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

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