental updates at intervals suited to the particular use case. Inputs to AI and ML use cases, are also filtered and validated for potential adversarial patterns or prompt attacks as per Oracle policy.
AIS-09.1	Is the output against adversarial patterns, failure patterns and unwanted behaviour, validated, filtered, modified, or blocked as necessary, according to organisational policies, applicable laws and regulations?	For each generative AI use case, prompts and data features are carefully engineered to reduce the risk of response "hallucinations" and to determine the output is relevant and useful. Oracle has established policies and practices that apply to the development and deployment of Oracle AI systems, including third-party models incorporated in our products and services. Additionally, the Guardrail Service reviews each large language model (LLM) response to determine it meets the specific requirements of the use case. This service evaluates factors such as accuracy, toxicity, sentiment, and repetitiveness. The Guardrail Service then provides a simple pass/fail result for each response.
AIS-10.1	Are processes, procedures and technical measures to secure APIs, including authorization flaws, API key management, regular security testing, defined, implemented and evaluated?	Dynamic analysis activity takes place during latter phases of product development because it requires that the product or component be able to run. Dynamic analysis is aimed at externally visible product interfaces and APIs and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing within Oracle. For more information, see https://www.oracle.com/corporate/securitypractices/assurance/development/analysis-testing.html. Oracle SaaS Cloud Security executes various security testing scenarios, using both static code and dynamic analysis tools as part of the manual and automated testing process, including security penetration tests on Oracle SaaS Cloud Applications. AI services and its APIs receive particular focus for potential AI-specific threats and potential failures as part of this process.
AIS-10.2	Are technical measures for any improvements reviewed and updated at least annually or after significant system changes?	Oracle SaaS Cloud Security standards and procedures follow the Oracle Corporate Security policies and are reviewed annually and updated as needed.
AIS-11.1	Are the security boundaries for agents established?	Oracle's data centers contain an isolated network environment used to deliver SaaS Cloud Services. Networking technologies are deployed in a layered approach designed to protect Your Content at the physical, data link, network, transport, database, and SaaS Cloud Service application levels. AI agents, models, and related AI and ML processes are partitioned using similar network and logical separation strategies, enabling customer and model isolation as per design. These include, but are not limited to, firewalls, routers with access control lists (ACLs), and load balancers. Access policies are deny-by-default. Only authorized traffic is allowed.
AIS-12.1	Are source code management practices, such as version control,	Oracle products including AI and ML code and data pipelines are developed with consistently high security assurance, and to help developers avoid

	code review and static code analysis, implemented and aligning with the SDLC process?	common coding mistakes, Oracle employs formal Secure Coding Standards. Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. All Oracle developers are required to be familiar with these standards and apply them when designing and building products. The coding standards have been developed over a number of years and incorporate best practices as well as lessons learned from ongoing vulnerability testing by Oracle's internal product assessment teams. The Secure Coding Standards are a key component of Oracle Software Security Assurance and following the requirements of the Standards is assessed throughout the supported life of all Oracle products. Oracle SaaS Cloud teams follow an SSDLC process and are required to take OSSA training which covers Oracle Secure Coding Standards. Compliance with Secure Coding Standards is being checked through various mechanisms during the SSDLC including security reviews, code reviews, and static code analysis and testing.
AIS-13.1	Are sandboxing techniques implemented to execute AI tools and plugins in isolated environments to prevent unintended interactions with critical systems or data and to limit the possibility of lateral movement?	The Oracle Fusion AI Platform is a multi-tenant environment, where each customer's data and trained ML models (for classic AI) remain completely isolated. No customer data is shared, mixed, or combined to train ML models, or to process GenAI requests. Pre-trained generative AI models (Large Language Models) are securely accessed by the Oracle Fusion AI Platform within a secure Oracle Cloud Infrastructure (OCI) environment (which may be outside of the local OCI region). Data does not persist in the Large Language Models, i.e., after a prompt is processed, no customer data is retained, and prompt data does not train the Large Language Model. Data processed within the Large Language Model is completely isolated, and no customer data is shared or combined. AI outcomes, predictions, and Gen AI responses are sent from a customer's Fusion AI Platform environment to the customer's Oracle Fusion Application via secure REST APIs via typical business workflows. Refer to "How do I override AI prompts for Oracle Fusion Cloud Applications", https://docs.oracle.com/en/cloud/saas/fusion-ai/aiaqa/how-do-i-override-oracle-ai-prompts-for-oracle-fusion-cloud-applications.html#u30256980
AIS-14.1	Are security measures implemented to protect cache systems in GenAI systems and services?	Oracle secures cache systems in GenAI services by enforcing access controls and authentication, encrypting data both at rest and in transit, and applying strict data minimization principles. Regulatory security reviews are regularly conducted to enable ongoing compliance. Additionally, role-based access controls are in place to limit access to only authorized users and services.
AIS-15.1	Are mechanisms implemented to enable the model to clearly distinguish user-provided input	In Oracle Fusion Cloud Applications, Generative AI requests are sent to large language models once the feature is enabled. This can occur either when a user provides input via the application UI or when the application automatically initiates a request based on user activity. Each request sends a pre-engineered, security-reviewed prompt and customer-specific context to the Fusion AI

	instructions from data and system instructions (e.g., system prompts)?	Platform Orchestration Service via REST API. Prompts and data features are designed to reduce hallucinations and enable relevant responses. Generally, prompts undergo Oracle Corporate Security Solution Assurance Process (CSSAP) review and are tested for vulnerabilities such as prompt injection and input boundary attacks.

Control Domain: Business Continuity Management & Operational Resilience

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

		https://www.oracle.com/corporate/security-practices/corporate/resilience-management/ Oracle SaaS Cloud Applications follow the RMRP operational services resilience attestation BC program and annual test performance. The SaaS Cloud Applications service level DR Kits, BIA, BC/DR plans, procedures, and QA testing is reviewed and approved at least annually, updated as needed during changes, and communicated to constituents. Tier-1 critical services are reviewed and approved quarterly.
BCR-02.1	Is the impact of business disruptions and risks determined to establish criteria for developing business continuity and operational resilience strategies and capabilities?	The RMRP Program is generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance. For more information about the program and requirements for Oracle Lines of Business, see https://www.oracle.com/corporate/securitypractices/corporate/resilience-management/ Oracle SaaS Cloud Services conducts a Risk Assessment and BIA that is reviewed annually. The service criticality analysis is reviewed bi-annually as established at the global RMRP level. To support the management and oversight of risk across all SaaS Cloud Applications, the SaaS Risk Management Program is aligned with standards that apply across all SaaS lines of business. The risk management framework (RMF) is maintained and updated by SaaS Cloud Security (SCS) Risk Management and implemented by management at all levels of SaaS.
BCR-02.2	Is the risk assessment and impact analysis, reviewed and updated at least annually or upon significant changes?	Oracle SaaS Cloud Services conducts a Risk Assessment and BIA that is reviewed annually. The service criticality analysis is reviewed bi-annually as established at the global RMRP level. To support the management and oversight of risk across all SaaS Cloud Applications, the SaaS Risk Management Program is aligned with standards that apply across all SaaS lines of business. The risk management framework (RMF) is maintained and updated by SaaS Cloud Security (SCS) Risk Management and implemented by management at all levels of SaaS.
BCR-03.1	Are strategies established to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions?	The RMRP PMO develops guidance as aids to LoB Risk Managers in managing their LOB's business continuity plans, testing and training procedures. The RMRP program requires all LOBs to: • Identify relevant business interruption scenarios, including essential people, resources, facilities and technology and AI and ML powered components. • Define business continuity plans and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Obtain approval of the plans from the LOB's executive For more information, see https://www.oracle.com/corporate/security-practices/corporate/resiliencemanagement/
BCR-04.1	Is a business continuity plan - based on the results of operational resilience strategies and capabilities -	Oracle SaaS Cloud Business Continuity Plan includes a routine Business Impact Assessment (BIA) and resilience strategies for the SaaS Cloud services. Oracle SaaS Cloud Applications relies on the Cloud Provider high availability

	established, documented, approved, communicated, applied, evaluated and maintained?	infrastructure for operational resiliency. The plan is reviewed and approved at least annually and updated as needed.
BCR-05.1	Is relevant documentation, both internal and from external parties, for supporting the business continuity and operational resilience programs, developed, identified, and acquired?	LOBs are required to annually review their business continuity plan with the objective of maintaining operational recovery capabilities, reflecting changes to the risk environment as well as new technology or revised business processes. Critical LOBs must: • Conduct a Business Impact Analysis that specifies a Recovery Time Objective and Recovery Point Objective (if appropriate to the function) and identifies the organization's business continuity contingencies strategy • Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Revise business continuity plans based on changes to operations, business requirements, and risks For more information, see https://www.oracle.com/corporate/security-practices/corporate/resiliencemanagement/ Oracle SaaS Cloud Business Continuity Plan and Disaster Recovery Plan includes a Business Impact Assessment, disaster scenarios, processes, risk assessment, and procedures for critical functions. The plans are reviewed and approved at least annually and updated as needed.
BCR-05.2	Is the documentation available to authorized stakeholders and reviewed at least annually or upon significant changes.?	Oracle SaaS Cloud Business Continuity and Disaster Recovery (BCDR) Program for Business Continuity (BC) and operational resilience documentation is available to authorized personnel and SaaS customers. The complete plan is an internal Oracle SaaS Cloud document. Assessment of the plan is available in the SOC 2 type 2 reports.
BCR-06.1	Is a structured approach to evaluate the effectiveness of the business continuity and operational resilience plans, followed at planned intervals or upon significant changes?	Oracle SaaS Cloud Business Continuity and Disaster Recovery (BCDR) Program has a regimented risk scenario testing cadence; including quarterly operational resilience table-top and an annual end-to-end quality assurance testing exercise. There are multiple testing exercises, including Global RMRP tabletop, service specific annual tabletop for Tier-2 services, and service specific 1 switchover/failover + 3 tabletop exercises for Tier-1 spread across quarters.
BCR-07.1	Are communication channels with all relevant stakeholders established and maintained in the course of business continuity and resilience procedures?	The internal Disaster Recovery Kit documentation includes a communication plan for each SaaS Service to be used during a crisis.
BCR-08.1	Are backups periodically performed?	Oracle periodically conducts SaaS Cloud backups of the customer's production data to minimize data loss in the event of an incident. The backup contains

		provisions for backup systems and configurations and data required to maintain operational resilience.
BCR-08.2	Is the confidentiality, integrity and availability of the backup, ensured and data restoration from backup verified for resiliency?	For integrity, backups are encrypted in transit and at rest. Backups are taken on Object Storage Service (OSS) which is driven by Oracle Identity and Access Management (IAM) policies providing for confidentiality and availability. SaaS Cloud Applications have implemented Recovery Manager (RMAN) to automate backups of customer data to maintain confidentiality and integrity of incremental backups that are taken daily/weekly. RMAN encrypts the backups, and they are stored at both the primary and DR data centers.
BCR-09.1	Is a disaster response plan to recover from natural and man-made disasters established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle SaaS Cloud DRP includes disaster scenarios. A communication plan is maintained and updated frequently with assessments based on periodic DR exercises. Oracle SaaS Cloud is required to conduct an annual review of plans with the objective of maintaining operational recovery capabilities reflecting changes to the risk environment, including natural and man-made disasters, as well as new or revised business processes.
BCR-09.2	Is the Disaster Response Plan updated at least annually or upon significant changes?	Oracle SaaS Cloud Disaster Recovery Plan (DRP) and procedures are reviewed, updated, and approved at least annually and updated as needed.
BCR-10.1	Is a structured approach to evaluate the effectiveness of the disaster response plan followed at planned intervals or upon significant changes, including, if possible, participation of local emergency authorities?	Oracle SaaS Cloud has a documented DR plan to perform annual testing to simulate disaster scenarios that model catastrophic events that may disrupt SaaS Cloud Application services. The DR plan and procedures are reviewed, updated at least annually, and updated as needed.
BCR-11.1	Are business-critical equipment supplemented with both locally redundant and geographically dispersed equipment located at a reasonable minimum distance in accordance with applicable industry standards?	Oracle maintains a redundant network infrastructure, including DNS servers to route between primary and secondary sites, network devices, and load balancers. Oracle cloud data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html. Oracle Cloud Infrastructure deploys a computing infrastructure designed to maintain service availability zones and continuity in the event of a disaster. Oracle Cloud Applications provides a set of high availability features, such as process death detection and restart, server clustering, server migration, cluster integration, Gridlink, load balancing, failover, backup and recovery, rolling upgrades, and rolling configuration changes, which protect an enterprise deployment from unplanned downtime and minimize planned downtime. These protection solutions include a standby site that is located in a different geographical location from the production site.

Control Domain: Change Control and Configuration Management

Question ID	Consensus Assessment Question	Oracle Response
CCC-01.1	Are policies and procedures for managing the risks associated with applying changes to assets owned, controlled or used by the organization, established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle SaaS Cloud follows an Information Security Standard aligned with risk management and security organization policies. Change management processes, based on industry best practices, govern both infrastructure and AI model deployments, enabling risk analysis is completed before new models are released.
CCC-01.2	Are the policies and procedures reviewed and updated at least annually or upon significant changes?	Oracle SaaS Cloud standards and procedures are reviewed annually and updated as needed.
CCC-02.1	Is a defined quality change control, approval and testing process incorporating baselines, testing and release standards, established, maintained and implemented?	Oracle SaaS Cloud Operation and Oracle Cloud Service Center (OCSC) for SaaS Cloud Applications establishes a standard change control process and includes approval and testing. A defined and developed testing strategy is executed for pre-production environments and post validation procedures. Automated tests and testing scenarios are predefined and updated as needed.
CCC-03.1	Is a change management procedure implemented to manage the risks associated with applying changes to assets owned, controlled or used by the organization?	Oracle SaaS Cloud Operation and Oracle Cloud Service Center (OCSC) for SaaS Cloud Applications change management process includes a documented risk assessment for internal and external assets and a risk plan that the change owner manages to address and mitigate risks throughout the change request process. Risks unique to AI models (data drift, poisoning, regulatory, etc.) are covered in these risk assessments.
CCC-04.1	Are procedures implemented and enforced to authorize the addition, removal, update, and management of assets owned, controlled, or used by the organization?	Oracle SaaS Cloud Security standards are in place to outline restrictions for adding, removing, and updating Oracle SaaS Cloud assets. All changes to assets are registered in the asset inventory and the relevant team can perform changes to the asset inventory. Changes to cloud production asset inventory are approved by the owner prior to the change and logged in the change management process. Technical restrictions are in place where safeguards are needed.
CCC-05.1	Are provisions included that limit changes directly impacting customer owned environments/tenants to explicitly authorized requests within service level agreements?	Oracle SaaS Cloud Operation and Oracle Cloud Service Center (OCSC) for SaaS Cloud Applications updates, upgrades, and planned maintenance windows are clearly communicated and followed to established service level agreements (SLA) for availability and performance for customers by leveraging the formal SaaS Cloud Change Management (CM) process.

CCC-06.1	Are change management baselines established for all relevant authorized changes on organization assets?	Oracle SaaS Cloud Change Management (CM) policies align with industry best practices. Baselines, which include AI service, code, models and configuration artifacts, are established and SaaS Cloud Security review for all relevant authorized changes, backup plans, notifications to customers, and testing in lower environments before implementing changes to production on Oracle SaaS Applications.
CCC-06.2	Is the change management baseline reviewed an updated at least annually or upon significant changes?	Oracle SaaS Cloud Change Management (CM) aligns with industry best practices. Baselines are established and SaaS Cloud Security review is conducted for all relevant authorized changes, backup plans, notifications to customers, and testing in lower environments before implementing changes to production on Oracle SaaS Applications.
CCC-07.1	Are detection measures with proactive notification implemented in case of changes deviating from the established baseline?	Oracle SaaS Cloud Operations and Oracle Cloud Service Center (OCSC) manage detection measures and notifications when a deviation exists within a SaaS Cloud application or infrastructure component, which includes monitoring unauthorized or anomalous changes related to AI/GenAI models. The process is automated by scanning all software components for security and coding standards and performed on a regular schedule to alert, monitor, and triage the event.
CCC-08.1	Is a procedure implemented (aligning with the requirements of GRC-04: Policy Exception Process) for the management of exceptions, including emergencies, in the change and configuration process?	An emergency change control procedure is in place for managing urgent change requests within SaaS Cloud Applications or infrastructure components.
CCC-09.1	Is a process defined and implemented to proactively roll back changes to a previous known good state in case of errors or security concerns?	Processes are in place to proactively roll back changes to a previously known "good state" to secure SaaS Cloud Applications. Standard operating procedures (SOP) define the steps to follow, including implementation, pre/peri/post validation, and rollback, as applicable.

Control Domain: Cryptography, Encryption & Key Management

Question ID	Consensus Assessment Question	Oracle Response
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle has formal cryptography, encryption, key management requirements, cryptographic algorithms and protocols. Compliance with these requirements is monitored by Oracle. Oracle products are required to use up-to-date versions of approved security-related implementations. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms. Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption

		when data is at rest (in storage) on laptops, devices, and removable media. For more information, see: https://www.oracle.com/corporate/securitypractices/corporate/data-protection/ Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption, cryptographic algorithms and key management. Oracle follows Oracle Software Security Assurance (OSSA) standards that align with industry best practices and NIST requirements, Oracle SaaS Cloud products and services are required to only use up-to-date versions of approved security-related implementations.
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually or upon significant changes?	Oracle Corporate Security policies (including policies that address cryptography, encryption, and key management) are reviewed annually and updated as needed.
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Oracle assigns a Security Lead who is responsible, along with the senior manager for their teams, for the security of SaaS Cloud Applications that defines, manages, and monitors their internal security assurance process functions of cryptography, encryption, and key management.
CEK-03.1	Is data protection, at-rest, in-transit and where applicable in-use, provided by using cryptographic libraries certified to approved standards?	Oracle follows Oracle cryptography standards. The security technologies outline standard cryptographic and key management procedures that support approved libraries designed to protect information assets at rest and in transit.
CEK-04.1	Are encryption algorithms utilized following industry standards for protecting data, based on the data classification and associated risks?	Oracle follows the approved Oracle Software Security Assurance (OSSA) standard, using appropriate encryption algorithms at rest and data in transit. For more information, see: https://www.oracle.com/corporate/securitypractices/corporate/data-protection/
CEK-05.1	Are standard change management procedures established to review, approve, implement, and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Oracle follows the approved product security Oracle Software Security Assurance (OSSA) standards for all security related mandatory changes to SaaS Cloud internal and external sources.
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for	Oracle follows the Oracle Software Security Assurance (OSSA) standards and procedures for Oracle Cloud SaaS products and services that employ approved encryption keys and defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use,

	downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	and replacement to protect SaaS Cloud Applications and services from malicious changes throughout their lifecycle.
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Representatives from Corporate Security and development organizations define recommended practices related to using and implementing cryptography in Oracle products, derived from frequent reviews of existing industry practices and current threat intelligence. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/governance/global-product-security.html. Oracle SaaS Cloud Information Security Risk Management Standard identifies potential SaaS information security risks, including cryptography, encryption, and key management through continued risk assessments on SaaS Cloud Applications, including risk visibility and risk remediation activities for all key management operations. Encryption algorithms and key lengths are monitored by the product security team and security operations center regularly to validate only appropriate and sufficient configuration is being used.
CEK-08.1	Are providers providing customers with the capability to manage their own data encryption keys?	Break Glass and Database Vault for Oracle SaaS Cloud Applications is an optional service that provides customers control over data encryption keys.
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure?	Oracle SaaS Cloud follows the Oracle Software Security Assurance (OSSA) approved standards and security technologies vulnerability handling process for protecting encryption and key management security vulnerability fixes on a risk prioritized basis. The key management systems are reviewed by accreditation auditors and are also reviewed by the product security team. The review includes vulnerability scans and configuration management according to SaaS Cloud Security and Privacy standards.
CEK-09.2	Are encryption and key management systems, policies, and processes audited preferably continuously but at least annually and after any security event?	Oracle SaaS Cloud Security follows the OSSA standards and procedures for encryption and key management system methods. The review includes vulnerability scans, pen testing, and configuration management by the product security teams and audited annually and updated as needed.
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Oracle SaaS Cloud Applications follows the Oracle standards and procedures for Key generation using Oracle approved implementations, methods, and parameters. Cryptographic key generations are used in accordance with the Global Product Security Secure Coding Standards and Cryptography and Directive and Approved Security Technologies Standards for Cryptographic Algorithms. These standards and procedures apply to cryptographic keys used for model payloads, protected AI inferencing, or LLM/GenAI use-cases.

CEK-11.1	Are cryptographic secrets and private keys that are provisioned for a unique purpose properly managed?	Oracle SaaS Cloud Applications do not provide or manage private keys; by default, environments are secured with Oracle-managed encryption keys. Private keys are the responsibility of the SaaS Cloud customer. For Oracle SaaS Fusion, customers who purchase the Oracle Break Glass add-on can use customer-managed keys, allowing them to provide and manage their own encryption keys. Oracle Enterprise Performance Manager offers a Bring Your Own Key (BYOK) option, which is not enabled by defult but as an add-on feature.
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks, and legal and regulatory requirements?	Cryptographic keys follow a rotation key management life cycle from generation, storage, distribution, use and destruction while maintaining integrity and confidentiality of SaaS Cloud Applications data. Cryptographic keys are revoked and removed before the end of the established cryptoperiod (when a key is known to have been compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions.
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures which include legal and regulatory requirement provisions?	Cryptographic key expiration and revocation are defined, implemented, and evaluated and revoked and replaced in the event the symmetric key, the asymmetric private key, and/or the password protecting the asymmetric private key have been compromised or no longer valid. Oracle SaaS Cloud Security follows the Oracle Software Security Assurance (OSSA) standards and procedures in accordance with the Oracle Software Security Assurance (OSSA) Key Management standards and guidance.
CEK-14.1	Are processes, procedures, and technical measures which include provisions for legal and regulatory requirements, defined, implemented and evaluated, to securely destroy cryptographic keys when they are no longer needed?	Oracle SaaS Cloud cryptographic key destruction processes and procedures and technical measures are defined and implemented to address key destruction and removal of unneeded keys in accordance with an automatic process and occurs when the customer and or entity is removed from the SaaS Cloud Applications.
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) defined, implemented, and evaluated, including provisions for legal and regulatory requirements?	Oracle SaaS Cloud follows Oracle Software Security Assurance (OSSA) key management lifecycle; key generation process to create keys in a pre-activated state. All key management processes, implementations and operations are defined, implemented, and include approved security technologies.

CEK-16.1	Are processes, procedures, and technical measures to monitor, review, and approve key transitions (e.g., from any state to/from suspension) defined, implemented, and evaluated including provisions for legal and regulatory requirements?	Oracle SaaS Cloud follows Oracle Software Security Assurance (OSSA) key management lifecycle services and automates the process of rotating, suspending, creating, and deleting keys to support the monitoring, review, and approval of key transitions.
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) defined, implemented, and evaluated including provisions for legal and regulatory requirements?	Cryptographic key expiration and revocation are defined, implemented, and evaluated and revoked and replaced in the event the symmetric key, the asymmetric private key, and/or the password protecting the asymmetric private key have been compromised or no longer valid. Oracle SaaS Cloud Security follows the Oracle Software Security Assurance (OSSA) standards and procedures in accordance with the Oracle Software Security Assurance (OSSA) Key Management standards and guidance.
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) defined, implemented, and evaluated including provisions for legal and regulatory requirements?	Oracle SaaS Cloud Security standards, including procedures and standards that address cryptography, encryption, and key management, support the key Management life cycle implementation to manage archived keys in a secure repository. Archived keys for AI/ML models (if used) are protected with least privilege and monitored.
CEK-19.1	Are processes, procedures, and technical measures to use compromised keys to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) defined implemented, and evaluated including provisions for legal and regulatory requirement?	Oracle SaaS Cloud standards and procedures use Additional Authenticated Data (AAD) to protect information that requires authentication. This approach supports common use cases and specific scenarios for SaaS Application services and features, and serves as a countermeasure aligned with NIST standards.
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) defined, implemented, and evaluated, including provisions for legal and regulatory requirement provisions?	Representatives from Corporate Security and development organizations define recommended practices related to using and implementing cryptography in Oracle products, derived from frequent reviews of existing industry practices and current threat intelligence. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/governance/global-product-security.html. Oracle SaaS Cloud Information Security Risk Management Standard identifies potential SaaS information security risks, including cryptography, encryption, and key management through continued risk assessments on SaaS Cloud Applications, including risk visibility and risk

		remediation activities for all key management operations. Encryption algorithms and key lengths are monitored by the product security team and security operations center regularly to validate only appropriate and sufficient configuration is being used.
CEK-21.1	Are key management system processes, procedures, and technical measures defined, implemented, and evaluated to track and report all cryptographic materials and status changes including provisions for legal and regulatory requirements?	Representatives from Corporate Security and development organizations define recommended practices related to using and implementing cryptography in Oracle products, derived from frequent reviews of existing industry practices and current threat intelligence. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/governance/global-product-security.html. Oracle SaaS Cloud Information Security Risk Management Standard identifies potential SaaS information security risks, including cryptography, encryption, and key management through continued risk assessments on SaaS Cloud Applications, including risk visibility and risk remediation activities for all key management operations. Encryption algorithms and key lengths are monitored by the product security team and security operations center regularly to validate that only appropriate configurations with sufficient key lengths are being used.

Control Domain: Datacenter Security

Question ID	Consensus Assessment Question	Oracle Response
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Oracle's Media Sanitization Policy specifies requirements including secure disposal of equipment and media used for data storage. This policy is established, documented, approved, communicated, and maintained. Oracle SaaS Cloud maintains Media Sanitization and Disposal procedures, and standards for the secure disposal of equipment used on SaaS managed systems, cloud storage, information in hard copy and on applicable electronic storage media that refers to Oracle SaaS customers' or vendors/suppliers, or on the personal hardware assets of Oracle SaaS users and contingent workers where confidential information is no longer required, and is enforced to protect from security threats that would compromise the retrieval and reconstruction of confidential information.
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Oracle SaaS Cloud applies data retention and disposal destruction in accordance with the SaaS Cloud Media Sanitization and Disposal standard, SaaS Cloud PI Data Protection standard, and procedures for managing and moving data during destruction.
DCS-01.3	Are all policies and procedures for the secure disposal of equipment used outside the organization's	Oracle Corporate Security policies (including policies that address secure disposal of equipment outside the organization's premises) are reviewed annually and updated as needed.

	premises reviewed and updated at least annually, or upon significant changes?	Oracle SaaS Cloud policies, procedures, and standards for the secure disposal of equipment used on SaaS managed systems, cloud storage, information in hard copy and on applicable electronic storage media that refers to Oracle SaaS customers' or vendors/suppliers, or on the personal hardware assets of Oracle SaaS users and contingent worker
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Oracle's Information Systems Inventory Policy requires that Line of Business (LOB) maintain accurate and comprehensive inventories of information systems, hardware and software. This policy is established, documented, approved, communicated, and maintained. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html. Third-party contractual agreements in accordance with the Oracle Supplier Information and Physical Security standards provide audit rights to verify the requirements meet relocation or transfer compliance. SaaS Cloud Applications customer data is deleted and irrecoverable as per any contractual agreements.
DCS-02.2	Are the written or cryptographically verifiable authorization required for relocation or transfer request?	Oracle SaaS Cloud Security requires SaaS Cloud Application customers to follow the cryptography guidance of relocation services by submitting a formal request in My Oracle Support (MOS). Only approved and authenticated customers have access to the portal.
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually, or upon significant changes?	Oracle Corporate Security policies (including policies that address the relocation or transfer of hardware, software, or data/information to any location) are reviewed annually and updated as needed. Oracle SaaS Cloud Security maintains Media Sanitization and Disposal standards, and third-party contractual agreements in accordance with the Oracle Supplier Information and Physical Security standards and are reviewed annually and updated as needed.
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, applied, evaluated and maintained?	Oracle Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/governance/global-physical-security.html. Procedure reviews are done by LOB Oracle SaaS Cloud Security maintains a Personnel Security Standard that is supported by the Oracle Physical Security policy that describes the requirements for maintaining a safe and secure work environment. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-physicalsecurity.html.
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms, and facilities) reviewed and updated	Oracle Corporate Security policies (including policies that address safe and secure working environments) are reviewed annually and updated as needed. Oracle SaaS Cloud Security Personnel Security Standard, including the Oracle

	at least annually, or upon significant changes?	Physical Security policy for maintaining a safe and secure work environment are reviewed annually and updated as needed.
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle SaaS Cloud Security maintains Information Protection standards and procedures that cover the handling and transmission of SaaS Cloud confidential information. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually, or upon significant changes?	Oracle Corporate Security policies (including policies that address the secure transportation of assets) are reviewed annually and updated as needed. Oracle SaaS Cloud Security Information Protection standards and procedures are reviewed annually and updated as needed.
DCS-05.1	Are the physical and logical assets (e.g. applications) classified and documented based on the organizational business risk?	Oracle's formal Information Protection Policy sets forth the requirements for classifying and handling public and confidential information. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html. Oracle SaaS Cloud Security Logical Access Controls policy, follows Oracle's formal Information Protection Policy standards that determine the classification scheme, based on SaaS Cloud Applications risk assessments, and documentation requirements for assets according to the sensitivity and criticality of information they store, transmit, and receive in SaaS Cloud Applications that contain confidential (restricted or highly restricted) information.
DCS-05.2	Is the assets' classification reviewed and updated at least annually or upon significant changes?	Oracle's formal Information Protection Policy sets forth the requirements for classifying and handling public and confidential information. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html.
DCS-06.1	Are all relevant physical and logical assets located at service provider sites catalogued and tracked within a secured system?	The Oracle Information Systems Inventory Policy requires that Lines of Business (LOB) maintain accurate and comprehensive inventories of information systems, hardware and software. Inventories must be managed within an approved inventory system. This policy defines required identifying attributes to be recorded for server hardware, software, data held on information systems, and information needed for disaster recovery and business continuity purposes. Oracle SaaS Cloud Security catalogues and tracks assets following the Oracle Information Systems Inventory Policy which requires accurate and comprehensive inventory of information systems, hardware, and software. Inventories must be managed within an approved inventory system. All system access is provisioned on a need-to-know basis.

DCS-06.2	Are catalogues reviewed and updated at least annually or upon significant changes?	The Oracle Information Systems Inventory Policy requires that Lines of Business (LOB) maintain accurate and comprehensive inventories of information systems, hardware and software. Inventories must be managed within an approved inventory system. This policy defines required identifying attributes to be recorded for server hardware, software, data held on information systems, and information needed for disaster recovery and business continuity purposes. Oracle SaaS Cloud Security catalogues and tracks assets following the Oracle Information Systems Inventory Policy which requires accurate and comprehensive inventory of information systems, hardware, and software. Inventories must be managed within an approved inventory system. All system access is provisioned on a need-to-know basis.
DCS-07.1	Are physical security perimeters designed and implemented to safeguard personnel, data, and information systems?	Oracle Global Physical Security uses a risk-based approach to physical and environmental security. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/governance/global-physical-security.html. Oracle SaaS Cloud provides assurance for physical security perimeters to safeguard personnel, data, and information systems in accordance with the Data Center Assessment Program. Oracle Cloud physical security secures data center perimeter to prevent unauthorized users to Oracle SaaS Cloud Applications information. The effectiveness of physical security controls is assessed and implemented by Global Physical Security. See: https://www.oracle.com/corporate/security-practices/corporate/physicalenvironmental.html.
DCS-08.1	Is equipment identification used as a method for connection authentication?	The Oracle Cloud Network Access (OCNA) VPN that Oracle staff use to connect to Oracle SaaS Cloud Applications uses both machine certificates and other identifiers to validate that the device is Oracle owned and provisioned before allowing access to resources. Oracle SaaS Cloud Application manages equipment identification in alignment with the ISO 27001 standard.
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Oracle has implemented the following protocols: • 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physicalenvironmental.html.
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors. Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises. Visitors are required to sign a visitor's register, be escorted and/or observed

		when they are on Oracle premises, and/or be bound by the terms of a confidentiality agreement with Oracle. Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving Oracle's employment must return keys/cards and key/cards are deactivated upon termination. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/physicalenvironmental.html.
DCS-10.1	Are datacenter surveillance systems at the external perimeter and at all the ingress and egress points, implemented, maintained, and operated to detect unauthorized ingress and egress attempts?	Oracle uses a mixture of 24/7 onsite security officers or patrol officers, depending on the risk/protection level of the facility. In all cases officers are responsible for patrols, alarm response, and recording of security incidents. Oracle has implemented centrally managed electronic access control systems with integrated intruder alarm capability and CCTV monitoring and recording. The access control system logs and CCTV recordings are retained for a period of 30-90 days as defined in Oracle's Record Retention Policy which are based on the facility's function, risk level and local laws. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physicalenvironmental.html.
DCS-11.1	Are data center personnel trained to safely manage adverse events, including but not limited to unauthorized ingress and egress attempts?	Personnel are trained in incident response and escalation procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/physical-environmental.html.
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Data centers hosting Oracle cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria. Oracle cloud service data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of a widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Personnel are trained in procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html.

DCS-13.1	Are data center environmental control systems designed to implement and maintain, and test for continual effectiveness of temperature and humidity conditions within accepted industry standards?	Data centers hosting Oracle cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria. Oracle cloud service data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of a widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Personnel are trained in procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html.
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Data centers hosting Oracle cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria. Oracle cloud service data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of a widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Personnel are trained in procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html.
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Data centers hosting Oracle cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat

		targets), standards compliance, and geopolitical considerations among other criteria. Oracle cloud service data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of a widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Personnel are trained in procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html.

Control Domain: Data Security and Privacy Lifecycle Management

Question ID	Consensus Assessment Question	Oracle Response
DSP-01.1	Are Security and Privacy Policies and Procedures established, documented, approved, communicated, applied, evaluated, and maintained for the classification, protection, preparation, and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level?	Oracle's information-asset classification determines corporate data-security requirements for Oracle-managed systems. Oracle policies provide global guidance for appropriate controls designed to protect corporate, cloud and customer data in accordance with the data classification. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/. Oracle SaaS Cloud maintains standards and procedures on data classification, protection, and handling throughout its data lifecycle, according to legal and regulatory requirements. Oracle SaaS Cloud follows Oracle's information asset classification policy that provides global guidance for appropriate controls designed to protect corporate, cloud, and customer data in accordance with the data classification. The Oracle Information Protection Policy sets forth the requirements for classifying and handling confidential information, including requirements for visual disclosure. The policy applies to all Oracle users and to all confidential information, whether the information belongs to Oracle, customers, or a third party.
DSP-01.2	Are Security and Privacy Policies and Procedures reviewed and updated at least annually?	Oracle policies (including policies that address data security and privacy) are reviewed annually and updated as needed. Oracle SaaS Cloud security standards and procedures for data security and privacy are reviewed annually and updated as needed.
DSP-02.1	Are industry-accepted methods applied for securely disposing of data from storage media so that it is not recoverable by any forensic means?	Oracle SaaS Cloud employs industry accepted methods are for secure data disposal from storage media. Oracle's media sanitation and disposal policy defines requirements for removal of information from electronic storage media

		and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data.
DSP-03.1	Are data inventories created and maintained at least for any sensitive, regulated, and personal data?	Oracle requires Oracle SaaS Cloud to document and maintain data inventories and data flows. This documentation is for internal use only. The customer is responsible for creating their data inventory.
DSP-03.2	Are inventories reviewed and updated at least annually or upon significant changes?	Oracle requires Oracle SaaS Cloud to document and maintain data inventories and data flows. This documentation is for internal use only. The customer is responsible for creating their data inventory.
DSP-04.1	Are data classified according to its type and sensitivity level?	Oracle categorizes information into four classes-Public, Internal, Restricted, and Highly Restricted-with each classification requiring corresponding levels of security controls, such as encryption requirements for non-Public data. For more information, see: https://www.oracle.com/corporate/securitypractices/corporate/information-assets-classification.html.
DSP-05.1	Are data flow documentation created to identify what data is processed, stored, or transmitted where?	Oracle SaaS Cloud Services documents the flow of customer PI through the product or service. The diagrams include details such as inbound and outbound SaaS Cloud customer traffic, ports and protocols, customer roles (such as end user & admin), data flows through the application, static data stores (such as SFTP servers and storage), and email gateways where applicable. All Oracle SaaS Cloud services provide this documentation during the Corporate Security Solutions Assurance Process (CSSAP) and/or upon request.
DSP-05.2	Are data flow documentation reviewed at defined intervals, at least annually, and after any change?	Oracle SaaS Cloud Data Flow documentation is reviewed at least annually and updated as needed.
DSP-06.1	Are ownership and stewardship of all relevant personal and sensitive data documented?	Oracle's Information Systems Asset Inventory policy requires that SaaS Cloud Security maintain accurate and comprehensive inventories of information systems, hardware, and software. Ownership and stewardship of all relevant personal and sensitive data is documented. The customer is the controller of their data.
DSP-06.2	Are reviews performed at least annually for the documented ownership and stewardship of all relevant personal and sensitive data?	Oracle SaaS Cloud customers own their data and manage access to their SaaS Cloud Applications. Oracle SaaS Cloud standards that address ownership and stewardship are reviewed annually and updated as needed.
DSP-07.1	Are systems, products, and business practices developed based upon a principle of security by design and industry best practices?	Oracle SaaS Cloud Services are based on the ISO/IEC 27001/27017, including other security standards that define security principles by design best practices for SaaS Cloud Applications. For more information, see: https://www.oracle.com/corporate/cloud-compliance/
DSP-08.1	Are systems, products, and business practices developed based upon a	Oracle SaaS Cloud Services are based on the ISO/IEC 27002, including other privacy standards that define principles by design best practices for SaaS Cloud

	principle of privacy by design and industry best practices?	Applications. For more information, see: https://www.oracle.com/corporate/cloud-compliance/
DSP-08.2	Are systems' privacy settings configured by default, according to all applicable laws and regulations?	Oracle SaaS Cloud privacy settings are configured following a Privacy by Design (PbD) methodology and according to applicable default privacy standards, laws, and regulations. Oracle SaaS Cloud adopts Privacy by Design (PbD) best practices. AI services restrict use of personal information (PI) to the explicit purposes stated in documentation and contracts, including controls for prompt/response data.
DSP-09.1	Are Data Protection Impact Assessments (DPIAs) conducted to evaluate the origin, nature, particularity, and severity of the risks upon the processing of personal data, according to any applicable laws, regulations, and industry best practices?	Oracle SaaS Cloud performs security and privacy impact assessments (PIAs) for all new products and system feature enhancements we wish to bring to market. Oracle legal teams perform Data Privacy Impact Assessments (DPIAs) in accordance with the Oracle Services Privacy Policy.
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated that implement any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations?	SaaS Cloud Corporate Single Sign-On standard sets forth the requirements to implement proper authentication and identity management for SaaS Cloud users when accessing Oracle SaaS Cloud environments. The standard includes requirements for application authentication and specific user requirements to protect unauthorized access of personal information (PI) or sensitive data. Oracle SaaS Cloud Services follows the Oracle Cloud – PI Data Protection Standard and procedures, as part of the privacy-by-design framework. Oracle Cloud Services provide functionality where a customer can restrict or object to the use of or transfer of customer PI. Please refer to the Data Processing Agreement for the definition of Personal Information (PI) - https://www.oracle.com/contracts/cloud-services/
DSP-11.1	Are processes, procedures, and technical measures defined and implemented to enable data subjects to request access to, modify, or delete their personal data according to applicable laws and regulations?	Oracle SaaS Cloud Services follows the Oracle Cloud – PI Data Protection Standard and procedures, as part of the privacy-by-design framework. Oracle Cloud Services provide functionality that enables customers to securely process data subject requests—such as accessing, modifying, or deleting personal data (including rectification, correction, or erasure) applicable to security, privacy, and regulatory requirements.
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure that personal data is processed according to applicable laws and regulations and for the purposes declared to the data subject?	SaaS Cloud Corporate Single Sign-On standard sets forth the requirements to implement proper authentication and identity management for SaaS Cloud users when accessing Oracle SaaS Cloud environments. The standard includes requirements for application authentication and specific user requirements to protect unauthorized access of personal information (PI) or sensitive data. Oracle SaaS Cloud Services follows the Oracle Cloud – PI Data Protection Standard and procedures, as part of the privacy-by-design framework. Oracle Cloud Services provide functionality where a customer can restrict or object to

		the use of or transfer of customer PI. Oracle SaaS Cloud Services follows the Oracle Cloud – PI Data Protection Standard and procedures, as part of the privacy-by-design framework. Oracle Cloud Services provide functionality that allows customers to securely process data subject requests—such as requests to access, modify, or delete personal data (including rectification, correction, or erasure) applicable to security, privacy, and regulatory requirements. Please refer to the Data Processing Agreement for the definition of Personal Information (PI) - https://www.oracle.com/contracts/cloud-services/
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for transferring and sub-processing personal data within the service supply chain according to applicable laws and regulations?	Please see the Oracle privacy policies at https://www.oracle.com/legal/privacy/ Oracle SaaS Cloud has processes, procedures, and technical measures in place for the transfer and sub-processing of personal data within the service supply chain. Oracle and Oracle Affiliates employees, as well as any third-party sub-processors that process personally identifiable information (PII), are subject to appropriate written confidentiality agreements, including regular training on information protection, and compliance with Oracle policies concerning protection of confidential information. Established privacy risk assessments evaluate the transfer and sub-processing of personal data within the SaaS Cloud service. Please refer to the Data Processing Agreement for Personal Information (PI) Definition - https://www.oracle.com/contracts/cloud-services/
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose the details of any personal or sensitive data access by sub-processors to the data owner before initiating that processing?	Oracle SaaS Cloud Services follows the Oracle Cloud – PI Data Protection Standard and procedures, as part of the privacy-by-design framework. Oracle SaaS Cloud Services follows the Data Processing Agreement regarding third-party vendors or sub-processors that process customer personal information. Oracle affiliates and third-party sub processors have access to services personal information to assist in the provision of services, such sub-processors shall be subject to the same level of data protection and security as Oracle under the terms of your order for services. Oracle is responsible for its sub-processors' compliance with the terms of your order for services. For more information, see: https://www.oracle.com/legal/privacy/services-privacy-policy/
DSP-15.1	Are authorizations obtained from data owners and associated risks managed before replicating or using production data in non-production environments?	In Oracle SaaS Cloud production data is not replicated to or used in non-production environments. Oracle will not use customer data in non-production environments or for testing purposes. Oracle SaaS cloud production and non-production environments are logically and physically segregated. Additionally, procedures are in place to help ensure production data is not used in non-production environments. Oracle SaaS Cloud customers may request a Production to Test (P2T) copy and data can be masked using Oracle's Data Masking solution to prevent sensitive data being used in the test environment

DSP-16.1	Are data retention, archiving, and deletion managed per business requirements, applicable laws, and regulations?	Oracle SaaS Cloud customers maintain responsibility for their data residing in their environment. SaaS Cloud can be configured by the customer to meet their objectives for data retention, archiving and deletion practices per their business requirements, applicable laws, and regulations. During the use of Oracle SaaS Cloud Applications, Oracle Cloud customers maintain responsibility for their data residing in their environment. Oracle SaaS Cloud Services provide a variety of configurable controls as part of the subscribed service.
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Oracle SaaS Cloud standards, procedures, and technical measures are defined and implemented to help protect sensitive data throughout its lifecycle. The customer remains solely responsible for their user access to the service provided. During the use of Oracle SaaS Cloud Applications, Oracle Cloud customers maintain responsibility for their data residing in their environment. Oracle SaaS Cloud Services provide a variety of configurable information protection services as part of the subscribed service.
DSP-18.1	Are the procedures to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations, implemented and described to the customers by the providers?	Oracle SaaS Cloud Services will promptly inform the SaaS Cloud customer of requests to provide access to Personally Identifiable Information (PII), unless otherwise required by law, for more information see Oracle Cloud Services Contracts – OCI -Privacy Documents: https://www.oracle.com/contracts/cloud-services/ Please refer to the Data Processing Agreement for Personal Information (PI) Definition - https://www.oracle.com/contracts/cloud-services/
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document the physical locations of data, including any locations where data is processed or backed up?	Oracle SaaS Cloud has processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locations where data is processed or backed up, for more information see Oracle Cloud Services Contracts - OCI - Privacy Documents: https://www.oracle.com/contracts/cloud-services/
DSP-20.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to: 1) Document and trace data sources, and 2) Make the data source available according to legal and regulatory requirements	As with all Oracle products and services, our development lifecycle for AI systems is subject to a governance framework that applies from the planning phase through implementation. For example, new AI systems undergo an initial technical review to assess their intended use, training data, accuracy, fairness, transparency, privacy, security, human control, and other factors as applicable. This detailed review helps us better understand the potential benefits and implications of an AI system, identify associated risks and mitigations, and promote informed decision-making and responsible behavior from the outset. These processes, procedures, and technical controls are defined, implemented, and evaluated to document and trace data sources and make them available in accordance with legal and regulatory requirements.
DSP-21.1	Are processes, procedures and	Oracle SaaS Cloud Applications takes a proactive approach to securing AI systems against data poisoning and backdoor attacks. Our comprehensive

	technical measures to prevent data poisoning in AI models and continuously detect such, defined, implemented and evaluated?	security strategy is designed to address these threats during the AI model training process: Preventing Data Poisoning through Data Isolation: Our Fusion AI Platform is built with a multi-tenant architecture, ensuring complete data isolation. Each customer's data and trained ML models are kept separate, preventing any data mixing or sharing that could lead to data poisoning. Data Minimization: For Classic AI, we follow the principle of data minimization. We only ingest the necessary data, pre-approved through our rigorous Oracle Corporate Security Solution Assurance Process (CSSAP) review, reducing the risk of poisoning attacks. Secure Coding Standards: Oracle's product development teams follow to the Secure Coding Standards (SCS), which include specific directives for AI/ML security. These standards cover AI governance, infrastructure, development, and data security, enabling us to identify and mitigate potential risks effectively.
DSP-22.1	Are Privacy Enhancing Technologies (PET) used for training data informed by risk and privacy impact analysis and business use cases?	Predictive AI (Classic AI) uses machine learning models trained on each customer's data within their own secure tenancy, with data minimization, and strict tenant isolation applied as needed based on risk and privacy assessments. In contrast, Generative AI relies on pre-trained foundational large language models, and Oracle evaluates and implements privacy controls and regulatory safeguards continuously to address evolving risks, privacy impacts, and business requirements where applicable. For Generative AI, a single provisioned large language model (LLM)–pre-trained by a trusted LLM provider for multiple customers, and Oracle applies rigorous privacy controls and regulatory safeguards to help protect input and output data. The implementation of Privacy-Enhancing Technologies (PETs) and other technical and procedural safeguards are evaluated and adapted as needed, based on risk, privacy impact assessments, and evolving business use cases to help ensure data is handled in a manner compliant with Oracle's privacy and security policies where applicable.
DSP-23.1	Is the consistency and conformity of training, fine-tuning or augmentation data regularly validated?	Architecturally Generative AI is rather different to Predictive AI. There is a single provisioned LLM (actual LLM used may vary between Use Case Patterns as the state of art evolves), rather than one model per customer as in the Predictive AI architectural pattern. This model has been pre-trained by the LLM provider, and is otherwise known as a Foundational Model. The LLMs used by Fusion SaaS Applications, specifically features classed as Agentic AI, will make use of OpenAI GPT-4.1 mini model (as of 25C release) which is hosted by OpenAI itself. Customers, if they prefer, can utilize the Llama model which is hosted in OCI. From Fusion 25D release onwards Oracle offers the ability for customers to bring their own models which may or may not be hosted within OCI. These Foundational Models are not further fine-tuned on customer data. In addition, it is important to note that no customer data (formed as part of a Prompt/Response) is employed within the Large Language Model or used to further tune and refine future LLM responses.

DSP-23.2	Is dataset versioning to ensure traceability implemented and are restrictions to prevent unauthorized changes, enforced?	Oracle SaaS implements dataset versioning for data ingested from Oracle Fusion Cloud Applications for traceability of training data throughout its lifecycle. Access to ingested datasets is tightly controlled with tenant-specific buckets in OCI Object Store, and role-based permissions. Data ingestion and versioning procedures are subject to Oracle's standard security review processes, for compliance with corporate security architecture standards.
DSP-24.1	Is training-data differentiation and relevance to the intended use of the AI Model, ensured?	There are two areas of AI that need to be considered, classic and generative AI. In the case of classic AI models that have been developed by Oracle SaaS to meet a specific set of requirements (e.g., account code combination prediction), Oracle SaaS provides training-data differentiation and relevance to the intended use of each AI model. During model training, data is read from the OCI Object Store, and data appropriate to the use case may be included in the training flow. Data flows and retraining are closely monitored for data quality and relevance, while model endpoints are deployed on OCI Data Science Service infrastructure. In the case of generative AI models that Oracle OCI hosts, the training data used for these types of models is more generic in nature e.g., training data is collected from multiple web sites, document sources, etc. The training of these models is the responsibility of the model providers, who are responsible for the training of their 'command' models.

Control Domain: Governance, Risk and Compliance

Question ID	Consensus Assessment Question	Oracle Response
GRC-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for an information governance program that is sponsored by the leadership of the organization and related to AI systems as well?	Corporate Information Security Policie are defined for the Line of Business management of information security across Oracle. Additionally, sets direction and provides advice to help protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners and employees. Also coordinates the reporting of information security risk to senior leadership such as the Oracle Security Oversight Committee and Board of Directors. Oracle Security manages programs and directly advises on the protection of data developed, accessed, used, maintained, and hosted by Oracle. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-informationsecurity.html. The SaaS Cloud Information Security Governance program defines standards and procedures that are reviewed and approved by organizational leadership to guide the development and maintenance of a comprehensive information security program.
GRC-01.2	Are policies and procedures for information governance program and	Oracle Corporate Security policies (including policies that address governance, risk, and compliance) are reviewed annually and updated as needed. Oracle

	related to AI systems reviewed and updated at least annually?	SaaS Cloud Security standards and procedures are reviewed on an annual basis and updated as needed.
GRC-02.1	Is a formal, documented, and leadership-sponsored AI risk management (AIRM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of risks, established and maintained?	Oracle Security manages the security departments, and collaborates with other Oracle teams to guide security controls at Oracle. These departments drive the corporate security programs, define corporate security policies, and provide security assurance oversight for Lines of Business. The Corporate Security Architecture manages a cross-organization working group focused on security architecture of corporate and cloud systems. Participation includes members from cloud service development, operations, and governance teams. Each Line of Business is responsible implementing associated procedures. Oracle Privacy & Security Legal manages the cross-organization oversight of privacy risks. For more information, see https://www.oracle.com/legal/privacy/
GRC-03.1	Are relevant organizational policies and associated procedures reviewed at least annually or when a substantial change within the organization, occurs?	Oracle Corporate Security policies are reviewed annually and updated as needed. The SaaS Cloud Information Security Standards are reviewed and updated annually, including when a substantial organizational change occurs.
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Oracle Security manages a security exception program which oversees LOB exception and exception management activity. The SaaS Cloud Information Security Governance program follows a standard process to identify, report, and manage deviation from SaaS Information Security Standards. Approved exceptions are managed, logged, and tracked when there are deviations.
GRC-05.1	Is an Information Security Program that includes programs for all the relevant domains of the AICM developed and implemented?	Oracle SaaS Cloud compliance program implements CCM domains are mapped to SaaS Cloud Applications and is CSA STAR certified. For more information, see https://www.oracle.com/corporate/cloudcompliance/
GRC-06.1	Are roles and responsibilities defined and documented for planning, implementing, operating, assessing, and improving governance programs?	Oracle SaaS Information Security Governance defines Roles and Responsibilities for planning, implementing, operating, assessing, and improving information security programs that are documented in SaaS Information Security Standards and supported by Corporate Information Security Policies.
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements, applicable to your organization, identified and documented?	Oracle SaaS Security standards, regulations, legal/contractual, and statutory requirements are identified and documented. The customer remains solely responsible for its regulatory compliance in its use of any Oracle SaaS Cloud Applications. The customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
GRC-07.2	Are all relevant standards, regulations, legal/contractual and statutory requirements reviewed and	Oracle Corporate Security policies (including policies that address governance, risk, and compliance) are reviewed annually and updated as needed. Oracle

	updated at least annually or when a substantial change occurs within the organization?	SaaS Cloud Security standards and procedures are reviewed on an annual basis and updated as needed.
GRC-08.01	Is contact established and maintained with related special interest groups and other relevant entities in line with business context?	Oracle is an Information Technology-Information Sharing and Analysis Center (IT-ISAC) organization. For more information, see https://www.it-isac.org/home and https://openssf.org/about/members/
GRC-09.1	Are policies and procedures defined, documented, and enforced for the acceptable use of AI services offered by the organization?	As with all Oracle products and services, our development lifecycle for AI systems is subject to a governance framework that applies from the planning phase through implementation. For example, new AI systems undergo an initial technical review to assess their intended use, training data, accuracy, fairness, transparency, privacy, security, human control, and other factors. This detailed review helps us better understand the potential benefits and implications of an AI system, identify associated risks and mitigations, and promote informed decision-making and responsible behavior from the outset.
GRC-09.2	Is effectiveness of the acceptable use of AI services policies and procedures evaluated by continuous risk assessments, reviews, and human oversight?	The effectiveness of our acceptable use of AI services policies and procedures is continuously evaluated through ongoing risk assessments, technical reviews, and required human oversight at every stage of the AI development lifecycle. Oracle's governance framework, including the Corporate Security Solution Assurance Process (CSSAP) implements regular review and adaptation of policies in alignment with evolving laws, industry standards, and AI risks. Post-deployment, we maintain monitoring, reporting channels, and oversight mechanisms to implement continual compliance, quality, and responsible use of AI services.
GRC-10.1	Is an AI Impact Assessment process and its criteria to regularly evaluate the ethical, societal, operational, legal, and security impacts of the AI system throughout its lifecycle, established, documented, and communicated to all relevant stakeholders?	During the design, build, testing, and maintenance of the AI Services, Oracle will comply with the Oracle Software Security Assurance methodology (OSSA) described in the Oracle Corporate Security Practices (part of the Service Specifications), including the OSSA product feature and quality testing and secure coding principles. We have established policies and practices that apply to the development and deployment of Oracle AI systems, including third-party models incorporated in our products and services. These policies and practices are aligned with applicable laws, regulations, and industry standards. Given the fast-paced nature of AI technological progress and legal, regulatory, and industry developments, we are frequently evaluating and updating these policies and practices.
GRC-11.1	Are AI systems, models, datasets & algorithms regularly evaluated for bias and fairness to ensure compliance with ethical standards?	As with all Oracle products and services, our development lifecycle for AI systems is subject to a governance framework that applies from the planning phase through implementation. For example, new AI systems undergo an initial technical review to assess their intended use, training data, accuracy, fairness, transparency, privacy, security, human control, and other factors. This detailed review helps us better understand the potential benefits and

		implications of an AI system, identify associated risks and mitigations, and promote informed decision-making and responsible behavior from the outset.
GRC-12.1	Is an ethics committee established to review AI applications, ensuring alignment with ethical standards and organizational values?	Oracle uses a comprehensive governance framework to align AI applications with ethical standards and organizational values. Oracle's Corporate Security Solution Assurance Process (CSSAP) and cross-functional oversight from teams in Security Architecture, Product Security, IT, Legal, and others, provide collaborative review throughout the AI development lifecycle. Additionally, universal Codes of Ethics and Business Conduct reinforce Oracle's commitment to ethics across all employees, partners, and suppliers
GRC-13.1	Is the degree of explainability required for the AI Services established, documented, and communicated?	Yes, the degree of explainability required for AI Services is clearly documented and communicated. Features and their underlying workings are detailed in our publicly available product documentation at docs.oracle.com (https://docs.oracle.com), supplemented by demos and transparent user interfaces. Customers have access to explanations of AI feature functionality, helping them understand and effectively leverage Oracle AI Services
GRC-14.1	Is the degree of explainability of the AI Services evaluated, documented, and communicated, including possible limitations and exceptions?	The degree of explainability for Oracle AI Services is regularly evaluated, documented, and clearly communicated. Comprehensive product feature documentation—including details on explainability, any limitations, and exceptions—is publicly available at docs.oracle.com (https://docs.oracle.com) with additional clarity provided through demos and transparent user interfaces.
GRC-15.1	Are processes, procedures, and technical measures to ensure human oversight and control of the AI system in compliance with regulatory requirements and organizational risk management, established, executed and assessed?	Oracle Fusion AI features within Oracle Fusion Cloud applications can be enabled simply and quickly by the customer, and do not require outside system integrator assistance to set up. Each AI feature can be enabled or disabled (see Oracle Help Center documentation for setup and enable/disable instructions for an individual Fusion AI feature). Fusion Applications implement Large Language Models (LLMs) that have been specifically selected by Product Development to produce the best results for the shipped AI Feature Patterns. In addition to the hosted LLMs, Fusion also utilizes an Embedding's model which is used for the RAG (Retrieval Augmented Generation) Interactive Q&A flows.

Control Domain: Human Resources

Question ID	Consensus Assessment Question	Oracle Response
HRS-01.1	Are new employee background verification policies and procedures (including but not limited to remote employees, contractors, and third	In accordance with Oracle policy, background checks are required for individuals being considered for employment. For more information, see https://www.oracle.com/corporate/careers/backgroundcheck.html. The Oracle Recruiting Privacy Policy describes the privacy and security practices of Oracle

	parties) established, documented, approved, communicated, applied, evaluated, and maintained?	when collecting, using and handling (processing) personal information about job applicants in connection with our online and offline recruitment activities. It also explains the choices candidates have in relation to these processing activities, see https://www.oracle.com/legal/privacy/recruiting-privacy-policy/.
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	In accordance with Oracle policy, background checks are required for individuals being considered for employment. For background check information organized by local law and regulation, see https://www.oracle.com/corporate/careers/background-check.html.
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Oracle Human Resources policies (including policies that address candidate and employee background checks) are reviewed annually and updated as needed. Oracle's SaaS Cloud security standard policies for candidates and employee background checks are reviewed annually and updated as needed.
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle's Acceptable Use Policy (AUP) guides the use of organizationally owned or managed assets. Employees must sign a confidentiality agreement as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/human-resources-security.html. Oracle SaaS Cloud Personnel Security Standard dictates that employees maintain the confidentiality of customer data, including SaaS physical and network access requirements. All employees are responsible for understanding and following corporate policies and SaaS standards.
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Oracle SaaS Cloud Personnel Security Standards are reviewed annually and updated as needed.
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs and are required by company policy. For more information see https://www.oracle.com/corporate/securitypractices/corporate/human-resources-security.html.

HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Oracle SaaS Cloud Personnel Security Standard provides key requirements to protect unattended workspaces to conceal confidential data, including data handling in physical, network, and government access environments, and are reviewed annually and updated as needed.
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Corporate Information Security policies guide the Line of Business management of information security across Oracle. For more information see https://www.oracle.com/corporate/security-practices/corporate/governance/global-informationsecurity.html. Data centers hosting cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/physical-environmental.html.
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Oracle Corporate Security policies (including policies intended to protect information accessed, processed, or stored at remote sites and locations) are reviewed annually and updated as needed. Oracle SaaS Cloud follows Oracle's physical security standards and policies, including guidelines intended to protect information accessed, processed, or stored at remote sites and locations, are reviewed annually and updated as needed.
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html.
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Oracle SaaS Cloud Personnel Security standards and procedures define the roles and responsibilities concerning changes in employment and are documented and communicated to all personnel.
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Oracle's Acceptable Use Policy (AUP) guides the use of organizationally owned or managed assets. Employees must sign a confidentiality agreement as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/human-resources-security.html. Oracle SaaS Cloud Personnel Security Standard

		dictates that employees maintain the confidentiality of customer data, including SaaS physical and network access requirements. All employees are responsible for understanding and following corporate policies and SaaS standards.
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Oracle's Acceptable Use Policy (AUP) guides the use of organizationally owned or managed assets. Employees must sign a confidentiality agreement as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/human-resources-security.html. Oracle SaaS Cloud Personnel Security Standard dictates that employees maintain the confidentiality of customer data, including SaaS physical and network access requirements. All employees are responsible for understanding and following corporate policies and SaaS standards.
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Oracle Cloud SaaS employee roles and responsibilities relating to information assets and security are defined, documented and communicated. Oracle SaaS Cloud PI data protection standards, information protection, information management, and record retention policies provide global guidance for appropriate controls designed to protect cloud and customer data in accordance with data classification.
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Oracle's Acceptable Use Policy (AUP) guides the use of organizationally owned or managed assets. Employees must sign a confidentiality agreement as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/human-resources-security.html. Oracle SaaS Cloud Personnel Security Standard dictates that employees maintain the confidentiality of customer data, including SaaS physical and network access requirements. All employees are responsible for understanding and following corporate policies and SaaS standards.
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Employees who fail to comply with these policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs and are required by company policy. For more information, see

		https://www.oracle.com/corporate/security-practices/corporate/humanresources-security.html.
HRS-11.2	Are regular security awareness training updates provided?	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Employees who fail to comply with these policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle policies. This course also covers data-privacy principles and data-handling practices that may apply to employee's jobs and are required by company policy. For more information, see https://www.oracle.com/corporate/security-practices/corporate/humanresources-security.html.
HRS-12.1	Are employees with access to sensitive organizational and personal data, provided with appropriate security awareness training and regular updates in organizational procedures, processes, and policies, relating to their professional function relative to the organization?	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Employees who fail to comply with these policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs and are required by company policy. For more information, see https://www.oracle.com/corporate/security-practices/corporate/humanresources-security.html.
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Oracle SaaS Cloud employees are required to complete security awareness training at least annually, depending on the employee's role, or other qualifying criteria to maintain legal, statutory, and regulatory compliance obligations.
HRS-14.1	Are the policies and procedures defining the AI training program for all relevant personnel of the organization established, documented, approved, communicated, applied, evaluated, and maintained?	There is a comprehensive approach to the AI training program for all relevant personnel. Such programs are designed, implemented, and maintained according to corporate governance standards to implement responsible, compliant, and effective AI use.
HRS-14.2	Are regular training updates given to personnel based on their roles?	Oracle SaaS Cloud employees are required to complete security awareness training at least annually, depending on the employee's role, or other

		qualifying criteria to maintain legal, statutory, and regulatory compliance obligations
HRS-15.1	Are the policies and procedures on the acceptable use of AI technologies within the organization established, documented, and communicated to all personnel?	Oracle offers an array of general and technical trainings and certifications through Oracle University. We take additional measures to promote learning about AI and its responsible use across our employees, such as providing access to: live and recorded internal and external presentations; industry conferences and seminars; professional associations and certifications; and online media, books, and papers. We also sponsor and organize educational events to foster dialogue about Oracle AI across our global community, including through our annual CloudWorld event and the subsequent global tour.

Control Domain: Identity & Access Management

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

		information assets that is documented, approved, communicated, implemented, applied, evaluated, and maintained.
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including password complexity and protection requirements) are reviewed annually and updated as needed. Oracle SaaS Cloud Security Password Standards are reviewed annually and updated as needed
IAM-03.1	Is the inventory of identities managed, stored and regularly reviewed, and is their level of access monitored?	Oracle SaaS Cloud Security follows the SaaS Cloud Security Logical Access Control standard for all SaaS Cloud owners access level and systems are managed, stored and reviewed periodically.
IAM-04.1	Are separation of duties principles employed when implementing information system access?	Oracle SaaS Cloud Security enforces well-defined roles, allowing for segregation of duties among operation users which is defined in the SaaS Logical Access Controls Standard. Operations are organized into functional groups, where each function is performed by separate groups of employees (e.g., database administrators, system administrators, and network engineers). Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval.
IAM-05.1	Are least privilege principles employed when implementing information system access?	Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are required to be based on the following principles: · Need to know: Does the user require this access for his job function? · Segregation of duties: Will the access result in a conflict of interest? · Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose? For more information, see https://www.oracle.com/corporate/security-practices/corporate/accesscontrol.html.
IAM-06.1	Is an identity access provisioning process which authorizes, records, and communicates access changes to data and assets, defined and implemented?	Oracle SaaS Cloud Security user accounts are managed with a provisioning process. Access to user groups and resources are approved in the permissions system prior to access provisioning. An expiration date is required for temporary access requests. SaaS Cloud users supporting the SaaS Cloud Applications and services are defined and implemented to authorize, record, and communicate data and assets access changes for users who are authorized to administer the device or asset.
IAM-07.1	Is identity access de-provisioned or modified, in a timely manner?	Oracle Lines of Business are required to regularly review network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/access-

		control.html. Oracle SaaS Cloud Security disables and revokes SaaS Cloud accounts if an employee leaves the company for any reason. SaaS Cloud entitlements are automatically disabled when there are system identity changes, and it is required to request new entitlements. The de-provision process prevents the user from accessing protected networks and devices in cloud environments.
IAM-08.1	Are user access for least privilege and separation of duties reviewed and revalidated with a frequency commensurated with organizational risk tolerance and at least annually or upon significant changes?	Oracle SaaS Cloud reviews entitlements on a quarterly audit basis and updates SaaS Cloud users and their access for least privilege and separation of duties with organization risk tolerance to meet SaaS Cloud compliance, security requirements.
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles, defined, implemented, and evaluated?	Oracle SaaS Cloud Security follows an approved separation of duties process for the segregation of privileged access roles with technical measures that define the requirements to implement data access, encryption, key management, and logging capabilities. Oracle SaaS Cloud employs the principle of least privilege allowing only authorized users access.
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a time-limited period?	Oracle SaaS Cloud access processes are defined and implemented. Privileged Access roles and rights have processes to implement that are reviewed on a quarterly basis. Privileged Account passwords expire on a shortened cycle. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/access-control.html.
IAM-10.2	Are procedures implemented to prevent the accumulation of segregated privileged access?	Oracle SaaS Cloud Security user accounts are managed with a provisioning process. Access to user groups and resources are approved in the permissions system prior to access provisioning. An expiration date is required for temporary access requests. SaaS Cloud users supporting the SaaS Cloud Applications and services are defined and implemented to authorize, record, and communicate data and assets access changes for users who are authorized to administer the device or asset.
IAM-11.1	Are processes and procedures defined, implemented, and evaluated for customers to participate, where applicable, in granting access for agreed high-risk (as defined by the organizational risk assessment) privileged access roles?	Oracle SaaS Cloud Security user accounts are managed with a provisioning process. Access to user groups and resources are approved in the permissions system prior to access provisioning. An expiration date is required for temporary access requests. SaaS Cloud users supporting the SaaS Cloud Applications and services are defined and implemented to authorize, record, and communicate data and assets access changes for users who are authorized to administer the device or asset.
IAM-12.1	Are processes, procedures, and technical measures defined, implemented, evaluated to ensure	Oracle SaaS Cloud follow the Logging and Log Analysis Standard and follows the Oracle Corporate Logging and Log Analysis Policy to help ensure that the logging infrastructure is defined, implemented, and evaluated to address

	the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it, is controlled through a procedure that ensures the segregation of duties and break glass procedures?	technical measures and logging best practices. SaaS Cloud users are only granted permission to access log data based on their assigned role.
IAM-13.1	Are processes, procedures, and technical measures, that ensure identities' activities are identifiable through uniquely associated IDs, defined, implemented, and evaluated?	Oracle SaaS Cloud Security Logical Access Controls Standards and access-control policies help ensure that users are identifiable through unique identification and access permission based on their assigned role. Approved users use different permission credentials to access only the data explicitly granted to SaaS cloud environments.
IAM-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for authenticating access to systems, applications, and data assets, including multifactor authentication for at least privileged user and sensitive data access?	Oracle SaaS Cloud Security Logical Access Controls Standard defines processes, procedures, and technical measures for authenticating access to Oracle Cloud systems, applications and data assets, including multi-factor authentication (MFA) for a least-privileged user and sensitive data access. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html.
IAM-14.2	Are digital certificates or alternatives adopted that achieve an equivalent level of security for system identities?	Oracle SaaS Cloud Security uses external and internal certificate authorities for digital certification generation. For SaaS Cloud customer facing URLs, Oracle uses external certificate authority vendors. For internal application communication, Oracle uses an external certificate authority.
IAM-15.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the secure management of passwords and other secrets?	Oracle SaaS Cloud Password Standard helps ensure processes, procedures, and technical measures are in place for the secure management of passwords. Password managed components protect the confidentiality, integrity, and availability of Oracle SaaS Cloud information assets. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html.
IAM-16.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to verify access to data and system functions are authorized?	Oracle SaaS Cloud Corporate Single Sign-On Standards and technical controls set forth the processes, procedures, and technical measures to help ensure proper authentication mechanisms are in place to verify a user's access requirements to Oracle SaaS Cloud information assets. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/.
IAM-17.1	Are policies and procedures defined for "need to know" access to knowledge, information and data	Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. Authorization decisions for granting, approval, and review of access

	within the organization and in the context of the AI system to be applied when regulating access to resources?	are required to be based on the following principles: · Need to know: Does the user require this access for his job function? · Segregation of duties: Will the access result in a conflict of interest? · Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose? For more information, see https://www.oracle.com/corporate/security-practices/corporate/accesscontrol.html. Oracle SaaS Cloud Security access is provided on a need-to-know and least-privileged basis for employees and approved third parties when implementing information system access to SaaS cloud environments. The principle of least trust is individually attributable or provides a one-to-one user-to account when providing access to all SaaS Cloud Applications data and information. AI outcomes, predictions, and Gen AI responses are sent from a customer's Fusion AI Platform environment to the customer's Oracle Fusion Application via secure REST APIs via typical business workflows.
IAM-18.1	Are role for access when allowing model output modification of AI-generated output established to ensure changes are made only by authorized identities?	Certain circumstances may require that Oracle Data Scientists obtain restricted access to. Access follows the approved and secure OCI policy rules in place as for other operational data access. Oracle SaaS Cloud Services follows the Oracle Cloud PI Data Protection Standard and procedures, as part of the privacy-by-design framework. Oracle Cloud Services provide functionality where a customer can securely process data subjects related requests to request access, modify, or delete personal data (including rectification, correction, or erasure) applicable to security, privacy, and regulatory requirements.
IAM-19.1	Are agents' access to the tools and plugins necessary for the activity or use case at hand, restricted to ensure adherence to the principles of need-to-know and least privilege?	Agent's access to tools and plugins within Oracle SaaS Cloud environments is restricted based on the principles of need-to-know and least privilege. Access rights are granted only to the minimum set of employees and authorized third parties necessary for the specific activity or use case, with individual user-to-account attribution for all SaaS Cloud Applications data and information.

Control Domain: Interoperability & Portability

Question ID	Consensus Assessment Question	Oracle Response
IPY-01.1	Are interoperability and portability policies and procedures established, documented, approved, communicated, evaluated, and maintained, including requirements for: a. Communications between application interfaces	Oracle SaaS Cloud Security documents available APIs for Oracle Cloud Applications that are in place for communications between application services. For more information, see https://docs.oracle.com/en/cloud/

	b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence?	
IPY-01.2	Are interoperability and portability policies and procedures reviewed and updated at least annually or upon significant changes?	Oracle SaaS Cloud Applications follows policies and procedures for communication between components information processing, including interoperability. Customers are provided network protocol information necessary to use the services.
IPY-02.1	Are application interface(s) to AICs provided so that they programmatically retrieve their data to enable interoperability and portability?	Oracle SaaS Cloud customer API calls, including actions from the customer administration console, are logged and retained for 90 days and cannot be deleted by customers. Where applicable, Cloud Services Contracts (CSC's) can programmatically retrieve their data via an application interface. Oracle SaaS Cloud Application customers may request an export of their logs by contacting Oracle Cloud Services.
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data, according to industry standards?	Oracle SaaS Cloud security implements a secure file transfer functionality that is built on commonly used network access storage platforms and uses secured protocols for transfer. The functionality can be used to upload files to a secure location (i.e., data import/export) on Oracle Cloud hosted service or downloading files at service termination. Secured data transfer between on-premises and a customer's tenancy; between customer's environments at other cloud providers, can be accomplished through a combination of industry standardized network protocols and the customer's design of their private networks.
IPY-04.1	Are agreements including provisions specifying AICs access to data upon contract termination, including: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the AICs d. Data deletion policy?	Oracle Cloud Hosting and Delivery Policies and the Oracle PaaS and IaaS Public Cloud Services Pillar document set forth Oracle Cloud Service Level Objective Policy which defines Target Service Availability Level and Target Service Uptime. This includes a provision specifying customer access to data upon contract termination. At the end of the Service Period, the customer's content is available for retrieval during a retrieval period set forth in the Service Specifications or required by law. Remaining content will be deleted or otherwise rendered unrecoverable. Data deletion best practices are described in more detail in the Service Specifications. For more information, see https://www.oracle.com/contracts/cloudservices/ .
Control Domain: Infrastructure Security		

Question ID	Consensus Assessment Question	Oracle Response
I&S-01.1	Has the organization established, documented, approved, communicated, applied, evaluated, and maintained policies and procedures for infrastructure and virtualization security?	Oracle SaaS Cloud follows a Network Security Standard and procedures that are established and approved, and follows security policies, For more information, see: https://www.oracle.com/corporate/security-practices/corporate/ .
I&S-01.2	Are these policies and procedures reviewed and updated at least annually, or upon significant changes?	Oracle SaaS Cloud Network Security Standards are established and approved, and follow information security policies and are reviewed annually and updated as needed.
I&S-02.1	Are availability, quality and the adequate capacity of resources, being planned and monitored in order to deliver the required system performance as determined by the business?	Oracle SaaS Cloud Services continuously collects and monitors capacity and utilization data. This is used to anticipate and plan for demand, helping to ensure SLAs and customer performance needs are met.
I&S-03.1	Are communications between environments being monitored, encrypted, and restricted to only authenticated and authorized connections, as justified by the business?	Oracle SaaS Cloud Security follows the OSSA standards for SaaS Cloud Applications and employs active continuous monitoring on the attack surface in accordance with OCI firewall logging and Network Intrusion Detection Systems to help identify and block suspicious traffic and security attacks. Oracle Cloud Services monitors log system errors and security alerts for incident management and forensic purposes for security event analysis. Communications between SaaS Cloud Applications environments are encrypted, including SaaS Cloud user/device authentication via passwords and multi-factor authentication. RBAC management principles are adopted with authorizing controls. Oracle SaaS Cloud Security follows the OSSA standards for Oracle SaaS Cloud Applications; environments are restricted to only authenticated and authorized connections by configuring and enabling secure communications.
I&S-03.2	Are these configurations reviewed at least annually and supported by a documented justification of all allowed services, protocols, ports, and compensating controls?	SaaS Cloud Security standards and procedures for network configurations are reviewed annually and updated as needed. Oracle SaaS Cloud Security follows the Oracle Cloud Network Security Standard and the OSSA standards to implement configurations are supported and documented on configuring the security on the SaaS Cloud Applications.
I&S-04.1	Are the host and guest OS, hypervisor, or infrastructure control plane, being hardened according to their respective best practices and	Oracle SaaS Cloud Security employs standardized system hardening practices across Oracle SaaS Cloud Applications network configurations and connections. This includes restricting protocol access, removing or disabling

	supported by technical controls as part of a security baseline?	unnecessary software and services, unnecessary user accounts, patch management, and logging.
I&S-05.1	Are production and non-production environments kept separate?	Oracle SaaS Cloud Services production and non-production SaaS Cloud Application environments are logically and physically segregated. Additionally, procedures are in place that dictate production data is not used in non-production environments.
I&S-06.1	Are applications and infrastructures designed, developed, deployed and configured such that tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	To mitigate security risks associated with SaaS Cloud Application customer data that are comingling inherent in multi-tenant clouds, SaaS Cloud environments are provisioned in Oracle's Isolated Tenancy Model, isolating one customer from other Oracle Cloud customers. Data is segregated from other Oracle Cloud customer data via dedicated database, virtual machines and VLANs.
I&S-07.1	Are secure and encrypted communication channels used when migrating servers, services, applications or data to hosted environments?	Access to Oracle SaaS Cloud Applications is through a secure communication protocol. Staging networks are segregated from production-level networks and utilized when migrating production data to virtual servers. Physical servers, applications, and virtual machines are not moved. New environments are provisioned using a hardened master image with customer data migrated once the provisioning process is complete. Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Customer configuration information (e.g., connection strings, application settings) supplied through the management portal is protected while in transit and at rest.
I&S-07.2	Are such channels including only up-to-date and approved protocols?	Access to Oracle SaaS Cloud Applications is through a secure communication protocol. Staging networks are segregated from production-level networks and utilized when migrating production data to virtual servers. Physical servers, applications, and virtual machines are not moved. New environments are provisioned using a hardened master image with customer data migrated once the provisioning process is complete. Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Customer configuration information (e.g., connection strings, application settings) supplied through the management portal is protected while in transit and at rest.
I&S-08.1	Are high-risk environments identified and documented?	Oracle SaaS Information Security Risk Management Standard addresses a risk management process to identify SaaS Cloud Application risks in high-risk environments associated with specific SaaS Applications and SaaS Risk Treatment SLAs to help protect customer data from misuse or compromise.
I&S-09.1	Are processes, procedures, and defense-in-depth techniques for the protection, detection, and timely	Oracle SaaS Cloud maintains a Network Security Standard and procedures that are established and approved, and follow the Network Security Management controls using only secure protocols, encrypted traffic, Network Intrusion Detection Systems and processes on all SaaS Cloud Network systems and

	response to network-based attacks, defined, implemented and evaluated?	devices and configured to log system events, network events, and NetFlow to the Cloud Security SIEM. Oracle Cloud Security has established automated controls to monitor and detect DDoS attacks.

Control Domain: Logging and Monitoring

Question ID	Consensus Assessment Question	Oracle Response
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Logging and monitoring policies are established, documented, approved, communicated, evaluated, and maintained by Oracle Corporate Security. Oracle Lines of Business (LoBs) are required to capture and store logs for certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communicationsoperations-management.html. Oracle SaaS Cloud security standards are in place to follow Oracle logging and monitoring procedures and are aligned with industry best practices.
LOG-01.2	Are policies and procedures reviewed, approved and updated at least annually, or upon significant changes?	Oracle Corporate Security policies (including policies that address logging and monitoring) are reviewed annually and updated as needed. The LOB is responsible implementing associated procedures. Oracle SaaS Cloud security standards are reviewed and approved annually and updated as needed.
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Oracle SaaS Cloud Security has a defined SaaS Cloud logging and Log Analysis standard and follows Oracle logging and log analysis policy. Logs are automatically collected from the SaaS Cloud Applications and retained.
LOG-03.1	Are security-related events within applications, the underlying infrastructure, and the supply chain being identified and monitored, and are other events being logged based on risk evaluation?	The Oracle SaaS Cloud Logging and Log Analysis Standard sets forth the requirements for regular system monitoring for log generation, storage, retention, and analysis to identify and remediate suspicious and unauthorized activities within SaaS Cloud Applications.
LOG-03.2	Is a system to generate alerts, defined and implemented, to responsible stakeholders based on security-related events and corresponding metrics?	Oracle SaaS Cloud Applications uses a proprietary event management system that is defined and implemented to identify and alert, and uses other alarms, when specific events occur in SaaS Cloud Applications and components. The alarm configuration is based on regulatory requirements, industry standards, SaaS Cloud infrastructure conducts internal penetration testing system actions and responses, and security operations round-table discussions. The SIEM users

		can triage events based on the severity and criticality of the content of the event, including systems, applications, users, or regulatory environment.
LOG-04.1	Is access to audit logs restricted and are the records of access logs maintained?	Oracle SaaS Cloud Logging and Log Analysis Standard defines security and parameters (including retention) for SaaS Cloud Application logs. These logs are restricted and provided on a need-to-know basis. Where possible, log files are protected by SHA 2 cryptographic hash sum and are monitored. Logs on intranet-accessible systems are relocated daily to systems that are not intranet accessible.
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Oracle SaaS Cloud follows the logging and log analysis policy and audit requirements to identify and remedy suspicious and unauthorized activities which may impact the confidentiality, integrity and availability of SaaS Cloud Applications and information assets on third-party systems.
LOG-05.2	Is a process, on reviewing and taking appropriate and timely actions on detected anomalies, defined, established and followed?	Oracle SaaS Cloud Detection and Response Team (DART) has defined procedures and processes to implement appropriate and timely actions on detected anomalies.
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Oracle information system clocks for SaaS Cloud components are synchronized via Network Time Protocol (NTP) to a primary and secondary authoritative time source.
LOG-07.1	Are information metadata system events that should be logged, established, documented, and implemented?	Oracle SaaS Cloud Applications follows the Oracle Cloud Services Logging and Log Analysis standard which defines the standards for log generation, storage, retention, analysis, and log archived retention periods.
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Oracle SaaS Cloud Security logging processes and threat landscape are continually reviewed, and logging requirement updates are made as necessary to include changing threats. The scope is reviewed annually and updated as needed. If necessary, the scope may be reviewed more frequently.
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Oracle SaaS Cloud components are configured to log events in accordance with the Oracle SaaS Cloud Security Logging and Log Analysis Standard. The scope of audited events is reviewed and updated at least annually or whenever there is a change in the threat environment. The Oracle SaaS Cloud Security Logging and Log Analysis Standard addresses the required auditable events, content of audit records, audit storage capacity, and responses to auditing failures.
LOG-09.1	Is the audit records protected from unauthorized access, modification, and deletion?	The Security Information and Event Management (SIEM), for Oracle SaaS Cloud Applications, is configured on a need-to-know and least privilege basis to help protect audit information and logging tools from unauthorized access, modification, and deletion. Oracle SaaS Cloud Security analysts are notified when attempts are detected.

LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Oracle SaaS Cloud monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. There are logs generated and mechanisms in place to review and respond to activity.
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Oracle SaaS Cloud monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. There are logs generated and mechanisms in place to review activity.
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Oracle SaaS Cloud follows the Logical Access Controls policy and associated requirements to monitor physical access logs. Access mechanisms are configured in a Central Logging System (CLS) to not allow malicious and unintentional alteration of the logs. The standard retention policy for logs is 90 days.
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Oracle SaaS Cloud processes and measures for reporting and monitoring system anomalies and failures are in place. Oracle SaaS Cloud components generate an alert to accountable service operations teams when audit failure events occur.
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Oracle SaaS Cloud accountable parties are promptly notified about anomalies and failures, SaaS Cloud Applications leverages a Security Information and Event Management (SIEM) solution to correlate information such as system events, firewall logs, WAF logs, network flows from the environment, and to alert on potential security events. Oracle SaaS Cloud Security personnel monitor the SIEM 24x7x365 and have defined processes to escalate events as needed. This process includes reporting and notification requirements to system owners and Oracle leadership.
LOG-14.1	Are all input events (content and metadata) logged and monitored to enable auditing and reporting on the usage of AI models?	Input events, including content and metadata are logged and monitored to enable auditing and reporting on the usage of AI models within OCI Generative AI Service. Prompts, responses, guardrail outcomes, and usage metrics are initially stored in an Autonomous Transaction Processing (ATP) Gen AI Metrics Store for up to 28 hours, after which the data is transferred to long-term storage in the Metrics Store on OCI Object Store to support auditing and reporting. Telemetry data on model usage, user interactions, and system performance is systematically collected and analyzed to optimize outputs, assess model quality, and inform model upgrades.
LOG-15.1	Are all output events (content and metadata) logged and monitored to enable auditing and reporting on the usage of AI models?	Output events, including both content and metadata are logged and monitored to enable comprehensive auditing and reporting on the usage of AI models within the OCI Generative AI Service. Prompts, responses, guardrail outcomes, and usage metrics are initially stored in an Autonomous Transaction

		Processing (ATP) Gen AI Metrics Store for up to 28 hours, after which they are moved to the OCI Object Store Metrics Store for long-term retention and auditability. Telemetry data–including user interactions with outputs and quality indicators–is continuously collected and analyzed to support model optimization, performance evaluation, and feature enhancements.

Control Domain: Model Security

Question ID	Consensus Assessment Question	Oracle Response
MDS-01.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure the security of the Training Pipeline?	As with all Oracle products and services, our development lifecycle for AI systems is subject to a governance framework that applies from the planning phase through implementation. For example, new AI systems undergo an initial technical review to assess their intended use, training data, accuracy, fairness, transparency, privacy, security, human control, and other factors. This detailed review helps us better understand the potential benefits and implications of an AI system, identify associated risks and mitigations, and promote informed decision-making and responsible behavior from the outset.
MDS-01.2	Are policies, procedures and technical measures to address new security threats and best practices regularly review and update?	Oracle conducts a review of AI systems prior to their deployment to assess their intended use, training data, accuracy, privacy, security, safety, fairness, transparency, and human control. Oracle conducts the AI system review again upon a material change to an AI system after deployment. The AI system review is designed to identify and mitigate risks of AI systems. Oracle maintains documentation of the AI system review, including an AI system report created upon completion of the AI system review.
MDS-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the periodic scanning of model artifacts for vulnerabilities and attacks at each step of the service lifecycle and at each handover point?	Oracle will update the AI Services to maintain operational stability, availability, security, performance, and currency as described in Section 4 (Oracle Cloud Change Management Policy) of the Oracle Cloud Hosting and Delivery Policies (part of the Service Specifications). Our development lifecycle includes many other human-centric controls, notably including our Corporate Security Solution Assurance Process (CSSAP). This review process was developed by and includes representatives from our Security Architecture, Information Security, Product Security, Information Technology, and Legal organizations and other key stakeholders. It is designed to provide an information security management review for all our products and services, including those with AI systems, prior to deployment in production. More information on CSSAP is available at https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.
MDS-02.2	Are policies, procedures and technical measures to address model	Oracle will update the AI Services to maintain operational stability, availability, security, performance, and currency as described in Section 4

	artifact scanning regularly reviewed and updated?	(Oracle Cloud Change Management Policy) of the Oracle Cloud Hosting and Delivery Policies (part of the Service Specifications). Our development lifecycle includes many other human-centric controls, notably including our Corporate Security Solution Assurance Process (CSSAP). This review process was developed by and includes representatives from our Security Architecture, Information Security, Product Security, Information Technology, and Legal organizations and other key stakeholders. It is designed to provide an information security management review for all our products and services, including those with AI systems, prior to deployment in production. More information on CSSAP is available at https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.
MDS-03.1	Are processes and procedures defined, implemented, enforced, and evaluated for documenting, approving, communicating, evaluating, and maintaining model documentation?	Oracle will update the AI Services to maintain operational stability, availability, security, performance, and currency as described in Section 4 (Oracle Cloud Change Management Policy) of the Oracle Cloud Hosting and Delivery Policies (part of the Service Specifications). Our development lifecycle includes many other human-centric controls, notably including our Corporate Security Solution Assurance Process (CSSAP). This review process was developed by and includes representatives from our Security Architecture, Information Security, Product Security, Information Technology, and Legal organizations and other key stakeholders. It is designed to provide an information security management review for all our products and services, including those with AI systems, prior to deployment in production. More information on CSSAP is available at https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.
MDS-03.2	Is the model documentation regularly reviewed and updated?	The model documentation is regularly reviewed and updated by the model provider. For third-party models incorporated in an Oracle AI system, the model provider creates and maintains the information and technical documentation about how the model was designed, developed, trained, and tested, and often publishes such documentation on its website. Information about OpenAI, xAI, Meta, and Cohere models is available at https://platform.openai.com/docs/overview https://docs.x.ai/docs/overview, https://www.llama.com/docs/overview/ https://docs.cohere.com/cohere-documentation respectively.
MDS-4.1	Are baseline requirements for Model documentation established and implemented?	The model documentation is regularly reviewed and updated by the model provider. For third-party models incorporated in an Oracle AI system, the model provider creates and maintains the information and technical documentation about how the model was designed, developed, trained, and tested, and often publishes such documentation on its website. For example,

		information about OpenAI, xAI, Meta, and Cohere models is available at https://platform.openai.com/docs/overview https://docs.x.ai/docs/overview https://www.llama.com/docs/overview/ https://docs.cohere.com/cohere-documentation respectively.
MDS-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the validation of the model documentation aligned with the current model?	The model documentation is regularly reviewed and updated by the model provider. For third-party models incorporated in an Oracle AI system, the model provider creates and maintains the information and technical documentation about how the model was designed, developed, trained, and tested, and often publishes such documentation on its website. For example, information about OpenAI, xAI, Meta, and Cohere models is available at https://platform.openai.com/docs/overview, https://docs.x.ai/docs/overview https://www.llama.com/docs/overview/ https://docs.cohere.com/cohere-documentation respectively.
MDS-06.1	Are processes and technical measures defined, implemented, and evaluated to regularly assess adversarial threats specific to each AI model?	Oracle defines, implements, and regularly evaluates processes and technical measures to assess adversarial threats specific to each AI model. Our policies and practices align with leading regulations and industry standards—including the EU AI Act, NIST AI Risk Management Framework, and ISO/IEC 42001/2023—and are frequently updated to address evolving AI threats and risks. For both Oracle-developed and third-party models, ongoing technical reviews, documentation, and risk assessments are conducted to identify and mitigate adversarial threats, ensuring continued protection and compliance across all Oracle AI systems.
MDS-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for Model Hardening to mitigate relevant adversarial attacks as identified in the Threat Analysis and Adversarial Threat Analysis?	Oracle defines, implements, and regularly evaluates processes, procedures, and technical measures for model hardening to mitigate adversarial attacks identified through Threat Analysis and Adversarial Threat Analysis. Our AI development lifecycle operates under a robust governance framework, beginning with initial technical reviews that assess security risks and necessary mitigations, including model robustness against adversarial threats. Human-centric controls—most notably the Corporate Security Solution Assurance Process (CSSAP)—further implement information security management review by cross-functional experts prior to production deployment, supporting continual risk assessment and hardening of all AI models in accordance with Oracle's security and compliance standards. For more information, see More information on CSSAP is available at https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.

MDS-08.1	Are checksums regularly calculated and compared using cryptographic hashes of model checkpoints to detect unauthorized modifications?	Checksums are regularly calculated and compared using cryptographic hashes of model checkpoints to detect unauthorized modifications and help maintain model integrity. This process involves generating a cryptographic hash (such as SHA-256) for each model checkpoint at the time of creation and storing it securely. Each time a checkpoint is accessed or loaded, its hash is recalculated and compared with the stored value to verify that the model has not been tampered with.
MDS-08.2	Are these measures applied at least annually based on the level of risk, or after any change of hands?	As with all Oracle products and services, our development lifecycle for AI systems is subject to a governance framework that applies from the planning phase through implementation. For example, new AI systems undergo an initial technical review to assess their intended use, training data, accuracy, fairness, transparency, privacy, security, human control, and other factors. This detailed review helps us better understand the potential benefits and implications of an AI system, identify associated risks and mitigations, and promote informed decision-making and responsible behavior from the outset.
MDS-09.1	Are models signed cryptographically and are signatures verified to ensure model provenance and ownership any time the model changes hands or is loaded from storage?	For Oracle Predictive AI, our proprietary models are cryptographically signed to establish model provenance and ownership. Each time a model is transferred or loaded from storage, its digital signature is verified to implement its authenticity and integrity—helping to prevent unauthorized modifications and confirming legitimate origin within Oracle's managed environments. For Generative AI, where we utilize third-party foundational models, Oracle relies on the model provider to sign models and deliver associated provenance metadata. When integrating or loading these third-party models, Oracle verifies the digital signatures and metadata, whenever available.
MDS-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for continuous monitoring of model performance metrics over time to identify sudden shifts or unexpected changes in predictions that could degrade model performance?	Data science monitoring promotes proper functioning for the following: · Model training, tuning, and retraining (for classic AI) · Generating predictions (for classic AI) · Generating responses from prompts (for GenAI) · Logging metrics and classic AI data model (prediction) quality, and GenAI response quality · Automating responses to quality issues
MDS-11.1	Are risk-based evaluation of the model and model serving infrastructure for model failure performed?	We have established policies and practices that apply to the development and deployment of Oracle AI systems, including third-party models incorporated in our products and services. These policies and practices are aligned with applicable laws, regulations, and industry standards. Given the fast-paced nature of AI technological progress and legal, regulatory, and industry developments, we are frequently evaluating and updating these policies and practices.
MDS-11.2	Are measures defined and implemented to mitigate model and	From time to time existing models are reviewed. A decision is taken to retain, upgrade, or replace, if it is determined there would be an improvement in its

	model serving infrastructure failures, and are they regularly evaluated throughout the AI system's lifecycle?	operation for the customer. The LLM Upgrade process is as follows. A thorough evaluation is performed to decide whether to take a new model. Updating of the model is handled as a rolling upgrade with prompt template seed data updated as required. These model updates would occur as part of the normal Fusion upgrade cycle currently.
MDS-12.1	Are processes established to evaluate the risk associated with open models?	Oracle focuses on risk across a broad range of contexts, from the data we use to train our proprietary AI systems, to the pre-trained models that we make available from third parties to the way those models are incorporated into our products and services. We identify, analyze, manage, and mitigate AI system risks throughout the development lifecycle. We benefit from the diverse perspectives and experience of many cross-functional teams that collaborate to align our approach to industry standards and enable us to deliver better products and services to our customers.
MDS-12.2	Are risk factors periodically reviewed, and is a process implemented to monitor and mitigate any determined vulnerabilities?	As with all Oracle products and services, our development lifecycle for AI systems is subject to a governance framework that applies from the planning phase through implementation. For example, new AI systems undergo an initial technical review to assess their intended use, training data, accuracy, fairness, transparency, privacy, security, human control, and other factors. This detailed review helps us better understand the potential benefits and implications of an AI system, identify associated risks and mitigations, and promote informed decision-making and responsible behavior from the outset. Our development lifecycle includes many other human-centric controls, notably including our Corporate Security Solution Assurance Process (CSSAP). This review process was developed by and includes representatives from our Security Architecture, Information Security, Product Security, Information Technology, and Legal organizations and other key stakeholders. It is designed to provide an information security management review for all our products and services, including those with AI systems, prior to deployment in production. More information on CSSAP is available at https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.
MDS-13.1	Are secure model formats and processes for AI model serialization adopted where applicable?	The Oracle Fusion AI Platform is a multi-tenant environment, where each customer's data and trained ML models (for classic AI) remain isolated. No customer data is shared, mixed, or combined to train ML models, or to process GenAI requests. Pre-trained generative AI models (LLMs) are securely accessed by the Oracle Fusion AI Platform within a secure Oracle Cloud Infrastructure (OCI) environment (which may be outside of the local OCI region). Data is not retained in the LLMs, i.e., after a prompt is processed, no customer data persists, and prompt data does not train the LLM. Data processed within the LLM is completely isolated, and no customer data is shared or combined. AI outcomes, predictions, and Gen AI responses are sent from a

		customer's Fusion AI Platform environment to the customer's Oracle Fusion Application via secure REST APIs via typical business workflows

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

Question ID	Consensus Assessment Question	Oracle Response
SEF-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for Security Incident Management, E-Discovery, and Forensics?	Policies and procedures for security incident management, e-discovery, and cloud forensics are established, documented, approved, communicated, applied, evaluated, and maintained with the oversight of Corporate Information Security Policies. Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed data has been improperly handled or accessed. Note that cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available logs and other tooling. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to security events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for security event and incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). GIS defines roles and responsibilities for the incident response teams embedded within the Lines of Business (LOBs). All LOBs must comply with GIS incident response guidance about detecting events and timely corrective actions. Upon discovery of an incident, Oracle defines an incident response plan for rapid and effective incident investigation, response, and recovery. Formal procedures and systems are utilized within the Lines of Business (LOBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary. For more information, see https://www.oracle.com/corporate/security-practices/corporate/securityincident-response.html. LOB is responsible implementing associated procedures. Oracle SaaS Cloud Information Security Standard follows the Oracle Corporate Information Security policy for Iincident management, e-discovery, and cloud digital forensics, and is applied, evaluated, and maintained. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html.
SEF-01.2	Are policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics reviewed and updated at least	Oracle Corporate Security policies and procedures that address security incident management, e-discovery and forensics are reviewed annually and updated as needed. Oracle SaaS Cloud Information Security Standards and

	annually or upon significant changes?	Incident Response Plan and procedures are reviewed annually and updated as needed.
SEF-02.1	Are Service Management Policies and Procedures established, documented, approved, communicated, applied, evaluated, and maintained for the timely management of security incidents?	Policies and procedures for security incident management, e-discovery, and cloud forensics are established, documented, approved, communicated, applied, evaluated, and maintained with the oversight of Corporate Information Security Policies. Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed data has been improperly handled or accessed. Note that cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available logs and other tooling. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to security events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for security event and incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). GIS defines roles and responsibilities for the incident response teams embedded within the Lines of Business (LOBs). All LOBs must comply with GIS incident response guidance about detecting events and timely corrective actions. Upon discovery of an incident, Oracle defines an incident response plan for rapid and effective incident investigation, response, and recovery. Formal procedures and systems are utilized within the Lines of Business (LOBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary. For more information, see https://www.oracle.com/corporate/security-practices/corporate/securityincident-response.html. LOB is responsible implementing associated procedures. Oracle SaaS Cloud Information Security Standard follows the Corporate Information Security policy for incident management, e-discovery, and cloud digital forensics, and is applied, evaluated, and maintained. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html.
SEF-02.2	Are Service Management Policies and Procedures reviewed and updated at least annually, or upon significant changes?	Oracle Corporate Security policies and procedures that address timely management of security incidents are reviewed annually and updated as needed. Oracle SaaS Cloud Security policies and procedures for timely management of security events are reviewed annually and updated as needed with the approval of GIS and in accordance with the Corporate Incident Response Plan (CIRP).
SEF-03.1	Is a security incident response plans which includes but is not limited to a communication strategy for notifying relevant internal departments,	Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and

	impacted AICs, and other business critical relationships (such as supply-chain) that may be impacted, established, documented, approved, communicated, applied, evaluated, and maintained?	resolution within Oracle's Lines of Business (LOBs). Corporate requirements for LOB incident-response programs and operational teams are defined per incident type: · Validating that an incident has occurred · Communicating with relevant parties and notifications · Preserving evidence · Documenting an incident itself and related response activities · Containing an incident · Addressing the root cause of an incident · Escalating an incident For more information, see https://www.oracle.com/corporate/security-practices/corporate/securityincident-response.html.
SEF-04.1	Is a structured approach followed, to evaluate the effectiveness of incident response plans at planned intervals or upon significant changes?	The Oracle SaaS Cloud Security Incident Response Team (IRT) conducts specialized training to test the effectiveness of the Incident Response Plan (IRP), as it applies to Incident Management and Response GIS policies and is reviewed annually and updated as needed. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html.
SEF-05.1	Are information security incident metrics established, monitored and reported?	Information security incident metrics are established and monitored in each Line of Business (LOB) with oversight by Corporate Information Security Policies.
SEF-06.1	Are security-related event triage processes, procedures and technical measures supporting business processes, defined, implemented and evaluated? **Alternative formulation:** Are processes procedures and technical measures supporting business processes to triage security-related events, defined, implemented and evaluated?	Oracle SaaS Cloud Information Security Standards and Incident Response Plan are reviewed annually and updated as needed. Incident handling processes, procedures, and technical measures are implemented to support SaaS Cloud Applications and triage security-related events in an efficient and timely manner.
SEF-07.1	Are processes, procedures and technical measures for security breach notifications defined and implemented?	In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents and incident history are not shared externally.
SEF-07.2	Are material security breaches and assumed security breaches, including any relevant supply chain breaches,	Policies and procedures for security incident management, e-discovery, and cloud forensics are established, documented, approved, communicated, applied, evaluated, and maintained with the oversight of Corporate

	reported as per applicable SLAs, laws and regulations?	Information Security Policies. Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed data has been improperly handled or accessed. Note that cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available logs and other tooling. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to security events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for security event and incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). GIS defines roles and responsibilities for the incident response teams embedded within the Lines of Business (LOBs). All LOBs must comply with GIS incident response guidance about detecting events and timely corrective actions. Upon discovery of an incident, Oracle defines an incident response plan for rapid and effective incident investigation, response, and recovery. Formal procedures and systems are utilized within the Lines of Business (LOBs) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary. For more information, see https://www.oracle.com/corporate/security-practices/corporate/securityincident-response.html. LOB is responsible implementing associated procedures. Oracle SaaS Cloud Information Security Standard follows the Oracle Corporate Information Security policy for incident management, e-discovery, and cloud digital forensics policy and is applied, evaluated, and maintained. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html.
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Oracle maintains points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.
SEF-08.2	Are the points of contacts reviewed and updated at least annually?	Oracle maintains points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.
SEF-09.1	Are incident categories and severity levels defined for AI systems, and response procedures determined for each, including automated response where applicable?	Severity definitions are identified in the Hosting and Delivery policies - 5.3 Severity Definitions. Refer Data Processing Agreement - Section 9. Incident Management and Breach Notification 9.2 Oracle will notify you of a confirmed Information Breach without undue delay but at the latest within 24 hours.

Control Domain: Supply Chain Management, Transparency, and Accountability

Question ID	Consensus Assessment Question	Oracle Response
STA-01.1	Are policies and procedures for supply chain risk management established, documented, approved, communicated, applied, evaluated, and maintained?	Managing security and privacy in the cloud is a shared responsibility between the customer and the service provider. The distribution of responsibilities varies based on the nature of the cloud service (IaaS, PaaS, SaaS). Oracle strongly recommends that customers determine the suitability of using cloud services in light of their own legal and regulatory compliance obligations. Making this determination is solely the customer's responsibility. For information, see https://www.oracle.com/cloud/compliance/ . Oracle has policies designed to protect the safety of its supply chain, guide how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as selects third-party technology used in corporate and cloud environments. Additionally, Oracle has policies to mitigate the risks associated with the malicious alteration of products before installation by customers. Oracle suppliers are required to comply with the Supplier Information and Physical Security Standards of mandatory security controls. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/supply-chain/ Oracle's Supplier Management Security Policy defines requirements for Lines of Business supplier management programs, to guide selection and management of suppliers each LOB utilizes. Oracle SaaS Cloud Security follows security standards and practices of the Shared Security Responsibility Model (SSRM) to implement and meet the Supplier Security Management Policy (SSMP) requirements when engaging and using suppliers.
STA-01.2	Are the policies and procedures reviewed and updated at least annually or upon significant changes?	Oracle SaaS Cloud Security standard follows the Supplier Security Policy and the Supply Chain Security Standard for implementing a Shared Security Responsibility Model (SSRM) process that is reviewed and updated annually and updated as needed. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html.
STA-02.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for applying the Shared Security Responsibility Model (SSRM) within the organization?	Oracle SaaS Cloud Security Shared Security Responsibility Model (SSRM) is applied, documented, implemented, and managed throughout the supply chain for the SaaS Cloud Security Applications. For more information, see https://www.oracle.com/corporate/suppliers/?er=221886.

STA-02.2	Are policies and procedures for applying the Shared Security Responsibility Model (SSRM) within the organization reviewed and updated at least annually, or upon significant changes?	Oracle SaaS Cloud Security standard follows the Supplier Security Policy and the Supply Chain Security Standard for implementing a Shared Security Responsibility Model (SSRM) process that is reviewed and updated annually and updated as needed. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html.
STA-03.1	Is the SSRM applied, documented, implemented and managed throughout the supply chain?	Oracle SaaS Cloud Security Shared Security Responsibility Model (SSRM) is applied, documented, implemented, and managed throughout the supply chain for the SaaS Cloud Security Applications. For more information, see https://www.oracle.com/corporate/suppliers/?er=221886.
STA-04.1	Are customers provided with SSRM guidance detailing its applicability throughout the supply chain?	Oracle SaaS Cloud Security follows the Supplier Security Policy and the Supply Chain Security Standard to provide SSRM guidance on the supply chain approval process with Oracle SaaS Cloud products and services.
STA-05.1	Is the shared ownership and applicability of all CSA AICM controls delineated according to the SSRM?	Oracle Cloud Hosting and Delivery Policies describe the customer (tenant) security obligations. Also, the Oracle Data Processing Agreement includes the responsibilities of the data controller (tenant/customer) versus data processor (Oracle). For more information see the Oracle Hosting and Delivery Policies and the Oracle Data Processing Agreement at https://www.oracle.com/contracts/cloud-services/.
STA-06.1	Are the SSRM documentation reviewed and validated?	Oracle SaaS Cloud Security SSRM documentation is reviewed annually and updated as needed. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/hosting-deliverypolicies.html.
STA-07.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Oracle SaaS Cloud Security conducts third-party security assessments in scope with audit standards, including Supplier activities that are aligned with external regulations.
STA-08.1	Is an inventory of all supply chain relationships maintained and developed?	Oracle SaaS Cloud has developed and maintains an inventory of all supply chain relationships. These agreements define the security, privacy, and compliance controls prior to the onset of services. Oracle SaaS Cloud Security follows the Corporate Information Security policy for supplier security program to develop and maintain supply chain relationships. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain.
STA-09.1	Are risk factors associated with the supply chain relationships periodically reviewed?	Oracle SaaS Cloud establishes and maintains a program designed to assess suppliers' risk factors, a risk-based analysis, and appropriate security measures to protect confidential information within the supply chain that is periodically reviewed annually and updated as needed.

STA-10.1	Are service agreements required to include at least the following mutually agreed upon provisions and/or terms? · Scope, characteristics and location of business relationship and services offered · Information security requirements (including SSRM) · Change management process · Logging and monitoring capability · Incident management and communication procedures · Right to audit and third party assessment · Service termination · Interoperability and portability requirements · Data privacy	Oracle SaaS Cloud Security follows the Supplier Security Policy and the Supply Chain Security Standard to provide SSRM guidance on the supply chain approval process with Oracle SaaS Cloud products and services.
STA-11.1	Are supply chain agreements reviewed at least annually or upon significant changes?	Oracle SaaS Cloud service agreements between CSPs and CSCs are reviewed annually and updated as needed. For more information, see https://www.oracle.com/be/corporate/contracts/cloudservices/contracts.html.
STA-12.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	SaaS Cloud assessments are conducted at least annually in alignment with the SaaS Risk Treatment SLAs to define conformance and to effectively update treatment plans.
STA-13.1	Are policies implemented requiring all service providers throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards?	Oracle Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when accessing Oracle or Oracle customer facilities, networks and/or information systems, handling Oracle confidential information, or controlling custody of Oracle hardware assets. Suppliers are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/suppliers.html.
STA-14.1	Are the IT governance policies and procedures for organization's supply chain partners periodically reviewed?	Oracle's Supplier Security Management Policy requires all lines of business to maintain a program which manages risk for their suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual supplier review, where appropriate per the risk to data confidentiality,

		availability or integrity introduced by the way each supplier's goods or services are leveraged. For more information, see: https://www.oracle.com/corporate/securitypractices/corporate/supply-chain/. The Oracle SaaS Cloud Standard sets forth the requirements governing third-party SaaS Cloud networks, applications, information systems, and servers that are reviewed annually and updated as needed.
STA-15.1	Is a process for conducting periodic security assessments for all organizations within the supply chain defined and implemented?	SaaS Cloud assessments are conducted at least annually in alignment with the SaaS Risk Treatment SLAs to define conformance and to effectively update treatment plans.
STA-16.1	Are processes defined, implemented, enforced, and evaluated for establishing a Bill of Material for the entire AI service supply chain, including the model, orchestrated services, and AI applications?	New AI systems undergo an initial technical review to assess their intended use, training data, accuracy, fairness, transparency, privacy, security, human control, and other factors. This detailed review helps us better understand the potential benefits and implications of an AI system, identify associated risks and mitigations, and promote informed decision-making and responsible behavior from the outset. Our development lifecycle includes many other human-centric controls, notably including our Corporate Security Solution Assurance Process (CSSAP). This review process was developed by and includes representatives from our Security Architecture, Information Security, Product Security, Information Technology, and Legal organizations and other key stakeholders. It is designed to provide an information security management review for all our products and services, including those with AI systems, prior to deployment in production. More information on CSSAP is available at https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.

Control Domain: Threat & Vulnerability Management

Question ID	Consensus Assessment Question	Oracle Response
TVM-01.1	Are policies and procedures that identify, report, and prioritize the remediation of vulnerabilities and threats in order to protect systems against vulnerability exploitation, established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle has formal practices designed to identify, analyze, and remediate the technical security vulnerabilities that may affect our enterprise systems and Oracle Cloud environments. The Oracle IT, security and development teams monitor relevant vendor and industry bulletins, including Oracle's own security advisories, to identify and assess relevant security patches. Additionally, Oracle requires that vulnerability scanning using automated scanning systems be frequently performed against the internally and externally facing systems it manages. Oracle also requires that penetration testing activities be performed periodically in production environments. Oracle's strategic priority for the handling of discovered vulnerabilities in Oracle Cloud

		is to remediate these issues according to their severity and the potential impact to the Oracle Cloud Services. The Common Vulnerability Scoring System (CVSS) Base Score is one of the criteria used in assessing the relative severity of vulnerabilities. Oracle requires that identified security vulnerabilities be identified and tracked in a defect tracking system. Oracle aims to complete all cloud service remediation activities, including testing, implementation, and reboot/reprovision (if required) within planned maintenance windows. However, emergency maintenance will be performed as required to address severe security vulnerabilities, as described in the Oracle Cloud Hosting and Delivery Policies and, as applicable, associated Pillar documentation. Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Customers and security researchers can report suspected security vulnerabilities to Oracle: How to Report Security Vulnerabilities to Oracle or by submitting a Service Request in their support system. For more information, see https://www.oracle.com/corporate/securitypractices/corporate/communications-operations-management.html and https://www.oracle.com/corporate/security-practices/assurance/vulnerability/. Oracle SaaS Cloud has formal practices designed to identify, analyze, and remediate security vulnerabilities that may affect SaaS Cloud Applications. The SaaS Cloud Threat and Vulnerability Management Standard and procedures define processes to manage discovered vulnerabilities within Oracle SaaS Cloud environments; identifying, maintaining awareness, and to remediate vulnerabilities in all Oracle SaaS Cloud Applications and systems with defined security requirements.
TVM-01.2	Are threats and vulnerabilities policies and procedures reviewed and updated at least annually or upon significant changes?	Oracle Corporate Security policies (including policies that address threat and vulnerability management) are reviewed annually and updated as needed. Oracle SaaS Cloud Threat and Vulnerability Management Standard and procedures are reviewed annually and updated as needed.
TVM-02.1	Are policies and procedures to protect against malware and malicious instructions, established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption for their organization. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html. Oracle SaaS Cloud Security policies and best practices are in place to protect against malware on SaaS

		Cloud managed assets. Endpoint Management solutions include antivirus scanning, intrusion protection, and firewall solutions on endpoint devices to be applied, evaluated, and maintained on laptops, desktops, and mobile devices.
TVM-02.2	Are malware and malicious instructions protection policies and procedures, reviewed and updated at least annually or upon significant changes?	Oracle Corporate Security policies (including policies that address asset management and malware protection) are reviewed annually and updated as needed. Oracle SaaS Cloud security standards, including standards that address asset management and malware protection, are reviewed annually and updated as needed.
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications based on the identified risk?	Oracle's SaaS Cloud processes, procedures, and technical measures are defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications -based on the identified risk.
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and indicators of compromise weekly or more frequently?	Oracle SaaS Cloud processes, procedures, and technical measures have been defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators on at least a weekly basis and antivirus updates generally occur daily.
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third party or open source libraries according to the organization's vulnerability management policy?	Oracle SaaS Cloud Security Threat and Vulnerability Management standard including processes, procedure, and technical measures are defined, implemented, and evaluated to identify updates for SaaS Cloud applications that use third-party open-source libraries are defined and supported in the Threat and Vulnerability management policy. Oracle SaaS Cloud follows the OSSA standard specific to Supply Chain Security. Additionally, the security and development teams monitor relevant vendor and industry bulletins, including Oracle's security advisories, to identify and assess relevant security patches. Various security testing activities are performed by the SaaS Cloud Application teams throughout the development cycle to identify potential events. These activities include using static and dynamic analysis tools, as well as vulnerability assessment tools. Customers and security researchers can report suspected security vulnerabilities to Oracle per the process documented at Oracle.com: How to Report Security Vulnerabilities to Oracle or by submitting a Service Request in their designated support system (for example, My Oracle Support (MOS) or Support Cloud).
TVM-06.1	Are processes, procedures, and technical measures defined,	Oracle SaaS Cloud processes, procedures, and technical measures are in place for independent third-party penetration testing. Oracle regularly performs

	implemented, and evaluated for the periodic performance of penetration testing by independent third parties?	penetration testing and security assessments against Oracle Cloud infrastructure, platforms, and applications to validate and improve the overall security of Oracle Cloud Services. Additionally, security assessments and penetration tests are performed by a third-party on SaaS Cloud Applications at least annually. Third party penetration testing summary results are available to customers upon request.
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated based on identified risks to support scheduled and emergency responses to vulnerability identification?	Oracle SaaS Cloud Threat and Vulnerability Management standard defines the methodology for managing discovered vulnerabilities within the SaaS Cloud environment. This standard also defines the scanning requirements and configuration identification and detection tools and processes; remediation timelines; as well as threat intelligence detection of SaaS managed assets at least monthly. For more information see https://www.oracle.com/corporate/security-practices/assurance/vulnerability/securityfixing.html.
TVM-08.1	Are risk-based models utilized to prioritize vulnerability remediation using an industry-recognized framework effectively?	Oracle uses the Common Vulnerability Scoring System (CVSS) to report the relative severity of security vulnerabilities when it discloses them. CVSS Base Score information is provided in the risk matrices published in Critical Patch Update and Security Alert Advisories. Oracle uses Common Vulnerabilities and Exposures (CVE) numbers to identify the vulnerabilities listed in the risk matrices in Critical Patch Update and Security Alert advisories. For more information, see https://www.oracle.com/corporate/securitypractices/assurance/vulnerability/. Oracle SaaS Cloud uses Common Vulnerability Scoring System (CVSS) to report relative severity of security vulnerabilities. Vulnerabilities are remediated in order of the risk they pose to users. This process is designed to patch the security holes with the greatest associated risk first, resulting in optimizing the security posture of all Oracle customers.
TVM-09.1	Are processes defined and implemented for tracking and reporting vulnerability identification and remediation activities that include stakeholder notification?	Oracle SaaS Cloud Security Vulnerability Management Security Standard establishes the requirements to track and report vulnerabilities including identification and remediation updates. For more information on Critical Patch Updates, Security Alerts and Bulletins see Critical Patch Updates, Security Alerts and Bulletins.
TVM-10.1	Are metrics established, monitored, and reported for vulnerability identification and remediation at defined intervals?	Oracle SaaS Cloud security has defined metrics to monitor vulnerabilities as they are identified through remediation processes, including the Security Health Review and Vulnerability Management Advocacy Program to monitor all vulnerabilities and remediation steps monthly.
TVM-11.1	Are processes, procedures, and technical measures to apply guardrails to the AI system defined and implemented?	Guardrails are also used by Oracle Product Development to test the quality of an LLM response to a given prompt during the product development lifecycle. A Prompt Response can be scored (via Scoring Service) in a number of different ways (Readability, Repetitiveness, etc.) with the resulting score stored within the Metrics Store after each completion. The Scoring Service is

		utilized by the Oracle Dev & QA teams to evaluate prompt performance prior to promoting the AI feature into the release train. Currently deployed guardrails For SaaS Cloud Applications, Prompt Injection, Content Moderation.
TVM-11.2	Are guardrails continuously evaluated for changes in regulatory requirements and risk scenarios?	Guardrails within Oracle's SaaS Cloud Applications AI systems are evaluated for alignment with evolving regulatory requirements and emerging risk scenarios. The Guardrail Service systematically assesses LLM responses against use case-specific criteria–such as accuracy, toxicity, sentiment, and repetitiveness, returning a clear pass or fail outcome. Evaluation results and metrics are logged and reviewed, allowing Oracle SaaS Cloud Applications to detect trends, address compliance updates, and strengthen controls as regulations and risk landscapes change. This continuous feedback loop implements that deployed guardrails remain effective, and in accordance with Oracle's security and compliance standards.
TVM-12.1	Are threat analysis processes and procedures defined, implemented, and evaluated to identify, assess, and review the threat landscape for Cloud and AI systems?	Oracle has defined, implemented, and continuously evaluates threat analysis processes and procedures to identify, assess, and review the evolving threat landscape for Cloud and AI systems. This is accomplished through the Corporate Security Solution Assurance Process (CSSAP), a comprehensive security management review developed collaboratively by Oracle Security, and supporting IT organizations. CSSAP incorporates regular risk and threat assessments, alignment with industry standards and regulations, and proactive monitoring of new security challenges to implement Oracle Cloud and AI systems remain secured and compliant. For more information, please see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.
TVM-12.2	Are threat models built according to industry best practices to inform the risk mitigation strategy?	Our development lifecycle includes many other human-centric controls, notably including our Corporate Security Solution Assurance Process (CSSAP). This review process was developed by and includes representatives from our Security Architecture, Information Security, Product Security, Information Technology, and Legal organizations and other key stakeholders. It is designed to provide an information security management review for all our products and services, including those with AI systems, prior to deployment in production. More information on CSSAP is available at https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.
TVM-13.1	Is a risk-based method for the prioritization and mitigation of threats, used, leveraging an industry-recognized framework to guide threat decision-making and protection measures?	Oracle uses a risk-based approach guided by industry-recognized frameworks to prioritize and mitigate threats on the Oracle Fusion AI Platform. Through the Corporate Security Solution Assurance Process (CSSAP)–developed by a cross-functional team across Oracle Security, and other key IT organizations, we implement a comprehensive and systematic review of AI and cloud security. This process aligns with industry standards and incorporates risk

		assessment methodologies, enabling threat decision-making and protection measures that address evolving risks and compliance requirements across the AI lifecycle. For more information, please see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html.

Control Domain: Universal Endpoint Management

Question ID	Consensus Assessment Question	Oracle Response
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops, and mobile devices. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption. Oracle employees are required to comply with email instructions from Oracle Information Technology teams and are responsible for promptly reporting to the Oracle employee helpdesk any virus or suspected virus infection that cannot be resolved by antivirus software. Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobiledevices.html. Oracle SaaS Cloud Security maintains a security standard that follows the GIS Endpoint Device Security policy and legal Information Protection policy to implement security requirements for all Cloud SaaS user endpoint devices and Cloud SaaS Application user endpoint protection environments which hold customer data are protected and are aligned with industry standards and reviewed during re-accreditation.
UEM-01.2	Are the policies and procedures reviewed and updated at least annually or upon significant system changes?	Oracle Corporate Security policies (including policies that address universal endpoint management) are reviewed annually and updated as needed. Oracle SaaS Cloud Security maintains a security standard in accordance with the GIS Endpoint Device Security policy and Legal Information Protection policy that are reviewed annually and updated as needed.
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	This list is approved by Oracle Corporate Architecture and maintained by Oracle Information Technology. Oracle SaaS Cloud Security defines applicable requirements for Universal Endpoint Management (UEM) when accessing or storing Oracle SaaS Cloud data and privacy information.

UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Endpoint validation is performed by automation approved by Oracle Corporate Architecture and maintained by Oracle Information Technology. Oracle SaaS Cloud Security implements processes to validate endpoint device compatibility with operating systems and applications with the Universal Endpoint Management (UEM) services requirements.
UEM-04.1	Is an inventory of all endpoints used to store and process company data maintained?	Oracle's Information Systems Asset Inventory Policy requires that Line of Business (LOB) maintain accurate and comprehensive inventories of information systems, hardware and software.
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption. To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full disk encryption software on their laptops and desktops, except where approved for justifiable business purposes. Data on the disk can only be accessed through the use of a private key stored as a password-protected file on the disk. A preboot login manager allows authorized users to login to unlock the key, boot the operating system, and access the data. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html. Oracle SaaS Cloud Services devices that maintain Oracle SaaS Cloud customer information on user devices must be encrypted using an Oracle Corporate approved endpoint encryption solution that validates endpoint encryption compliance monitoring, and a local firewall is installed to enforce policies and security controls.
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Oracle SaaS Cloud Services devices have a secure desktop management software installed on interactive-used endpoints that is configured to require an automatic lock screen, automatically locks the screen after a defined period of inactivity. SaaS Cloud Applications enforce an automatic lock screen as a default setting that cannot be changed.
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	The Oracle Information Technology keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. OIT is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. OIT provides automation to verify antivirus configuration. Oracle employees are required to comply with email instructions from OIT and are responsible for promptly reporting to the Oracle employee helpdesk any virus or suspected virus infection that cannot be resolved by antivirus software. Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. For more information, see https://www.oracle.com/corporate/security- practices/corporate/laptopmobile-devices.html. Oracle SaaS Cloud follows the Endpoint Device Security Policy

		requirement to follow the change management process during security updates to endpoint operating systems and SaaS applications patches to protect all user endpoint devices.

UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption. To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full disk encryption software on their laptops and desktops, except where approved for justifiable business purposes. Data on the disk can only be accessed through the use of a private key stored as a password-protected file on the disk. A preboot login manager allows authorized users to login to unlock the key, boot the operating system, and access the data. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html. Oracle SaaS Cloud Services devices that maintain Oracle SaaS Cloud customer information on user devices must be encrypted using an Oracle Corporate approved endpoint encryption solution that validates endpoint encryption compliance monitoring, and a local firewall is installed to enforce policies and security controls.
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Antivirus software must be scheduled to perform threat definition updates and virus scans. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobiledevices.html.
UEM-10.1	Are software firewalls properly configured on managed endpoints?	Oracle SaaS Cloud follows the SaaS Network Security Standard for virtual firewall rules. The internal software firewalls are configured on endpoint devices to protect SaaS Cloud Applications.
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules in accordance with a risk assessment?	Oracle SaaS Cloud Applications do not have a commercial DLP deployed. Oracle SaaS Cloud Security workstations with access to scoped data and servers containing SaaS Cloud Services information is managed with DLP-type technologies to secure confidential information and endpoints.
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints, according to all applicable laws and regulations?	Unless required by regional or governmental regulations, geolocation capabilities are not in place for mobile endpoints.

UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Oracle SaaS Cloud Security sets forth the standards, procedures, and security requirements to secure desktop and mobile device management software with remote wipe capabilities. For more information please see: https://www.oracle.com/secure-global-desktop/#rc30p2.
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Oracle has formal requirements for its suppliers to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when: · Accessing Oracle and Oracle customers' facilities, networks and/or information systems. · Handling Oracle confidential information, and Oracle hardware assets placed in their custody. In addition, Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/ SaaS Cloud Security defines third-party security requirements for its suppliers to confirm they protect third-party information that is entrusted to them. The Oracle SaaS Cloud Third-Party Access Standard defines security controls that Oracle SaaS Cloud vendors and third parties must comply; technical and contractual measures that are defined, implemented, and evaluated when accessing Oracle SaaS Cloud Applications and services assets.