ORACLE

Consensus Assessment – Questionnaire (CAIQ) v4.0 for Oracle Fusion SaaS Cloud Applications

June 2023, | Fusion SaaS Cloud Applications - Version 4

PURPOSE STATEMENT

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

The answers contained in this CAIQ version 4.0 are related to specific Oracle SaaS Cloud Services as listed in the "Oracle SaaS Cloud Services in Scope" section below.

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

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

DISCLAIMER

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

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

ORACLE PRODUCTS IN SCOPE

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

- Human Capital Management: https://www.oracle.com/human-capital-management/
- Supply Chain and Manufacturing: https://www.oracle.com/scm/ (Excluding Logistics, Blockchain and IOT)
- Sales: https://www.oracle.com/cx/sales/ (Excluding Commerce, Configure-Price-Quote and Subscription Management)
- Enterprise Resource Planning: https://www.oracle.com/erp/ (Excluding Enterprise Performance Management (EPM))

Oracle Cloud at Customers services are excluded from the scope of this document. Service and Marketing cloud services are also excluded from the scope of this document.

CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ) VERSION 4

Control Domain: Audit & Assurance

Question ID	Consensus Assessment Question	Oracle Response
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained through Oracle's Business Assessment & Audit (BA&A) program. BA&A is an internal independent global audit organization which performs global process and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards and select laws and regulations across Oracle's Lines of Business and business units. Any key risks or control gaps identified by BA&A during these reviews are tracked through to remediation. These reviews, identified risks, or control gaps are confidential and shared with executive leadership and Oracle's Board of Directors. The audit rights of customers for whom Oracle processes data are described in the Oracle Data Protection agreement. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing. The audit rights of customers for Oracle services are described in the applicable Oracle Privacy Policy. For more information, see https://www.oracle.com/legal/privacy.
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Oracle Corporate Security policies (including Audit and Assurance policies) are reviewed annually and updated as needed. Fusion SaaS Cloud Applications standards supporting Oracle Corporate Security policies are reviewed annually and updated as needed.
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	See A&A-01.1. Oracle's Business Assessment & Audit (BA&A) is independent. Its operational activities and procedures are conducted at least annually in alignment with the Institute of Internal Auditors (IIA) Standards. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/business-assessment-audit/. Independent external audits and assessments of Fusion SaaS Cloud Applications are conducted at a minimum on an annual basis. Customers may request access to available audit reports for a particular Oracle SaaS Cloud Service through My Oracle Support (MOS) or via Sales.
A&A-03.1	Are independent audit and assurance assessments performed according to risk-	See A&A-01.1. Oracle's Business Assessment & Audit (BA&A) is independent. Its operational activities and procedures are conducted in compliance with Institute of Internal Auditors (IIA) and Oracle Risk Management Standard. Independent external audits and assessments of Fusion SaaS Cloud Applications are approved based on risk plans reviewed under Oracle risk policies and standards. For mor information, see; https://www.oracle.com/corporate/cloud-compliance/.

	based plans and policies?	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	The relevance of standards, regulations, legal/contractual and statutory requirements applicable to the audit are verified before the audit activity is approved. Compliance with those standards is to be verified by the Oracle Line of Business (LoB) or other relevant Oracle party before requesting the audit activity be approved. Oracle Legal monitors the global regulatory landscape to identify legislation applicable to Oracle, including regional and local teams monitoring changes in relevant jurisdictions. Oracle Legal, partners with Corporate Security and other organizations to manage Oracle's compliance to regulatory obligations across all lines of business.
		Fusion SaaS Cloud Applications engage with external assessment entities & independent auditors to verify that Fusion SaaS Cloud Applications have a comprehensive control environment that includes policies, processes, & security controls for the delivery of Oracle's applications, infrastructure & platform services. These efforts conform with ISO/IEC 27001 standards and Corporate Security Policies. For more information see: https://www.oracle.com/corporate/cloud-compliance/.
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	An audit management process inclusive of risk analysis, security control assessments, remediation schedules and reporting are in place for Fusion SaaS Cloud Applications and followed for internal and external audits.
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	A risk-based corrective action plan to remediate audit findings is in place. Any key risks or control gaps identified by Oracle's Business Assessment & Audit (BA&A) during these reviews are tracked through remediation. Risk-based corrective action plans to remediate audit findings are established, documented, and communicated to BA&A for approval before being applied and maintained by Oracle's Lines of Business with evaluation by BA&A and executive leadership.
		A risk-based corrective plan to remediate audit findings is in place. Any key risks or control gaps identified during an internal or external compliance assessment for Fusion SaaS Cloud Applications follows a defined process following a risk-based approach to remediation. This process is owned by the Oracle SaaS Compliance team.
A&A-06.2	Is the remediation status of audit	Risks, control gaps, and remediation statuses identified by Oracle's Business Assessment & Audit (BA&A) are shared with executive leadership and Oracle's Board of Directors.

	findings reviewed and reported to relevant stakeholders?	Fusion SaaS Cloud Applications remediation status of audit findings are reviewed and reported to appropriate stakeholders until findings are resolved.

Control Domain: Application & Interface Security

Question ID	Consensus Assessment Question	Oracle Response
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Application security policies and procedures are in place to support application security capabilities. Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience. Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at: **Reducing the incidence of security weaknesses in all Oracle products** Oracle Software Security Assurance key programs include Oracle's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups, and the use of automated analysis and testing tools. **Reducing the impact of security weaknesses in Oracle products and services** Oracle has adopted transparent security vulnerability disclosure and remediation practices. The company is committed to treating all customers equally and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs. **Fostering security innovations** Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help organizations implement and manage consistent security controls across the technical environments in which they operate, on-premises and in the cloud. For more information, see https://www.oracle.com/corporate/security-practices/assurance/.
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address application security) are reviewed annually and updated as needed. Fusion SaaS Cloud Applications Security standards supporting the Oracle Corporate Security policies are reviewed annually and updated as needed.
AIS-02.1	Are baseline requirements to secure different applications established,	Baseline requirements to secure applications are documented and maintained. Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/configuration.html

	documented, and maintained?	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Technical and operational metrics are in place to help ensure that business objectives, security requirements and compliance obligations continue to be met. Fusion SaaS Cloud Applications Service teams maintain a set of defined technical and operational metrics to help meet business objectives, security requirements and compliance obligations.
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Oracle employs formal Secure Coding Standards as a roadmap and guide for developers in their efforts to produce secure code. The standards discuss general security knowledge areas such as design principles, cryptography and communications security, common vulnerabilities, etc., and provide specific guidance on topics such as data validation, Computer Generated Imagery (CGI), user management, and more.
		Fusion SaaS Cloud Applications follow a defined SDLC process. Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Developing secure software requires consistently applied methodologies across the organization; methodologies that conform to stated policies, objectives, and principles. Oracle's objective is to produce secure code. To that end, Oracle requires that all of development abide by secure coding principles that have been documented and maintained to remain relevant. Additionally, Oracle has adapted its secure coding principles for use by our consulting and services organizations when they are engaged in producing code on behalf of our customers. For more information, see: https://www.oracle.com/corporate/security-practices/assurance/
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Fusion SaaS Cloud Applications have defined testing strategies as part of our Development Security Operations (DevSecOps) development principles. We consistently validate all SaaS application upgrades through a defined vulnerability testing process. Oracle regularly performs penetration and vulnerability testing and security assessments against the Oracle Cloud infrastructure, platforms, and applications. These tests are intended to validate and improve the overall security of Oracle Cloud services.

AIS-05.2	Is testing automated when applicable and possible?	Fusion SaaS Cloud Applications security testing includes both functional and non-functional and comprehensively tests for security vulnerabilities and weaknesses. Functional and non-functional security tests complement each other to provide security coverage of Fusion services. Application security vulnerability testing for Fusion SaaS Cloud Applications is automated to remediate when possible. All application security updates are delivered through security patches and this process is automated wherever possible.
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Cloud services are deployed in a specific configuration, or a small number of configurations. Testing must be performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment. Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/configuration.html.
		Strategies and capabilities are defined and implemented to deploy new code for Fusion SaaS Cloud Applications in a secure manner. Testing must be performed on the product in this configuration, with pre-deployment tests performed in an environment identical to the production environment. Development organizations are required to provide a capability where the security configuration of a cloud service can be evaluated against the secure configuration baseline in an automated manner, efficiently, consistently, and reliably across a fleet of instances. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/configuration.html.
AIS-06.2	Is the deployment and integration of application code automated where possible?	Fusion SaaS Cloud Applications use automated tools were applicable and available for integration, build and deployment of Fusion code.
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Application security vulnerabilities are identified and remediated following defined processes. Fusion SaaS Cloud Applications follow a clearly defined process for regularly testing, assessing, evaluating, and maintaining the effectiveness of the technical and organizational security measures described. Regular scans are conducted, Oracle Developers use static and dynamic analysis tools to detect security defects in Oracle code prior to deploying to production. Identified issues are evaluated and addressed in order of priority and severity. Oracle management tracks metrics regarding issue identification and resolution. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Fusion Application security vulnerabilities are remediated through the build and release pipeline. All application security updates are delivered through security patches and this process is automated whenever possible.

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?	Business continuity management and operational resilience policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained through the Risk Management Resiliency Program (RMRP). The objective of the RMRP is to establish a business-resiliency framework to help provide an efficient response to business interruption events affecting Oracle's operations. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/. The RMRP approach 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 goal of the program is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored. Each of these sub-programs is a uniquely diverse discipline. However, by consolidating emergency response, crisis management, business continuity, and disaster recovery, they can become a robust collaborative and communicative system. Oracle's RMRP is designed to engage multiple aspects of emergency management and business continuity from the onset of an event and to leverage them based on the needs of the situation. The RMRP is implemented and managed locally, regionally, and globally. The RMRP program management office provides executive scorecard reporting on program activities and status within the lines of business.
		Fusion SaaS Cloud Applications have a detailed SaaS Business Continuity / Disaster Recovery (BCDR) Program. The details of the SaaS Cloud Services BCDR program is covered under the Risk Management resiliency Program (RMRP). The program is driven by Policy documents like H&D Policy, DPA and SaaS Pillar Document. Risk Assessment, Business Impact Analysis and Business Continuity Plans are annually reviewed and updated. For operational purposes Crisis Communication Plan, DR Staffing Plan and Disaster Recovery Procedures are maintained. Periodic exercises are executed, and results are documented. Customer reports are published, and findings are followed through to completions. See for additional information: https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf https://www.oracle.com/a/ocom/docs/ocloud-hosting-delivery-policies-3089853.pdf https://www.oracle.com/content/published/api/v1.1/assets/CONTC1EA18FD31C648CFAC82B1CC2C186232/native/Data%20Processing%20Agreement%20for%20Oracle%20Services%20-%20010123.pdf?cb=_cache_ee77&channelToken=117bec9b3b4e4e90a1c4c9069d210baf&download=false
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including business continuity management and operational resilience policies) are reviewed annually and updated as needed.
		Fusion SaaS Cloud Applications Risk Assessment, Business Impact Analysis and Business Continuity Plans are reviewed annually and updated as needed.
BCR-02.1	Are criteria for developing business continuity and operational resiliency	Corporate business continuity policy, standards, and practices are governed by the RMRP Program Management Office (PMO) and are generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance. The disaster recovery test preparedness process has been developed following industry standards and best practices. This ensures that Oracle Fusion SaaS Cloud Service follows a repeatable defined process to ensure proper adherence to Oracle standards for Disaster Recovery. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/

	strategies and capabilities established based on business disruption and risk impacts?	To support the management and oversight of risk across all SaaS Cloud Applications, the SaaS Risk Management Program is aligned with the ISO 27000/31000 series, FedRAMP, NIST recommendations and applies across SaaS lines of business. This risk management framework 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 developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	The RMRP PMO develops planning materials and tools as aids to LoB Risk Managers in managing their business continuity plans, testing and training procedures. The RMRP program requires all LoBs to: • Identify relevant business interruption scenarios, including essential people, resources, facilities, and technology • Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Obtain approval from the LoB's executive For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/.
		Fusion SaaS Cloud Applications follows a definitive path of Risk Assessment and BIA on an annual basis. Followed by a schedule of exercises in line with policy document. Results are internally published, and findings are addressed through a remediation program.
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	See BCR-03.1
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	The critical LoBs (Includes Fusion SaaS Cloud Applications) are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. They must: • Conduct a Business Impact Analysis that specifies a Recovery Time Objective and Recovery Point Objective (if appropriate to the function) and identifies the organization's business continuity contingencies strategy • Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Revise business continuity plans based on changes to operations, business requirements, and risks For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/.
		Fusion SaaS Cloud Applications, Risk Assessment, Business Impact Analysis and Business Continuity Plans are documented, developed, maintained and updated to support business continuity and operational resilience plans.

BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Business Continuity and operational resilience documentation is available to internal authorized stakeholders.
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Oracle policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals of business continuity and operational resilience documentation for critical business operations.
		Fusion SaaS Cloud Applications Risk Assessment, Business Impact Analysis and Business Continuity Plan are reviewed annually and updated as necessary.
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	The critical LoBs (Includes Fusion SaaS Cloud Applications) are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/business-continuity.html.
		Fusion SaaS Cloud Applications conduct quarterly operational resilience table-top exercises and an annual end-to-end exercise.
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	The Risk Management Resiliency Program (RMRP) objective is to establish a business-resiliency framework to help provide an efficient response to business-interruption events affecting Oracle's operations. The RMRP is implemented and managed locally, regionally, and globally. The RMRP program is comprised of four Risk Management functions: 1. Emergency Response, managed by Real Estate Facilities Environment, Health and Safety Program 2. Crisis Management, managed by Global Physical Security 3. Business Continuity Management, managed by the corporate RMRP Program Management Office and operated by LOBs 4. Disaster Recovery, managed by LOBs, Information Technology teams and cloud Operations teams These reports are Oracle Confidential.
		Fusion SaaS Cloud Applications business continuity and resilience procedures include the following requirements: • Identify relevant business interruption scenarios, including essential people, resources, facilities, and technology • Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information • Obtain approval from the LoB's executive Results are published and findings are addressed through a remediation program.

<table>
<tr><td rowspan="2">BCR-08.1</td><td rowspan="2">Is cloud data periodically backed up?</td><td>Oracle has identified certain critical internal infrastructure systems that are backed up and can be restored. For these systems, Oracle performs the following backups as applicable:
Database: Full and incremental backups
Archive logs: Full and incremental backups
Source code repository backups performed on a recurring basis.</td></tr>
<tr><td>Fusion SaaS Cloud Applications periodically makes backups of the customer's production data in the Oracle Cloud Services for Oracle's sole use to minimize data loss in the event of an incident. The data is backed up to OCI's Object Storage Service (OSS). Backups are replicated to another Oracle-managed data center within the same region wherever possible.

<table><tr><th colspan="3">Fusion SaaS Cloud Services Backup Retention</th></tr><tr><th>BACKUP TYPE</th><th>FREQUENCY</th><th>RETENTION</th></tr><tr><td>Incremental</td><td>Daily</td><td>14 Days</td></tr><tr><td>Full</td><td>Weekly</td><td>60 Days</td></tr></table></td></tr>
<tr><td>BCR-08.2</td><td>Is the confidentiality, integrity, and availability of backup data ensured?</td><td>The confidentiality, integrity, and availability of backup data is tested via compliance with the Oracle SaaS standards. The standard requires at a minimum, backups be tested on an annual basis to ensure data can be restored during a catastrophic event. Testing must:
Demonstrate the ability to recover the data at the local data center and at a geographically remote disaster recovery site.
Be representative of the actual incident including retrieval from off-site storage, appropriate shipping, and realistic storage library setup of remote site.
Fusion 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.

Data and application backups are stored on disk and on OSS. Disks and OSS are encrypted. Only authorized personnel who have undergone appropriate training are allowed to access.</td></tr>
<tr><td rowspan="2">BCR-08.3</td><td rowspan="2">Can backups be restored appropriately for resiliency?</td><td>Oracle systems backup restoration tests are performed.</td></tr>
<tr><td>Fusion SaaS Cloud Applications backups can be restored appropriately for resiliency; Fusion SaaS Cloud Applications backups can be restored as needed to maintain resiliency. Backups are evaluated monthly for restorability. Reports and results are documented.</td></tr>
<tr><td rowspan="2">BCR-09.1</td><td rowspan="2">Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?</td><td>Oracle's corporate Disaster Recovery (DR) plan focuses on the resiliency of computing infrastructure supporting Oracle's internal operations and cloud services. Oracle's production data centers are geographically separated and have component and power redundancy, with backup generators in place for availability of data center resources in case of a disaster, whether natural or man-made.
For more information, see https://www.oracle.com/corporate/security-practices/corporate/resilience-management/disaster-recovery.html.</td></tr>
<tr><td>Fusion SaaS Cloud Applications complies with Oracles Risk Management Resiliency Program (RMRP) indicating functional business continuity planning is managed by the Risk Manager within each Line of Business (LoB). Fusion SaaS Cloud Applications is required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes</td></tr>
</table>

BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Fusion SaaS Cloud Applications DR and BCR plans are reviewed annually and updated as needed. This is part of the Functional business continuity planning managed by the Risk Manager within each Line of Business (LoB). The critical LoBs are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes.
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Fusion SaaS Cloud Applications perform three tabletop exercises and one functional failover/switchover exercise annually.
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	Local emergency authorities are not included in the exercises.
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Oracle maintains a redundant network infrastructure, including DNS servers to route between primary and secondary sites, network devices, and load balancers. Oracle cloud data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
		Oracle deploys the Fusion SaaS Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services. Oracle Fusion includes an extensive 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 geographically located at a different location than the production site. For more information, please refer to the following documents: • https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf • Oracle Cloud Hosting and Delivery Policies: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html#hd. • Oracle SaaS Cloud Services: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html#saas.

Control Domain: Change Control & Configuration Management

Question ID	Consensus Assessment Question	Oracle Response

CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, and maintained (regardless of whether asset management is internal or external)?	Oracle Fusion SaaS Cloud Applications follows formal change management procedures to provide review, testing, and approval of changes prior to deployment in the Oracle Cloud production environment. Changes made through change management procedures include system and service maintenance activities, management of application upgrades and updates, and coordination of customer specific changes where required. For changes to your services that are governed by Oracle's change control procedures please see: Oracle Cloud Hosting and Delivery Policies.
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Oracle Fusion SaaS Cloud Applications adhere to Oracle Corporate policies and review standards annually and updated as needed.
CCC-02.1	Is a defined quality change control, approval, and testing process (with established baselines, testing, and release standards) followed?	Oracle Fusion Cloud Applications use a standard change management and testing process designed for the purpose of ensuring availability, confidentiality, and integrity. Risks associated with changing Fusion SaaS Cloud Applications are assessed as defined in the Oracle Cloud Operations SaaS Change Management Standard. Weekly formal change reviews through a Change Advisory Board (CAB) are recommended across all Cloud product LOBs to ensure proper transparency with all key stakeholders.

CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Oracle Corporate Security Solution Assurance Process (CSSAP) is a security review process developed by Corporate Security Architecture, Global Information Security, Global Product Security, Oracle Global IT, and Oracle's IT organizations to provide comprehensive information-security management review. CSSAP helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be carried out throughout the project lifecycle: Pre-review: the risk management teams in each line of business must perform a pre-assessment of each project using the approved template CSSAP review: the security architecture team reviews the submitted plans and performs a technical security design review Security assessment review: based on risk level, systems and applications undergo security verification testing before production use Reviews ensure that projects are aligned with: Oracle Corporate Security Architecture strategy and direction Oracle Corporate security, privacy and legal policies, procedures and standards For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
		Risks assoicated with changing Fusion SaaS Cloud Applications are assessed as defined in the Oracle Cloud Operations SaaS Change Management Standard. Weekly formal change reviews through a Change Advisory Board (CAB) are recommended across all Cloud product LOBs to ensure proper transparency with all key stakeholders.
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted	Oracle's Network Security Policy establishes requirements for network management, network access and network device management, including authentication and authorization requirements for both physical devices and software-based systems. Unused network ports must be deactivated. Acceptable Use Policy also supports restrictions of adding, removing and management of organizational assets. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html.
		Oracle policies and standards are in place outlining restrictions for adding, removing and updating Oracle assets. Additionally, technical restrictions are in place were possible.
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements	Oracle's SaaS Cloud Services do not involve customer owned environments unless the customer creates connections via approved APIs. Oracle aims to ensure API updates are not disruptive to CSC-owned environments. For more information see: https://docs.oracle.com/search/?q=api&category=cloud&product=en%2Fcloud%2Fsaas

	(SLAs) between CSPs and CSCs?	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Change management baselines are established for all relevant authorized changes on Fusion SaaS Cloud Applications assets.
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Detection measures are implemented with proactive notification for changes that deviate from established baseline configurations. Fusion SaaS Cloud Applications use a centralized system for managing the access and integrity of device configurations. Change controls are in place to ensure only approved changes are applied. Regular audits are performed to confirm compliance with security and operational procedures. Also, internal weekly scans are performed on the infrastructure.
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Fusion SaaS Cloud Applications has implemented standards and procedures to manage exceptions, including emergencies, in the change and configuration process.
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	Please see CCC-01.1 Fusion SaaS Cloud Applications exception process aligns with the GRC-04: Policy Exception Process.
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in	Processes are in place to proactively roll back changes to a previously known “good state”. Standard operating procedures (SOP) define the steps to follow, including implementation, pre/peri/post validation, and rollback, as applicable.

	case of errors or security concerns?	

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, and key management requirements. Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to use up-to-date versions of approved security-related implementations. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms. Oracle's Information Protection Policy defines high-level requirements for protecting data via encryption when data is at rest (in storage) on laptops, devices, and removable media. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/
		Fusion SaaS Cloud Applications adheres to documented standards supporting Oracle corporate encryption and key management policies. These standards are documented, managed, communicated, applied, and evaluated. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies and standards (including polices and standards 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's Cryptography Review Board (CRB) defines and promotes cryptography-related technical standards for Oracle products and services. The group is primarily responsible for making technical decisions and authoring internal standards to address government and industry requirements. Representatives from Corporate Security and development organizations define best practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence. CRB's responsibilities include: Creating and maintaining standards for cryptography algorithms, protocols, and their parameters Providing approved standards in multiple formats, for readability and automation Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle Providing practical guidance on using cryptography Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography For more information, see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html
		Fusion SaaS Cloud Applications adheres to the Oracle OSSA Cryptography and OSSA Key Management standards.

CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Data at-rest and in-transit is cryptographically protected using cryptographic libraries certified to approved standards. Solutions for managing encryption keys and cryptographic libraries at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). Oracle defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include: • Locations and technologies for storing encryption keys • Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures • Changing default encryption keys • Replacement schedule for various types of encryption keys For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
		Fusion SaaS Cloud Applications adheres to the Oracle OSSA Cryptography and OSSA Key Management standards.
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to only use up-to-date versions of approved security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
		Appropriate data protection encryption algorithms are used based on data classification, associated risks, and encryption technology usability for Fusion SaaS Cloud Applications. All Customer data is classified as "Confidential – Internal Only" or higher. Each tablespace within the Database has its own encryption key (AES-128). Tablespace keys are stored and encrypted (AES-128) within the Oracle by the master encryption key or key encryption key (KEK) which is encrypted using AES-256 and there is a unique KEK for each tenant. Backups are encrypted with tenant specific keys. When using Break Glass for Fusion SaaS Cloud Applications, the Master Transparent Data Encryption (TDE) key is stored in a FIPS 140-2, Level 3-certified HSM and customers can generate their own master TDE key and then reset, revoke, or restore the key.
CEK-05.1	Are standard change management procedures established to review, approve, implement, and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Change management procedures are established to review, approve, implement, and communicate changes. Formal change management processes are mandatory for all Oracle cryptography changes that occur. Oracle defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
		Oracle Fusion SaaS Applications adhere to the Oracle SaaS Change Management Standard which supports Corporate Policies and procedures for Change Management.

CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Solutions for managing encryption keys at Oracle must be approved per Corporate Security Solution Assurance Process (CSSAP). Oracle defines requirements for encryption, including cipher strengths, key management, generation, exchange/transmission, storage, use, and replacement. Specific requirements in this standard include: Locations and technologies for storing encryption keys Controls to provide confidentiality, availability, and integrity of transmitted encryption keys, such as digital signatures Changing default encryption keys Replacement schedule for various types of encryption keys For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html
		Fusion SaaS Cloud Applications changes to cryptography, encryption and key management related systems, policies and procedures are managed and adopted to account for downstream effects of the changes, including residual risk based on a cost-benefit analysis. Oracle's Cryptography Review Board oversees cryptography governance. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Oracle's Cryptography Review Board oversees cryptography governance. Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services. The group is primarily responsible for making technical decisions and authoring internal standards to address government and industry requirements. Representatives from Corporate Security and development organizations define best practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence. CRB's responsibilities include: Creating and maintaining standards for cryptography algorithms, protocols, and their parameters Providing approved standards in multiple formats, for readability and automation Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle Providing practical guidance on using cryptography Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography For more information, see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
		Fusion SaaS Cloud Applications adhere to Oracles formal Approved Cryptography Standard.
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	Fusion SaaS Cloud Applications provide CSCs with the capacity to manage their own data encryption keys (where applicable) with services such as (Break Glass) For more information, please see: https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/overview-oracle-break-glass.html

CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Encryption and key management systems, policies and processes are audited as part of our compliance function. Please see CEK-01.1
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Encryption and key management systems, policies, and processes are audited, at a minimum, on an annual basis.
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Oracle has formal cryptography, encryption, and key management requirements. Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services 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. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Oracle has a formal Key Management Program supported by processes, procedures, and recommendations (aligned with NIST controls) that define specifics regarding key provisioning. Oracle policy and standards require all keys be managed securely. Oracle Fusion SaaS Cloud Application uses Public Key infrastructure to secure customer provided KEKs to the HSM, inside of which the KEK is decrypted. HSMs are used to protect keys, wherever Break Glass is deployed. See: https://www.oracle.com/security/cloud-security/key-management/

CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Oracle has a formal Key Management Program supported by processes, procedures, and recommendations (aligned with NIST controls) that define specifics regarding key rotation. For Fusion SaaS Cloud Applications, cryptographic key rotation occurs based on regulation, certification, or for other security reasons. Customers with a subscription to Break Glass can manage their own keys and rotate those keys as needed.
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Cryptographic keys are revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions. Fusion SaaS Cloud Applications has procedures and processes to revoke and remove cryptographic keys before the end of the established cryptoperiod (e.g., when a key is compromised, or an entity is no longer part of the organization.)

CEK-14.1	Are processes, and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Oracle has defined processes and technical measures in place that defines the approved methods for key destruction, revocation of keys stored in hardware security modules and that address legal and regulatory requirements. These standards are part of the OSSA (Oracle Software Security Assurance Practices). Fusion SaaS Cloud Applications has established and implemented procedures to enforce segregation of key management and key usage duties. Key management encompasses the entire life cycle of cryptographic keys and has identified a method for establishing and managing keys in each management phase from generation, installation, storage, rotation, and destruction.
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Fusion SaaS Cloud Applications adheres to Oracle Software Security Assurance Practices for all HSMKey`1 practices. Processes, procedures, and technical measures are in place to create keys in a pre-activated state. Keys are not created prior to authorization to use. https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/controllingtde-keys.html
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state	Fusion SaaS Cloud Applications adheres to Oracle Software Security Assurance Practices for all key management practices. Processes, procedures, and technical measures are in place to monitor, review and approve key transitions. Processes include: • Generating Your TDE Master Key • Resetting TDE Master Encryption Key

	to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	• Revoking Your TDE Master Encryption Key • Restoring Your TDE Master Encryption Key https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/controllingtde-keys.html
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Fusion SaaS Cloud Applications adheres to Oracle Software Security Assurance Practices for all key management practices. Processes, procedures, and technical measures are in place to deactivate keys as required. Processes include: • Generating Your TDE Master Key • Resetting TDE Master Encryption Key • Revoking Your TDE Master Encryption Key • Restoring Your TDE Master Encryption Key https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/controllingtde-keys.html
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Fusion SaaS Cloud Applications adheres to Oracle Software Security Assurance Practices for all key management practices. Processes, procedures, and technical measures are in place to manage archived keys in a secure repository. Processes include: • Generating Your TDE Master Key • Resetting TDE Master Encryption Key • Revoking Your TDE Master Encryption Key • Restoring Your TDE Master Encryption Key https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/controllingtde-keys.html
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios	Oracle Fusion Cloud Applications adhere to OSSA Cryptography Standard which adheres to the Oracle Corporate security's formal policies and procedures governing the use of encryption. Oracle Fusion SaaS Cloud Applications have formal processes, procedures, and technical measures for encrypting customer data in transit (e.g., HTTPS TLS 1.2, SFTP) and at rest (e.g., currently AES-256).

	(e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Processes, procedures and technical measures to assess operational continuity risks are defined, implemented and evaluated to include legal and regulatory requirement provisions.
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and	Key management system processes, procedures and technical measures are defined, implemented, and evaluated to track and report all cryptographic materials and status changes including legal and regulatory requirements. Oracle's Cryptography Review Board oversees cryptography governance. Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services. The group is primarily responsible for making technical decisions and authoring internal standards to address government and industry requirements. Representatives from Corporate Security and development organizations define best practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence. CRB's responsibilities include: • Creating and maintaining standards for cryptography algorithms, protocols, and their parameters • Providing approved standards in multiple formats, for readability and automation • Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle • Providing practical guidance on using cryptography

	status changes that include legal and regulatory requirements provisions?	• Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography For more information see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-product-security.html See also: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html

Control Domain: Data Center Security

Question ID	Consensus Assessment Question	Oracle Response
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Oracle's Media Sanitization and Disposal Policy specifies requirements including secure disposal of equipment and media used for data storage. This policy is established, documented, approved, communicated, enforced, and maintained as part of Oracle Security Policy. Fusion SaaS Cloud Applications have processes and procedures to comply with Oracle's Media Sanitization and Disposable Policy and Enterprise Engineering Media Sanitization and Disposal Standard. Development of this standard has been guided by Corporate Information Security Policies, guidance from NIST SP800-88 Rev. 1 and has been adapted to align with Oracle policies and standard practices. This standard is designed to ensure compliance with Oracle Policy and provides Line of Business specific requirements that meets Policy.
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Oracle's Media Sanitation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. Fusion SaaS Cloud Applications adheres to Oracles Media Sanitization and Disposal Policy. This policy aligns with NIST SP800-88 Rev. 1.
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's	Oracle Corporate Security policies (including polices 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?	
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?	Policies and procedures for the relocation or transfer of Oracle assets is documented, approved, communicated, implemented, enforced, and maintained. Standards for handling assets and the security requirements to undertake when transferring assets is addressed.
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Fusion SaaS Cloud Applications require authenticated customers requesting a relocation of their services to submit a formal request via My Oracle Support (MOS). Only approved and authenticated customers have access to use this 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?	Oracle Corporate Security policies (including polices that address the relocation or transfer of hardware, software, or data/information to any location) are reviewed annually and updated as needed. Fusion SaaS Cloud Applications adhere to Oracle's Corporation Security policies.
DCS-03.1	Are policies and procedures for maintaining a safe and secure working	Policies and procedures for maintaining a safe and secure working environment is in place. Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html

	environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address safe and secure working environments) are reviewed annually and updated as needed.
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Policies and procedures for the secure transportation of physical media are established, documented, approved, communicated, enforced, evaluated, and maintained. For more informattion, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address the secure transportation of assets) are reviewed annually and updated as needed.
DCS-05.1	Is the classification and	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/c corporate/information-assets-classification.html

	documentation of physical and logical assets based on the organizational business risk?	Per Oracle Information Protection Policy, Fusion SaaS Cloud Applications information assets are classified according to the sensitivity and criticality of information they store, transmit, and receive.
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	The Oracle Information Systems Inventory Policy requires that Line 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.
		Fusion SaaS Cloud Applications catalogues and tracks assets in adherence with 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. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html.
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Oracle Global Physical Security uses a risk-based approach for physical and environmental security. Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html
		Fusion SaaS Cloud Applications have physical security perimeters implemented to safeguard personnel, data, and information systems. The Oracle Cloud Hosting and Delivery Policies contain a description of physical security controls. Oracle provides secured computing facilities for both office locations and production cloud infrastructure. Common controls between office locations and Oracle controlled co-locations/datacenters currently include for example: o Physical access requires authorization and is monitored. o All employees and visitors must visibly wear official identification while onsite o Visitors must sign a visitor's register and be escorted and/or observed while onsite o Possession of keys/access cards and the ability to access the locations is monitored. Staff leaving Oracle employment must return keys/cards Additional physical security safeguards are in place for Oracle controlled Cloud data centers, which currently include safeguards such as: o Premises are monitored by CCTV. o Entrances are protected by physical barriers designed to prevent unauthorized entry by vehicles o Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and	The goal is to balance prevention, detection, protection, and response, while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. Physical security perimeters are established between administrative, business areas and processing/hosting locations.

	processing facilities?	Oracle has implemented physical security perimeters between administrative and business areas and processing facilities. Oracle leverages an integrated security management system with electronic photo ID badges, cardholder access control, biometrics, recorded digital video surveillance, and alarm monitoring. Main entrances are staffed 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management. Intrusion detection alarm systems and a 24x7 security protection unit, secure the building perimeter.
DCS-08.1	Is equipment identification used as a method for connection authentication?	Equipment identification is used as a method for connection authentication. The VPN that Oracle staff use to connect to Oracle Fusion SaaS Cloud Applications uses machine certificates and other identifiers to validate that the device is Oracle owned and provisioned before allowing access to resources. Fusion 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/physical-environmental.html
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors. Visitors are required to sign a visitor's register, be escorted and/or observed when they are on Oracle premises, and/or be bound by the terms of a confidentiality agreement with Oracle. Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving Oracle's employment must return keys/cards and key/cards are deactivated upon termination. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html

DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Oracle use a mixture of 24/7 onsite security officers or patrol officers, depending on the risk/protection level of the facility. In all cases officers are responsible for patrols, alarm response, and recording of security incidents. Oracle has implemented centrally managed electronic access control systems with integrated intruder alarm capability. The access logs are kept for a minimum of six months. The retention period for CCTV monitoring and recording ranges from 30-90 days minimum, depending on the facility's functions and risk level. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Personnel are trained in incident response and escalation procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Processes, procedures, and technical measures are in place to ensure risk-based protection of Oracle data centers. Data centers hosting Oracle cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria. Oracle cloud service data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Personnel are trained in incident response and escalation procedures to address security and availability events that may arise. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall	See DCS-12.1

	within accepted industry standards effectively implemented and maintained?	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	See DCS-12.1
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	See DCS-12.1

Control Domain: Data Security & Privacy Lifecycle

Question ID	Consensus Assessment Question	Oracle Response
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable	Oracle's information-asset classification determines corporate data-security requirements for Oracle-managed systems and data. 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 Legal closely monitors the global regulatory landscape to identify legislation applicable to Oracle, including regional and local teams monitoring changes in relevant jurisdictions. Oracle Legal partners with Corporate Security and other organizations to manage Oracle's compliance to regulatory obligations across all lines of business. For more information, see https://www.oracle.com/legal/ Oracle Global Trade Compliance (GTC) is responsible for import and export oversight, guidance, and enforcement to enable worldwide trade compliant processes across Oracle. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-trade-compliance.html Customer remains solely responsible for its regulatory compliance in its use of any Oracle Cloud services. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
		Fusion SaaS Cloud Applications adhere to Oracle's Information Asset Classification Policy. The SaaS Cloud PI Data Protection Standard supports this compliance.

	laws and regulations, standards, and risk level?	
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address data security and privacy) are reviewed annually and updated as needed.
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Industry accepted methods are applied for secure data disposal from storage media. Oracle's Media Sanitation and Disposal Policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/ Fusion SaaS Cloud Applications adheres to Oracle's Media Sanitization and Disposal Policy.
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Data inventory of sensitive and personal information is maintained by Fusion SaaS Cloud Applications. This documentation is for internal use only. Fusion HCM SaaS Cloud Applications provides its customers with a data dictionary. Information regarding tables, views, and columns can be found here: https://docs.oracle.com/cloud/farel12/globalcs_gs/OEDMH/HCM_Tables_and_Views_Overview.htm#TablesAndViewsOverview-CF2A89FB
DSP-04.1	Is data classified according to type and sensitivity levels?	Oracle Oracle's formal Information Protection Policy sets forth the requirements for classifying and handling public and confidential information. Oracle categorizes information into four classes—Public, Internal, Restricted, and Highly Restricted—with each classification requiring corresponding levels of security controls, such as encryption requirements for non-Public data: For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Data flow documentation is created and maintained by Fusion SaaS Cloud Applications. This documentation is for internal use only. Oracle Fusion SaaS Cloud Applications diagrams are available during a client audit. Customer audits may be performed annually per the Oracle Data Processing agreement, section 7. Please see: https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Data Flow documentation is reviewed at least annually and updated as needed.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Oracle's Information Systems Asset Inventory Policy requires that Line of Business (LoB) 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	Is data ownership and stewardship documentation reviewed at least annually?	Oracle Corporate Security policies (including polices that address ownership and stewardship) are reviewed annually and updated as needed.
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Systems, products, and business practices are based on security principles by design and per international security standards and best practices. Oracle's security policies and practices cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27001:2013 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27002:2022 standards. Some Oracle products and services are certified per specific industry and government standards such as ISO/IEC 27001:2013, AICPA SSAE Number 18 (SOC), Payment Card Industry Data Security Standards (PCI DSS) and other standards.
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Systems, products, and business practices are based on privacy principles by design and per industry best practices. Oracle's privacy policies and practices cover the management of privacy for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO 27018 and SSAE18 SOC1 / SOC2.
DSP-08.2	Are systems' privacy settings configured by default and according to all	Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html Fusion SaaS Cloud Applications privacy settings are configured following a Privacy by Design (PbD) methodology and according to applicable laws and regulations. Fusion SaaS Cloud Applications adopt Privacy by Design best practices https://www.oracle.com/legal/privacy/services-privacy-policy.html

	applicable laws and regulations?	
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations, and industry best practices?	Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html Oracle Legal teams perform DPIAs. Oracle Fusion SaaS Cloud Applications performs impact assessments for all new products and feature enhancements we wish to bring to market.
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Processes, procedures, and technical measures are in place to ensure transfer of sensitive data is protected from unauthorized access and is compliant with data transfer laws and regulations. Oracle has BCR/P in place as well as an approved Data Protection Agreement (DPA.) See the following links for additional information: https://www.oracle.com/ie/corporate/contracts/cloud-services/contracts.html https://www.oracle.com/ie/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf Fusion SaaS Cloud Applications, secure file transfer functionality, 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 secured location, most commonly for data import/export on the Oracle Cloud hosted service or downloading files at service termination. All uploaded files are scanned using Internet Content Adaptation Protocol (ICAP) before being stored in the cloud service.
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request	Processes, procedures, and technical measures are defined and implemented to enable Data Subject Rights Requests to access, modify, or delete personal data. Note: Oracle is not the controller of the data. If Oracle directly receives any requests or inquiries from Individuals, it will promptly pass on such requests to customer without responding to the Individual. Otherwise, Oracle will advise the Individual to identify and contact the relevant controller(s). Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html

	access to, modify, or delete personal data (per applicable laws and regulations)?	
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html See DSP-10.1
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Oracle complies with all applicable laws and regulations. For more information, see https://www.oracle.com/legal/privacy/ Fusion SaaS Cloud Applications 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 Personal Information, are subject to appropriate written confidentiality arrangements, including regular training on information protection, and compliance with Oracle policies concerning protection of confidential information.
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to	Process, procedures, and technical measures are defined, implemented, and evaluated as part of Oracle Privacy policies. Please see the following for additional information. https://www.oracle.com/ie/legal/privacy/

	the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Fusion SaaS Cloud Applications has processes, procedures, and technical measures defined and implemented to disclose details to data owners of any personal or sensitive data access by sub-processors. To the extent Oracle engages Oracle affiliates and third-party sub processors to have access to Services Personal Information to assist in the provision of Services, such sub-processors shall be subject to the same level of data protection and security as Oracle under the terms of Your order for Services. Oracle is responsible for its sub- processors' compliance with the terms of Your order for Services. Oracle maintains lists of Oracle affiliates and sub processors that may process Services Personal Information. Additional information is available to You via My Oracle Support (https://support.oracle.com) Document ID 2121811.1, or other applicable primary support tool provided for the Services. Please refer to the Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Replicating or using production data in non-production environments is not performed at Oracle. Oracle will not use customer data in non-production environments or for testing purposes. Production and non-production environments are logically and physically segregated. Additionally, procedures are in place to ensure production data is not used in non-production environments. 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. For More information, please see: https://docs.oracle.com/cd/E25178_01/fusionapps.1111/e14496/securing.htm#BCGBHCDC.
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	During the use of Oracle Fusion 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. Customer data is that data uploaded or generated for use within the subscribed Oracle SaaS Cloud Services. Oracle Cloud Hosting and Delivery Policies describe the Oracle SaaS Cloud Services Continuity Policy, Oracle SaaS Cloud Services High Availability Strategy, Oracle SaaS Cloud Services Backup Strategy and Oracle SaaS Cloud Services Level Agreement: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html.
		Fusion SaaS Cloud Applications 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 Fusion 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. Customer data is data uploaded or generated for use within the subscribed Oracle SaaS Cloud Services. Oracle Cloud Hosting and Delivery Policies describe the Oracle SaaS Cloud Services Continuity Policy, Oracle SaaS Cloud Services High Availability Strategy, Oracle SaaS Cloud Services Backup Strategy and Oracle SaaS Cloud Services Level Agreement: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to	Oracle Fusion SaaS Cloud Applications have policies, practices, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle. Customer remains solely responsible for their user access to the service provided. During the use of Oracle Fusion SaaS Cloud Applications Oracle Cloud customers maintain responsibility for their data residing in their environment. Oracle SaaS Cloud Services provide a variety of

	protect sensitive data throughout its lifecycle?	configurable information protection services as part of the subscribed service. Customer data is data uploaded or generated for use within the subscribed Oracle SaaS Cloud Services. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/data-protection/
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	For Oracle Fusion Applications, please see: https://www.oracle.com/contracts/cloud-services/ Oracle will promptly inform You (Customer) of requests to provide access to Personal Information, unless otherwise required by law.
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Please see https://www.oracle.com/contracts/cloud-services/ Oracle will promptly inform You (Customer) of requests to provide access to Personal Information unless otherwise required by law.
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Fusion SaaS Cloud Applications 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 Oracle Fusion Applications, please see https://www.oracle.com/contracts/cloud-services/

Control Domain: Governance, Risk & Compliance

Question ID	Consensus Assessment Question	Oracle Response
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Information governance program policies and procedures sponsored by organizational leadership is established, documented, approved, communicated, applied, evaluated, and maintained. Global Information Security (GIS) defines policies for the management of information security across Oracle. Additionally, GIS sets direction and provides advice to help protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners, and employees. GIS also coordinates the reporting of information security risk to senior leadership including the Oracle Security Oversight Committee and Board of Directors. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address governance, risk, and compliance) are reviewed annually and updated as needed. Fusion SaaS Cloud Applications standards and procedures (including those that address governance, risk, and compliance) are reviewed annually and updated as needed.
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of	Oracle has an established, formal, documented and leadership-sponsored enterprise risk management program that includes policies which direct Oracle LoBs to have procedures and standards for identification, evaluation, ownership, treatment and acceptance of cloud security and privacy risks. Corporate Security Architecture manages a cross-organization working group focused on security architecture (including policy for the management of security risks), with the goal of collaboratively guiding security for Oracle cloud services. Participation includes members from Oracle cloud service development, operations, and governance teams. Oracle Privacy & Security Legal manages the cross-organization oversight of privacy risks. For more information, see https://www.oracle.com/legal/privacy/. The Chief Corporate Architect, who reports directly to the Executive Chairman and Chief Technology Officer (CTO), is one of the directors of the Oracle Security Oversight Committee (OSOC). The Chief Corporate Architect manages the Corporate Security departments which guide security controls at Oracle. These departments drive the corporate security programs, define corporate security policies, and provide global oversight for Oracle's security policies and requirements.

	cloud security and privacy risks?	
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Oracle Corporate Security policies (including policies that address governance, risk, and compliance) are reviewed annually and updated as needed.
		Fusion SaaS Cloud Applications standards and procedures (including those that address cloud security and privacy risks) are reviewed annually and updated as needed.
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Global Information Security (GIS) manages a security exception management process to review deviations from corporate information security policies.
		Fusion SaaS Cloud Applications adhere to Corporate Policies including an approved exception process when deviations from policy occur.
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Oracles Information security program (including programs of all relevant CCM domains) has been developed and implemented. Oracle's security policies cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, including employees and contractors. These policies are aligned with the ISO/IEC 27001:2013 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27002:2022 standards. Some Oracle products and services are certified per specific International, industry and government standards such as ISO/IEC 27001:2013 AICPA SSAE Number 18 (SOC), Payment Card Industry Data Security Standards (PCI DSS) and other standards. Fusion SaaS Cloud Applications are CSA STAR certified. The CCM is used as the standard to assess the security posture of organizations on the Security, Trust, Assurance and Risk (STAR) registry.
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance	See GRC-05.1

	programs defined and documented?	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	All relevant standards, regulations, legal/contractual, and statutory requirements applicable to Oracle are identified and documented. Oracle Legal monitors the global regulatory landscape to identify legislation applicable to Oracle, including regional and local teams monitoring changes in relevant jurisdictions. Oracle Legal partners with Corporate Security and other organizations to manage Oracle's compliance to regulatory obligations across all lines of business. In addition, Oracle Global Trade Compliance (GTC) is responsible for import and export oversight, guidance, and enforcement to enable worldwide trade compliant processes across Oracle. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/global-trade-compliance.html. Customer remains solely responsible for its regulatory compliance in its use of any Oracle Cloud services. Customer must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Oracle is a member of the Information Technology-Information Sharing and Analysis Center (IT-ISAC) organizations. For more information, see: https://www.it-isac.org/home and https://openssf.org/about/members/

Control Domain: Human Resource Security

Question ID	Consensus Assessment Question	Oracle Response
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved,	In accordance with Oracle policy, background checks are required for individuals being considered for employment. For more information, see https://www.oracle.com/corporate/careers/background-check.html

	communicated, applied, evaluated, and maintained?	
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	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 Corporate Security policies (including polices that address candidate 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 employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services. For more information, see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html

HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally owned or managed assets reviewed and updated at least annually?	Oracle Corporate Security policies (including the Acceptable Use Policy) are reviewed annually and updated as needed. Oracle has formal requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, internet access, enterprise data, customer data, and other company resources available to Oracle employees, contractors and visitors. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Policies and procedures requiring unattended workspaces and data handling procedures are documented. In addition, each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy. For more information see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Oracle Corporate Security policies (including policies that address data handling) 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,	Policies and procedures to protect information accessed, processed, or stored at remote sites and locations are established, documented, approved, communicated, applied, evaluated, and maintained. Oracle Global Information Security (GIS) defines policies for the management of information security across Oracle. The Oracle Information Protection policy specifically defines proper handling of data based on its classification. For more information see: https://www.oracle.com/corporate/security-practices/corporate/governance/global-information-security.html Data centers hosting cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk

	documented, approved, communicated, applied, evaluated, and maintained?	manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria. For more information, see https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Oracle Corporate Security policies (including polices intended to protect information accessed, processed, or stored at remote sites and locations) are reviewed annually and updated as needed.
HRS-05.1	Are return procedures of organizationally owned assets by terminated employees established and documented?	Procedures are in place to have all company owned assets returned upon employee termination.
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems,	Please see HRS-02.1

	resources, and assets?	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Please see HRS-02.1
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Employee roles and responsibilities relating to information assets and security are documented and communicated. 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 data classification. Oracle's corporate security controls can be grouped into three categories: administrative, physical, and technical security controls. • Administrative controls, including logical access control and human resource processes • Physical controls designed to prevent unauthorized physical access to servers and data-processing environments • Technical controls, including secure configurations and encryption for data at rest and in transit For more information, see https://www.oracle.com/corporate/security-practices/corporate/data-protection/ 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
		Fusion SaaS Cloud Applications adhere to the SaaS Logical Access Controls Standard and supports the Oracle Corporate Security Policies (Logical Access Control Policies).
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?	See HRS-02.1
HRS-11.1	Is a security awareness training	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Security reviews, assessments, and audits are conducted periodically to confirm compliance with Oracle information-security policies, procedures, and

	program for all employees of the organization established, documented, approved, communicated, applied, evaluated, and maintained?	practices. Employees who fail to comply with these policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy. For more information, see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
HRS-11.2	Are regular security awareness training updates provided?	See HRS-11.1
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	See HRS-11.1
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	See HRS-11.1
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established	See HRS-11.1

	policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	

Control Domain: Identity & Access Management

Question ID	Consensus Assessment Question	Oracle Response
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	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/corpoate/security-practices/corporate/access-control.html Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services.
		Fusion SaaS Cloud Applications Logical Access Controls Standard is documented, approved, communicated, implemented, applied, evaluated, and maintained. Focus is on access to the Fusion SaaS Cloud Applications environment by Oracle staff. Fusion SaaS Cloud Service customers manage access for their users. Functionality to do so is provided in Fusion Applications.
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including policies applicable to identity and access management) are reviewed annually and updated as needed.
		Fusion SaaS Cloud Applications standards (including the SaaS 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,	Strong password policies and procedures are established, documented, approved, communicated, implemented, applied, evaluated, and maintained. Oracle has strong password policies (including length and complexity requirements) for the Oracle network, operating system, email, database and other accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. Identity management systems are required to comply with Corporate Security Architecture requirements. For more information, see https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html

	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.
		Fusion SaaS Cloud Applications Security Standards (including the SaaS password security standard, that addresses complexity and protection requirements) are reviewed annually and updated as needed.
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	System identity information and levels of access is managed, stored, and reviewed. Logical access controls for applications and systems must provide identification, authentication, authorization, accountability, and auditing functionality. Oracle regularly reviews network and operating system accounts regarding the appropriate employee access levels. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		The SaaS Logical Access Control standard, for applications and systems, such as Fusion SaaS Application Services, must provide identification, authentication, authorization, accountability, and auditing functionality.
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Separation of duties principle is employed when implementing information system access. The Oracle Logical Access Controls Policy and standard describes logical access control requirements for Oracle systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined 'users' with access to Oracle systems, which are not Internet facing publicly accessible systems. Oracle SaaS security has developed its own standard that further extends/refines the one coming from Oracle corporate security, for the SaaS LoB. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest?
		Fusion SaaS Cloud Applications enforce well-defined roles, allowing for segregation of duties among operations staff 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. Examples of functional groups include database administrators, system administrators, and network engineers. Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval.
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest? • Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose? For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		Fusion SaaS Cloud Applications customers are responsible for ensuring least privilege in their use of Oracle Fusion SaaS Cloud Applications.

IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	A user access provisioning process is defined and implemented. Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		Customers are responsible for the user access provisioning in their use of Oracle Fusion SaaS Cloud Applications.
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access. For more information, see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
		Customers are responsible for de-provisioning users in their use of Oracle Fusion SaaS Cloud Applications.
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Customers are responsible for review and revalidation of user access levels within their use of Oracle Fusion SaaS Cloud Applications. Oracle reviews and revalidates Oracle administrative user access for least privilege and separation of duties on a quarterly cadence. Fusion SaaS Cloud Applications service employee access management covers on-boarding, internal/external transitions, and terminations. All terminations are processed automatically through the Oracle Human Resources Management System (HRMS). After a termination is processed, automated notifications are issued for terminations (regardless of type) based on the effective date of the termination.
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access,	Oracle Fusion SaaS Cloud Applications adhere to the documented Oracle Network Security Standard that defines requirements and processes that include segregation of privileged access.

	encryption, key management capabilities, and logging capabilities are distinct and separate?	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Oracle access processes are defined and implemented. Privileged Access roles and rights have processes to ensure they are reviewed on a quarterly basis. Privileged Account passwords expire on a shortened cycle. For more information see: For more information see https://www.oracle.com/corporate/security-practices/corporate/access-control.html
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. This policy does not apply to publicly accessible, internet-facing Oracle systems or end users. Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. All network administration accounts, deployed in an Oracle managed network, must be provisioned and managed by a corporate sanctioned access governance system.
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	Fusion SaaS Cloud Application Customers can control Oracle personnel access to their environments by subscribing to Break Glass (where applicable.) • **Access Approval** – Stringent Access control restricted by Internal & Customer approvals (Justification, SR, Geo-location) • **Time Bound** – Access revoked & passwords rotated after customer defined time windows • **Reporting** – Audit reports for access history
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access	Logging processes are in place and are reviewed by external third-party auditors for our continued compliance with other Compliance frameworks (i.e., SOC1, SOC2, PCI-DSS and ISO27001.) Logs are immutable where technically possible otherwise compensating controls are in place to ensure a secure logging infrastructure.

	(including privileged access roles) defined, implemented, and evaluated?	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	See IAM-12.1
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Customers are primarily responsible for the management of identity and access to their data in their use of Oracle cloud services. For Oracle, processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) are defined, implemented, and evaluated. Each user is assigned a unique identifier/account through OIM.
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined,	Processes, procedures, and technical measures are in place for authenticating access to systems, applications and data assets including multifactor authentication for a least-privileged user and sensitive data access. The Oracle Logical Access Control Policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest? • Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?

	implemented, and evaluated?	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Oracle uses external and internal certificate authorities for certification generation. For 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 for the secure management of passwords defined, implemented, and evaluated?	Processes, procedures, and technical measures are in place for the secure management of passwords. Please refer to: https://www.oracle.com/corporate/security-practices/corporate/access-control.html
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Processes, procedures, and technical measures are in place to verify access to data and systems resources. Oracle's Access Control security practices define these measures. For example, for administration of network security and network-management devices, Oracle requires IT personnel to use secure protocols with authentication, authorization, and strong encryption. Network devices must be in an environment protected with physical access controls and other physical security measure standards defined by Global Physical Security (GPS). Communications to and from the Oracle corporate network must pass through network security devices at the border of Oracle's internal corporate network. Remote connections to the Oracle corporate network must exclusively use virtual private networks (VPN) that have been approved via the Corporate Security Solution Assurance Process (CSSAP). Access to the Oracle corporate network by suppliers and third parties is subject to limitations and prior approval per Oracle's Third-Party Network Access Policy. See: https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html

Control Domain: Interoperability & Portability

Question ID	Consensus Assessment Question	Oracle Response
IPY-01.1	Are policies and procedures established, documented, approved, communicated,	Oracle Fusion SaaS Cloud Applications have policies and procedures in place for communications between application services.

	applied, evaluated, and maintained for communications between application services (e.g., APIs)?	
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Oracle Fusion SaaS Cloud Applications have policies and procedures in place for information processing interoperability. Customers are provided network protocol information necessary to use the services. For more information please see: https://docs.oracle.com/en/cloud/saas/financials/23b/farfa/index.html https://docs.oracle.com/en/cloud/saas/human-resources/23b/farws/index.html https://docs.oracle.com/en/cloud/saas/sales/faaps/index.html
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Oracle Fusion SaaS Cloud Applications have policies and procedures established and maintained to support application development portability. Please also see Section 6, Oracle Hosting and Delivery Policy: https://www.oracle.com/mx/a/ocom/docs/corporate/cloud-hosting-delivery-policies-soc.pdf
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability,	Oracle Fusion SaaS Cloud Applications have policies and procedures are established, documented, approved communicated and applied for information/data exchange, usages, portability, integrity, and persistence. Please see: https://www.oracle.com/mx/a/ocom/docs/corporate/cloud-hosting-delivery-policies-soc.pdf

	integrity, and persistence?	
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Oracle Fusion SaaS Cloud Applications polices (including interoperability and portability policies) are reviewed annually and updated as needed.
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Oracle Fusion SaaS Cloud Applications policy and procedures are in place and where applicable CSC's can programmatically retrieve their data via an application interface. Please see: https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf https://docs.oracle.com/en/cloud/saas/financials/23b/farfa/index.html https://docs.oracle.com/en/cloud/saas/human-resources/23b/farws/index.html https://docs.oracle.com/en/cloud/saas/sales/faaps/index.html
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Cryptographically secure and standardized network protocols are implemented for the management, import, and export of data. Oracle's Cryptography Review Board defines and promotes cryptography-related technical standards for Oracle products and services. The group is primarily responsible for making technical decisions and authoring internal standards to address government and industry requirements. Representatives from Corporate Security and development organizations define best practices related to using and implementing cryptography in Oracle software products and cloud services, derived from frequent reviews of existing industry practices and current threat intelligence. CRB's responsibilities include: • Creating and maintaining standards for cryptography algorithms, protocols, and their parameters • Providing approved standards in multiple formats, for readability and automation • Defining approved cryptography providers as well as recommended and approved key management solutions for use by Oracle • Providing practical guidance on using cryptography • Performing forward-looking research and developing technology prototypes on topics such as post quantum cryptography Communications to and from the Oracle corporate network must pass through network-security devices at the network boundary. Access to the Oracle corporate network by third parties is subject to prior approval. Remote connections to the Oracle corporate network must exclusively use approved virtual private network (VPN) solutions. To learn more about Oracle's network management practices, please see Network Communications Security. For more information, please see: https://www.oracle.com/corporate/security- practices/corporate/governance/global-product-security.html
IPY-04.1	Do agreements include provisions specifying CSC data access upon	Oracles Cloud Hosting and Delivery policies include provisions for CSC data access upon contract termination. For a period of 60 days upon termination of the Oracle Cloud Services, Oracle will make available, via secure protocols and in a structured, machine-readable format,

	contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Customer Content residing in the production Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by Customer. Any terms and conditions related to Oracle's performance of the applicable services shall be specified in the customer order for services documentation. Please refer to https://www.oracle.com/mx/a/ocom/docs/corporate/cloud-hosting-delivery-policies-soc.pdf

Control Domain: Infrastructure & Virtualization Services

Question ID	Consensus Assessment Question	Oracle Response
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Infrastructure and virtualization security policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained. See https://www.oracle.com/corporate/security-practices/corporate/
		Oracle Fusion SaaS Cloud Applications adhere to the infrastructure and virtualization security policies.
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Oracle policies (including policies applicable to infrastructure and virtualization security policies) are reviewed annually and updated as needed.
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers	Oracle Fusion SaaS Cloud Services collects and monitors capacity and utilization data. This data is used to plan for adequate capacity to meet current, projected, and anticipated needs and customer service level agreements.

	required system performance, as determined by the business?	
IVS-03.1	Are communications between environments monitored?	Fusion SaaS Cloud Applications communication between environments is monitored. Specifically, our intrusion-detection systems within the Oracle Cloud Infrastructure to provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle utilizes a network-based monitoring approach to detect attacks on open firewall ports within Oracle's Cloud Infrastructure. Events are analyzed using signature detection, which involves pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to Oracle's security personnel for review and response to potential threats. For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html.
IVS-03.2	Are communications between environments encrypted?	Oracle has corporate policies and standards that define the approved cryptographic algorithms and protocols. Connections to the customer administration console, currently APIs or host region must be made over an encrypted protocol using HTTPS and TLS 1.2 or above. Encryption is employed to protect data and virtual machine images during transport across public networks. To enable deep packet inspection by Oracle Cloud Intrusion Detection systems (IDS), inbound network traffic is decrypted at the load balancer.
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Communications to and from the Oracle corporate network must pass through network-security devices at the network boundary. Access to the Oracle corporate network by third parties is subject to prior approval. Remote connections to the Oracle corporate network must exclusively use approved virtual private network (VPN) solutions. To learn more about Oracle's network management practices, please see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html As defined the Oracle Network Security Policy, Fusion SaaS Cloud Applications restrict communication between environments to only authenticated and authorized connections.
IVS-03.4	Are network configurations reviewed at least annually?	Fusion SaaS Cloud Applications network configurations are reviewed at least annually and updated as needed.
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Oracle follows a defined process Corporate Security Solution Assurance Process (CSSAP) developed by Corporate Security Architecture Global Information Security, Oracle Global Product Security, Oracle Global IT, and Oracles IT organization. This process ensures justification and approval of the new configuration has occurred. For more information see: https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html

IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Oracle employs standardized system hardening practices across Oracle Fusion SaaS Cloud Applications devices. This includes restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, and logging.
IVS-05.1	Are production and non-production environments separated?	Fusion SaaS Cloud Applications production and non-production environments are logically and physically segregated. Additionally, procedures are in place to ensure production data is not used in non-production environments.
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	To mitigate security risks associated with Cloud customer data comingling inherent in multi-tenant clouds, Fusion SaaS Cloud Applications 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.
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or	Your access to Oracle Fusion SaaS Cloud Applications is through a secure communication protocol provided by Oracle. Staging networks are segregated from production-level networks and utilized when migrating production data to virtual servers. Physical servers, applications, and virtual machines are not moved. New environments are provisioned using a hardened master image with customer data migrated once the provisioning process is complete. Communication 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.

	data to cloud environments?	
IVS-08.1	Are high-risk environments identified and documented?	Oracle's Information Systems Asset Inventory Policy requires that Line of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware, and software. This policy applies to all information assets held on any Oracle system, including both enterprise systems and cloud services. In addition, Oracles Information Protection Policy requires all assets be classified based on their risk level.
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Processes, procedures, and defense-in-depth techniques are defined and implemented. Fusion SaaS Cloud Applications defense-in-depth security framework helps protect and detect network-based attacks. Specifically, our intrusion-detection systems within the Oracle Cloud Infrastructure to provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle utilizes a network-based monitoring approach to detect attacks on open firewall ports within Oracle's Cloud Infrastructure. Events are analyzed using signature detection, which involves pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to Oracle's security personnel for review and response to potential threats. For more information, see https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html.

Control Domain: Logging & Monitoring

Question ID	Consensus Assessment Question	Oracle Response
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Logging and monitoring policies are established, documented, approved, communicated, applied, evaluated, and maintained by Oracle Corporate Security. Oracle centrally logs certain security-related activities, such as events and activities from operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html
		Fusion SaaS Cloud Applications Security has procedures and standards in place to support Oracle Logging and Monitoring polices.
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address logging and monitoring) are reviewed annually and updated as needed.
		Fusion SaaS Cloud Applications Security standards and procedures are reviewed 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?	Processes, procedures, and technical measures are in place to ensure audit log security and retention. Oracle centrally logs certain security-related activities, such as events and activities from operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Log files are protected by strong cryptography, multi-factor authentication, and secure architectures. Oracle adheres to least privilege practices, and access to audit logs is monitored. The information management and records retention policy outline the required retention of audit logs, security events, and any protentional investigative reports. The retention of these records also adheres to any applicable government and compliance programs. Fusion SaaS Cloud Applications has a defined SaaS Cloud Logging and Log Analysis Standard. This standard supports the Oracle Logging and Log Analysis Policy. The following are defined in the standard: 1) Information included in the log collection record 2) Events to be logged 3) Log Storage 4) Retention period and classification 5) Frequency of Analysis of Logs
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	All Security related events (system events, firewall logs, network flows, etc.) from Fusion SaaS Cloud Applications and it's underlaying infrastructure are logged into a Security Information and Event Management (SIEM) solution to correlate information and alert on any potential security event. Oracle security personnel monitors these events 24x7x365 and have defined processes to enable the incident response process.
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	A system is defined and implemented to generate alerts and notify responsible stakeholders. Oracle Cloud Infrastructure has deployed a security information and event monitoring (SIEM) solution in each region which ingests and stores security-related logs and alerts from networking devices, hosts, and other components within the infrastructure. Access to logs is controlled in a permissions system and is restricted to authorized personnel. Oracle Cloud Infrastructure's Detection and Response team (DART) monitors the SIEM for event correlations and other relevant detection scenarios on a 24x7 basis to defend and protect against unauthorized intrusions and activity in the production environment.
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Fusion SaaS Cloud Applications 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 security personnel have engineered SIEM detections to monitor for anomalous activities. Oracle has dedicated detection and response teams that focus on designing and implementing solutions to help identify Tactics, Techniques, and Procedures (TTPs) of threat actors.
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Fusion SaaS Cloud Applications Detection and Response Team (DART) has defined procedures and processes to ensure appropriate and timely actions are taken on detected anomalies.
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Network Time Protocol (NTP) is used for common time reference across the Oracle SaaS architecture.
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Fusion SaaS Cloud Applications adhere to 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?	Fusion SaaS Cloud Application logging requirements and threat landscape are continually reviewed, and logging requirement updates 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?	Fusion audit and access logs are generated and capture security-relevant information on application, databases, WAF, and network devices, to name a few.

LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Fusion SaaS Cloud Applications access logs are preserved in its unmodified original format, as generated by the system, for evidentiary purposes. Access to logs for review and analysis purposes are restricted to authorized personnel on a "need-to-know" basis in accordance with the Logical Access Controls Policy and associated Standard. Access mechanisms must be configured to not allow malicious and unintentional alteration of the logs. Users, including those with privileged access rights, should not have permission to delete or deactivate logs of their own activities. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Please see LOG-02.1
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Oracle monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. There are logs generated and mechanisms in place to review/respond to activity.
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Oracle monitors operational activities as they relate to key lifecycle and other cryptographic operational efforts. 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?	For data centers hosting Fusion SaaS Cloud Applications, Oracle leverages an integrated security management system with electronic photo ID badges, cardholder access control, biometrics, recorded digital video surveillance, and alarm monitoring. Main entrances are staffed 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management. Intrusion detection alarm systems and a 24x7 security protection unit secure the building perimeter. Fusion SaaS Cloud Applications access is restricted, and physical access logs are retained. Colocation building access logs for the building may be managed and retained by the collocation datacentre provider. The standard retention policy for logs is 90 days.
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and	Processes and measures for reporting and monitoring system anomalies and failures are in place. Fusion SaaS Cloud Applications Detection and Response Team has defined processes and technical measures to detect anomalies and failures, those processes are reviewed on a continual basis.

	failures defined, implemented, and evaluated?	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Accountable parties are immediately notified about anomalies and failures, Fusion 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 any potential security event. Oracle security personnel monitor the SIEM 24x7x365 and have defined processes to escalate events as needed. This process includes reporting and notification requirements to system owners and Oracle leadership.

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

Question ID	Consensus Assessment Question	Oracle Response
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Policies and procedures for security incident management, e-discovery, and cloud forensics are established, documented, approved, communicated, applied, evaluated, and maintained with the oversight of Oracle Global Information Security. Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed customer data has been unproperly handled or accessed. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). 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. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems within the Lines of Business (LoBs) are utilized to collect information and maintain a chain of custody for evidence during incident investigation. Oracle can support legally admissible forensic data collection when necessary. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
SEF-01.2	Are policies and procedures reviewed and updated annually?	Oracle Corporate Security policies and procedures (including security incident management, e-discovery, and forensics) are reviewed annually and updated as needed. Fusion SaaS Cloud Applications standards and procedures (including security incident management, e-discovery, and forensics) are reviewed annually and updated as needed.
SEF-02.1	Are policies and procedures for timely management of security incidents established,	See SEF-01.1

	documented, approved, communicated, applied, evaluated, and maintained?	
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Oracle Corporate Security policies and procedures (including timely management of security incidents) are reviewed annually and updated as needed.
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). Corporate requirements for LoB incident-response programs and operational teams are defined per incident type: • Validating that an incident has occurred • Communicating with relevant parties and notifications • Preserving evidence • Documenting an incident itself and related response activities • Containing an incident • Addressing the root cause of an incident • Escalating an incident For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	The Oracle's Lines of Business (LoBs) security incident response plans are tested and updated as needed. For more information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
SEF-05.1	Are information security incident	Information security incident metrics are established and monitored with the oversight of the Oracle Global Information Security.

	metrics established and monitored?	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	See SEF-01.1
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Processes, procedures, and technical measures for security breach notification are 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. For more information, see: https://www.oracle.com/be/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	See SEF 01.1 Oracle complies with applicable SLAs, law, and regulation. 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 regulatory authorities, national and local law enforcement, and other legal jurisdictional authorities.

Control Domain: Supply Chain Management, Transparency & Accountability

Question ID	Consensus Assessment Question	Oracle Response
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Policies and procedures are implemented regarding the shared security responsibility model (SSRM). Managing security and privacy in the cloud is often a shared responsibility between the cloud customer and the cloud service provider. The distribution of responsibilities between the cloud service provider and customer also varies based on the nature of the cloud service (IaaS, PaaS, SaaS). Before deploying Oracle cloud service, Oracle strongly recommends that cloud customers formally analyze their cloud strategy to determine the suitability of using the applicable Oracle cloud services considering their own legal and regulatory compliance obligations. Making this determination remains solely the responsibility of customers. For information on the Oracle Cloud Compliance Shared Management Model, see https://www.oracle.com/cloud/compliance/ Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers. Oracle suppliers are required to protect the data and assets Oracle entrusts to them. These Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when accessing Oracle or Oracle customer facilities, networks and/or information systems, handling Oracle confidential information, or controlling custody of Oracle hardware assets. Suppliers 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/
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Oracle Corporate Security policies (including policies applicable to shared security responsibility model) are reviewed annually and updated as needed. For more information, see https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	The Security Shared Responsibility Model (SSRM) is applied, documented, implemented, and managed through the supply chain for the Fusion SaaS Cloud Applications. For more information see: https://www.oracle.com/corporate/suppliers.html

STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Oracle's Supply Chain Risk Management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services. Quality and reliability for Oracle's hardware systems are addressed through a variety of practices, including design, development, manufacturing and materials management processes. Inspection and testing processes Requiring that hardware supply chain suppliers have quality control processes and measurement systems. Requiring that hardware supply chain suppliers comply with applicable Oracle requirements and specification. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	The Oracle Cloud Hosting and Delivery Policies describe the customer (tenant) security obligations. Also, the Oracle Data Processing Agreement includes the responsibilities of the data controller (tenant/customer) versus data processor (Oracle). Please see the Oracle Hosting and Delivery Policies located at https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html and the Oracle Data Processing Agreement at and https://www.oracle.com/contracts/cloud-services/
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Fusion SaaS Cloud Applications reviews and validates SSRM Documentation annually. Please see https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	All portions of the SSRM the organization is responsible for is implemented, operated, audited, and assessed. Oracle's security policies cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27001:2013 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27002:2022 standards. Corporate Security Architecture manages a cross-organization working group focused on security architecture, with the goal of collaboratively guiding security for Oracle cloud services. Participation includes members from Oracle cloud service development, operations, and governance teams.
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	An inventory of all supply chain relationships is developed and maintained. Oracle maintains master service agreements with vendors for services and products. These agreements define agreed upon security, privacy, and compliance controls prior to the onset of services. These controls meet requirements of Oracle policy. Oracle Cloud Services currently maintains contracts with third-party vendors for co-location facilities (for certain services), transportation and storage of encrypted customer backup tapes to off-site storage facilities (for certain services) and various data center functions such as physical security guards, systems maintenance and facility building operations/ maintenance. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
STA-08.1	Are risk factors associated with all organizations within the supply	Oracle's Supply Chain Risk Management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services. Supply availability, continuity and resiliency in Oracle's hardware supply chain are addressed through a variety of practices, including:

	chain periodically reviewed by CSPs?	• Multi-supplier and/or multi-location sourcing strategies where possible and reasonable • Review of supplier financial and business conditions • Requiring suppliers to meet minimum purchase periods and provide end-of-life (EOL)/end-of-support-life (EOSL) notice • Requesting advance notification of product changes from suppliers so that Oracle can assess and address any potential impact • Managing inventory availability due to changes in market conditions and due to natural disasters For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination	Service agreements between CSPs and CSCs incorporate these provisions and/or terms, see the following Oracle documents: Hosting and Delivery Policy, Services Pillar Document, Data Processing Agreement https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html https://www.oracle.com/be/corporate/contracts/cloud-services/contracts.html https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf

	• Interoperability and portability requirements • Data privacy	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Oracle's Supplier Security Management Policy requires all lines of business which utilize third party providers to maintain a program which manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each supplier's goods or services are leveraged.
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Fusion SaaS Cloud Applications have processes for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities. Oracle's Supplier Security Management Policy requires all lines of business which utilize third party providers to maintain a program which manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each supplier's goods or services are leveraged.
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Oracle suppliers are required to protect the 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 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-partners.html
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Oracle's Supplier Security Management Policy requires all lines of business which utilize third party providers to maintain a program which manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each supplier's goods or services are leveraged. For more information, see: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/

STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	See STA-13.1

Control Domain: Threat & Vulnerability Management

Question ID	Consensus Assessment Question	Oracle Response
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	The Oracle Patching and Security Alerts Implementation Policy requires the deployment of the Oracle Critical Patch Update and Security Alert updates as well as associated recommendations. This policy also includes requirements for remediating vulnerabilities in non-Oracle technology using a risk-based approach. For more information, see https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html and https://www.oracle.com/corporate/security-practices/assurance/vulnerability/
		Fusion SaaS Cloud Applications has formal practices designed to identify, analyze, and remediate security vulnerabilities that may affect Fusion SaaS Cloud Applications. The Oracle security and development teams monitor relevant vendor and industry bulletins, including Oracle's security advisories, to identify and assess relevant security patches. Additionally, various security testing activities are performed by the Fusion SaaS Cloud Application teams throughout the development cycle to identify potential issues. 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). Oracle's strategic priority for handling vulnerabilities is to remediate these issues according to their severity and the risk they pose in the context of the use of Fusion SaaS Cloud Applications. The Common Vulnerability Scoring System (CVSS) Base Score is one of the criteria used in assessing the relative severity of vulnerabilities. All vulnerabilities identified are tracked in a defect tracking system. Security fixes are thoroughly tested to avoid issues in production. Prior to each major version of Fusion SaaS Cloud Applications, Oracle security teams perform internal security reviews, architectural security standards reviews and penetration tests. Formal security criteria are defined before releasing a new product or major version into production. Vulnerability scanning using automated scanning systems is performed both internally for all SaaS infrastructure and application assets and externally for Internet facing assets for Fusion SaaS Cloud Applications. Penetration testing in production environment is performed periodically by an external penetration testing company and summary reports are available upon request for existing customers of Fusion SaaS Cloud Applications. Oracle Fusion SaaS Cloud Applications aims to complete all remediation actions, including testing, customer notification, implementation, and reboot/reprovision (if required) within planned maintenance windows. However, if emergency maintenance is required, the process in Section 4 of the Oracle Cloud Hosting and Delivery Policies is utilized.

		Please see: https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address vulnerability management) are reviewed annually and updated as needed. Fusion SaaS Cloud Applications policies and procedures (including policies and procedures that address vulnerability management) are reviewed annually and updated as needed.
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that receive, store, access, transmit or otherwise handle Oracle or customer information must be encrypted using approved software. Reports are provided to lines of business management to verify deployment of device encryption for their organization. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html Fusion SaaS Cloud Applications has policies and practices in place to protect against malware on managed assets. 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. All uploaded files are scanned using Internet Content Adaptation Protocol (ICAP) before being stored in the cloud service. 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
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Oracle Corporate Security policies (including polices that address asset management and malware protection) are reviewed annually and updated as needed. Fusion SaaS Cloud Applications Security Standards (including standards that address asst 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	Processes, procedures, and technical measures are defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk.) Please see: https://www.oracle.com/security-alerts/ Also, see section: Order of Fixing Security Vulnerabilities https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html

	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 compromise indicators weekly (or more frequent) basis?	Processes, procedures, and technical measures are defined, implemented, and evaluated to update detection tools, threat signature and compromise indicators on at least a weekly basis. Antivirus updates generally occur daily. Please see TVM-01.1 Fusion SaaS Cloud Applications processes, procedures, and technical measures have been defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators on at least a weekly basis. Antivirus updates generally occur daily.
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Processes, procedures, and technical measures are defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to Oracles Vulnerability management policy.) Please see TVM-01.1 Fusion SaaS Cloud Applications adhere to the OSSA standard specific to Supply Chain Security in addition the security and development teams monitor relevant vendor and industry bulletins, including Oracle's security advisories, to identify and assess relevant security patches. Additionally, various security testing activities are performed by the Fusion SaaS Cloud Application teams throughout the development cycle to identify potential issues. 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, implemented, and evaluated for periodic, independent, third-party penetration testing?	Processes, procedures, and technical measures are in place for independent third-party penetration testing. Oracle regularly performs 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 / Penetration Tests are performed by a third-party on Fusion SaaS Cloud Applications at least annually. Third party summary results are available to customers upon request. Processes, procedures, and technical measures are in place for third-party Fusion SaaS Cloud Applications penetration testing. These tests are conducted at least annually. Third-party testing summary results are available to customers upon request.
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Processes procedures, and technical measures are in place for vulnerability detection on organizationally managed assets at least monthly. Oracle policy requires the use of antivirus, intrusion protection, and firewall solutions on endpoint devices such as laptops, desktops, and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. All uploaded files are scanned using Internet Content Adaptation Protocol (ICAP) before being stored in the cloud service. 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. Fusion Cloud Applications utilize either host-based or Network-based Intrusion Detection Systems (IDS) to protect the environment. IDS sensors are deployed in Intrusion Detection mode to monitor suspicious network traffic. IDS alerts are routed to a centralized monitoring system that is managed by the security operations teams 24x7x365.
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Oracle uses the Common Vulnerability Scoring System (CVSS) Base Score to report the relative severity of security vulnerabilities when it discloses them. CVSS information is provided in risk matrices published in the security advisories as individual metrics which cover the technical aspects of the vulnerabilities, such as the preconditions required for successful exploitation. Additionally, Common Vulnerabilities and Exposures (CVE) identifiers can be used by Oracle to identify the vulnerabilities listed in the risk matrices. CVE numbers are unique, common identifiers for publicly known information about security vulnerabilities. The CVE program is co-sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security and is managed by MITRE corporation. Oracle is a CVE Numbering Authority (CNA), that is the company can issue CVE numbers for vulnerabilities in its products. For more information, see https://www.oracle.com/corporate/security-practices/assurance/vulnerability/
		Fusion SaaS Cloud Applications use 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 in the Critical Patch Update, resulting in optimizing the security posture of all Oracle customers. See: https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html

TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	See TVM-01.1 Fusion SaaS Cloud Applications has defined processes and standards (The Oracle Fusion SaaS Cloud Applications Vulnerability Management Security Standard) to track and report on vulnerabilities to remediation.
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	See TVM-01.1 Fusion SaaS Cloud Applications Security has defined metrics to monitor vulnerabilities as they are identified through to remediation. Processes include (Security Health Review and Vulnerability Management Advocacy Program) monitoring all vulnerabilities and remediation steps monthly.

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?	Policies and procedures are in place for the management and security of all endpoints. Oracle policies set the requirements for 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 for their organization. Oracle employees are required to comply with email instructions from Oracle Information Technology (OIT) and are responsible for promptly reporting to the Oracle employee helpdesk any virus or suspected virus infection that cannot be resolved by antivirus software. Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
UEM-01.2	Are universal endpoint management policies and procedures reviewed and	Oracle Corporate Security policies (including polices that address universal endpoint management) are reviewed annually and updated as needed.
		Fusion SaaS Cloud Applications standards (including standards that address universal endpoint management) are reviewed annually and updated as needed

	updated at least annually?	
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?	See UEM-01.1. This list is approved by Oracle Corporate Architecture and maintained by Oracle Information Technology.
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	See UEM-01.1. Endpoint validation is performed by automation approved by Oracle Corporate Architecture and maintained by Oracle information Technology. Fusion SaaS Cloud Applications have processes implemented to validate endpoint device compatibility with operating systems and applications.
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Oracle's Information Systems Asset Inventory Policy requires that Line of Business (LoB) maintain accurate and comprehensive inventories of information systems, hardware, and software. Oracle policy specifies the data (or fields) which must be maintained about these information systems in the approved system inventory. For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html
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	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. To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full disk encryption software on company owned or personal laptops and desktops, except were approved for justifiable business purposes. Data on the disk can only be accessed with 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

	and/or store, transmit, or process organizational data?	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Interactive-used endpoints are configured to require an automatic lock screen. Oracle computers have secure desktop management software installed that lock screens automatically after a defined period of inactivity. This includes computers used to manage Oracle SaaS Cloud Services. Fusion 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?	Oracle Cloud Operations performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software to maintain operational stability, availability, security, performance, and currency of the Oracle Cloud. Oracle follows formal change management procedures to provide review, testing, and approval of changes prior to application deployment in the Oracle Cloud production environment. Changes made through change management procedures include system and service maintenance activities, management of application upgrades and updates, and coordination of customer specific changes where required. Oracle works to architect Cloud Services to minimize service interruption during implementation of changes. Fusion SaaS Cloud Applications follow formal change management procedures to provide review, testing, and approval of changes prior to application is deployed in the Oracle Cloud production environment. Changes made through change management procedures include system and service maintenance activities, management of application upgrades and updates, and coordination of customer specific changes where required. Oracle works to architect cloud services to minimize service interruption during implementation of changes.
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	See UEM-05.1
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Antivirus detection and prevention technology and Windows Server Update Services (WSUS) are managed to ensure they are up to date with virus definitions and security updates. Antivirus software must be scheduled to perform daily threat definition updates and virus scans. For more information, please see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html

UEM-10.1	Are software firewalls configured on managed endpoints?	Oracle policy requires the use of antivirus, intrusion protection and firewall software on laptops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. While desktops and laptops do not process customer data, they are encrypted using approved software. Reports enable lines of business management to verify deployment of laptop encryption for their organization. For more information, see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
		Internal and external software firewalls are configured on managed devices supporting Fusion SaaS Cloud Applications. The Oracle Cloud Infrastructure Web Application Firewall (Oracle WAF) is a cloud-based, global security service that protects applications from malicious and unwanted internet traffic. The WAF which is fully integrated with the Oracle Cloud Infrastructure management console—can protect any internet-facing web application and provides consistent rule enforcement across an organization's web applications.
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Fusion SaaS Cloud Applications does not have a commercial DLP deployed.
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Unless required by regional or governmental regulations, geolocation capabilities are not in place for mobile endpoints.
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Processes, procedures, and technical measures are defined and implemented to enable remote company data deletion on managed endpoint devices. Oracle's secure desktop, and mobile device management software has remote wipe capabilities. For more information please see: https://www.oracle.com/secure-global-desktop/#rc30p2 https://docs.oracle.com/en/virtualization/secure-global-desktop/index.html
UEM-14.1	Are processes, procedures, technical and/or contractual measures defined, implemented, and	Process, procedures, technical and/or contractual measures are in place 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

	evaluated to maintain proper security of third-party endpoints with access to organizational assets?	• Handling Oracle confidential information, and Oracle hardware assets placed in their custody 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/ Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.

CONNECT WITH US

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

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle