ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Fusion Cloud Applications

December, 2020 | Version 1.01

PURPOSE STATEMENT

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

The answers contained in this CAIQ version 3.1 are related to specific Oracle cloud services as listed in the "Oracle Cloud Services in Scope" section below.

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

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

DISCLAIMER

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

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

ORACLE CLOUD SERVICES IN SCOPE

This document applies to the following Oracle Fusion Cloud Applications delivered as a SaaS service deployed at Oracle data centers or third-party data centers retained by Oracle, with the exception of Oracle Cloud at Customer Services:

- Enterprise Resource Planning: https://www.oracle.com/erp/ (Excluding Enterprise Performance Management (EPM))
- Human Capital Management: https://www.oracle.com/human-capital-management/
- Supply Chain & 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)

Service and Marketing cloud services are also excluded from the scope of this document.

TABLE OF CONTENTS

CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ)

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Application & Interface Security: Application Security	AIS-01.1	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience. To ensure that Oracle products are developed with consistently high security assurance, and to help developers avoid common coding mistakes, Oracle employs formal secure coding standards. For more information, see https://www.oracle.com/corporate/security-practices/assurance/
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	Security testing of Oracle code includes both functional and non-functional activities for verification of product features and quality. Although these types of tests often target overlapping product features, they have orthogonal goals and are carried out by different teams. Functional and non-functional security tests complement each other to provide security coverage of Oracle products. Static security analysis of source code is the initial line of defense used during the product development cycle. Oracle uses a static code analyzer from Fortify Software, an HP company, as well a variety of internally developed tools, to catch problems while code is being written. Products developed in most modern programming languages (such as C/C++, Java, C#) and platforms (J2EE, .NET) are scanned to identify possible security issues. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	Oracle Developers use static and dynamic analysis tools to detect security defects in Oracle code prior to production. Identified issues are evaluated and addressed in order of priority and severity. Oracle management tracks metrics regarding issue identification and resolution. For more information, see https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Oracle Software Security Assurance (OSSA) policies require that third-party components (e.g., open source components used in the Oracle Clouds or distributed in traditional Oracle product distributions) be appropriately assessed for security purposes. Additionally, Oracle has formal policies and procedures which define requirements for managing the safety of its supply chain, including how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments.

		deployed to all mobile devices that are permitted to store, transmit, or process company data?	common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Encryption	MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	To protect sensitive Oracle information, Oracle personnel are required to install Oracle-approved, full-disk encryption software on their laptops, except where approved for justifiable business purposes. Data on the disk can only be accessed through the use of a private key stored as a password-protected file on the disk. A preboot login manager allows authorized users to login to unlock the key, boot the operating system, and access the data.
Mobile Security: Jailbreaking and Rooting	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. Any Oracle employee who is discovered violating this standard may be subject to disciplinary action up to and including termination of employment.
	MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Legal	MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	Oracle policy requires the use of antivirus intrusion protection and firewall software on laptops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that process Oracle or customer information must be encrypted using approved software. Reports enable lines of business management to verify deployment of laptop encryption for their organization.
	MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?	Oracle places a strong emphasis on personnel security. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.
Mobile Security: Lockout Screen	MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	Oracle's Global Desktop Strategy (GDS) organization keeps anti-virus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. GDS is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. GDS provides automation to verify anti-virus configuration. Oracle employees are required to comply with email instructions from the GDS organization and are responsible for promptly reporting to the Oracle employee helpdesk any virus or suspected virus infection that cannot be resolved by antivirus software.

Mobile Security: Operating Systems	MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Passwords	MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	Oracle enforces strong password policies for the Oracle network, operating system, and database accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. When Oracle compliance organizations determine that a password is not in compliance with strong password standards, they work with the applicable employee and line of business to bring the password into compliance with the standards.
	MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?	The use of passwords is addressed in the Oracle Password Policy. Oracle employees are obligated to follow rules for password length and complexity, and to keep their passwords confidential and secured at all times. Passwords may not be disclosed to unauthorized persons.
	MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	Oracle enforces strong password policies for the Oracle network, operating system, and database accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords.
Mobile Security: Policy	MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	Oracle implements a wide variety of technical security controls designed to protect the confidentiality, integrity, and availability of corporate information assets. These controls are guided by industry standards and are deployed across the corporate infrastructure using a risk-based approach.
	MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
	MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	Oracle policy requires the use of antivirus intrusion protection and firewall software on laptops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that process Oracle or customer information must be encrypted using approved software. Reports enable lines of business management to verify deployment of laptop encryption for their organization.

Mobile Security: Remote Wipe	MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
	MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Security Patches	MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
	MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Mobile Security: Users	MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
	MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	Access control refers to the policies, procedures, and tools that govern access to and use of resources. Examples of resources include a physical server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol. Least privilege is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.
Additional Comments for Control Domain above:			

Security Incident Management, E-Discovery, & Cloud Forensics: Contact / Authority Maintenance	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Oracle evaluates and responds to events that create suspicion of unauthorized access to or handling of customer data, whether the data is held on Oracle hardware assets or on the personal hardware assets of Oracle employees and contingent workers. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to incidents. This policy authorizes Oracle Global Information Security (GIS) organization to serve as the primary contact for security incident response, as well as to provide overall direction for incident prevention, identification, investigation, and resolution.
Security Incident Management, E-Discovery, & Cloud Forensics: Incident Management	SEF-02.1	Do you have a documented security incident response plan?	Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and central systems are utilized globally to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	In the event that Oracle determines that a security incident has occurred, Oracle promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared.
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	The Oracle Data Processing Agreement describes Oracle's obligations in the event of a personal information breach. Individual tenant service agreements may describe additional responsibilities during a security incident. https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
	SEF-02.4	Have you tested your security incident response plans in the last year?	Oracle Global Information Security (GIS) organization serves as the primary contact for security incident response, as well as to provide overall direction for incident prevention, identification, investigation, and resolution. GIS defines roles and responsibilities for the incident response teams embedded within the Lines of Business (LoBs). All LoBs must comply with GIS incident response guidance about detecting events and timely corrective actions. Corporate requirements for LoB incident-response programs and operational teams are defined per incident type: • Validating that an incident has occurred • Communicating with relevant parties and notifications • Preserving evidence • Documenting an incident itself and related response activities • Containing an incident • Eradicating an incident • Escalating an incident

Security Incident Management, E-Discovery, & Cloud Forensics: Incident Reporting	SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	Formal procedures and central systems are utilized globally to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
	SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	In the event that Oracle determines that a security incident has occurred, Oracle promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities.
Security Incident Management, E-Discovery, & Cloud Forensics: Incident Response Legal Preparation	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	Reflecting the recommended practices in prevalent security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets.
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Formal procedures and central systems are utilized globally to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
	SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	Formal procedures and central systems are utilized globally to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Formal procedures and central systems are utilized globally to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
Security Incident Management, E-Discovery, & Cloud Forensics: Incident Response Metrics	SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	Oracle evaluates and responds to events that create suspicion of unauthorized access to or handling of customer data, whether the data is held on Oracle hardware assets or on the personal hardware assets of Oracle employees and contingent workers. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to incidents. This policy authorizes Oracle Global Information Security (GIS) organization to serve as the primary contact for security incident response, as well as to provide overall direction for incident prevention, identification, investigation, and resolution.

	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	Incident history is Oracle Confidential and is not shared externally.
Additional Comments for Control Domain above:			
Supply Chain Management, Transparency, and Accountability: Data Quality and Integrity	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers.
	STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	Access control refers to the policies, procedures, and tools that govern access to and use of resources. Examples of resources include a physical server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol. • Least privilege is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties. • Default-deny is a network-oriented approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination.
Supply Chain Management, Transparency, and Accountability: Incident Reporting	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	In the event that Oracle determines that a security incident has occurred, Oracle promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared. Incident history is also Oracle Confidential and is not shared externally. See Oracle Cloud Hosting and Delivery Policies, Pillar Documents and Service Descriptions for specific details about incident notifications: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
Supply Chain Management, Transparency, and Accountability: Network / Infrastructure Services	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	See Oracle Cloud Hosting and Delivery Policies and Pillar documents: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	STA-03.2	Do you provide tenants with capacity planning and use reports?	Capacity planning information is Oracle Confidential and is not shared externally.
Supply Chain Management, Transparency, and Accountability:	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies,	The Chief Corporate Architect, who reports directly to the Executive Chairman and Chief Technology Officer (CTO), is one of the directors of the Oracle Security Oversight Committee (OSOC). The Chief Corporate Architect manages the functional

Provider Internal Assessments		procedures, and supporting measures and metrics?	departments directly responsible for identifying and implementing security controls at Oracle.
Supply Chain Management, Transparency, and Accountability: Third Party Agreements	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	Oracle also has formal requirements for its suppliers and partners to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle confidential information, and Oracle hardware assets placed in their custody Agreements required for Oracle suppliers are at: https://www.oracle.com/corporate/suppliers.html
	STA-05.2	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	Oracle's Supply Chain Risk Management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services.
	STA-05.3	Does legal counsel review all third-party agreements?	Oracle's Supply Chain Risk Management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services.
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	Oracle suppliers are required to adhere to the Oracle Supplier Code of Ethics and Business Conduct, which includes policies related to the security of confidential information and intellectual property of Oracle and third parties.
	STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Oracle Cloud Hosting and Delivery Policies describe the Oracle Cloud Service Continuity Policy, Oracle Cloud Services High Availability Strategy, Oracle Cloud Services Backup Strategy and Oracle Cloud Service Level Agreement. Service-specific Pillar documents provide additional information about specific cloud services: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	A customer's order specifies the Data Center Region in which the services environment and storage of customer data will reside. Oracle provides production and test environments in the Data Center Region stated in the order. In the event of a disaster, the production service will be restored in the Data Center Region stated in the order. Oracle and its affiliates may perform certain aspects of Fusion Cloud Applications, such as service administration and support, as well as other Services (including Professional Services and disaster recovery), from locations and/or through use of subcontractors, worldwide.

	STA-05.7	Can you provide the physical location/geography of storage of a tenant's data upon request?	Customers can request the city and country for their cloud service instances.
	STA-05.8	Can you provide the physical location/geography of storage of a tenant's data in advance?	Customers should discuss available choices for locations of their cloud service instances with their account representative.
	STA-05.9	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	A customer's order specifies the Data Center Region in which the services environment will reside. Oracle provides production and test environments in the Data Center Region stated in the order. In the event of a disaster, the production service will be restored in the Data Center Region stated in the order. Oracle and its affiliates may perform certain aspects of Cloud Services, such as service administration and support, as well as other Services (including Professional Services and disaster recovery), from locations and/or through use of subcontractors, worldwide.
	STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Oracle Privacy Policies are available at https://www.oracle.com/legal/privacy/ Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and central systems are utilized globally to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
	STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	See Oracle Cloud Hosting and Delivery Policies and Pillar documents: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
	STA-05.12	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	Lists of subprocessors for Oracle Cloud services are available in My Oracle Support (https://support.oracle.com) "Oracle General Data Protection Regulation (GDPR) Resource Center", article ID # 111.2. Agreements with subprocesors are Oracle Confidential.
Supply Chain Management, Transparency, and Accountability: Supply Chain Governance Reviews	STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers. For more information, see https://www.oracle.com/corporate/security-practices/corporate/supply-chain/

			Oracle suppliers and partners are required to protect the data and assets Oracle entrusts to them. These Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when accessing Oracle or Oracle customer facilities, networks and/or information systems, handling Oracle confidential information, or controlling custody of Oracle hardware assets. Suppliers and partners are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards.
Supply Chain Management, Transparency, and Accountability: Supply Chain Metrics	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	Oracle also has formal requirements for its suppliers and partners to confirm they protect the Oracle and third-party data and assets entrusted to them. The Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when: • Accessing Oracle and Oracle customers' facilities, networks and/or information systems • Handling Oracle confidential information, and Oracle hardware assets placed in their custody Oracle suppliers are required to sign the agreements at https://www.oracle.com/corporate/suppliers.html
	STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	Oracle's Supply Chain Risk Management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services. Quality and reliability for Oracle's hardware systems are addressed through a variety of practices, including: • Design, development, manufacturing and materials management processes Inspection and testing processes • Requiring that hardware supply chain suppliers have quality control processes and measurement systems • Requiring that hardware supply chain suppliers comply with applicable Oracle requirements and specifications
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Supply availability and continuity and resiliency in Oracle's hardware supply chain are addressed through a variety of practices, including: • Multi-supplier and/or multi-location sourcing strategies where possible and reasonable • Review of supplier financial and business conditions • Requiring suppliers to meet minimum purchase periods and provide end-of-life (EOL)/end-of-support-life (EOSL) notice • Requesting advance notification of product changes from suppliers so that Oracle can assess and address any potential impact • Managing inventory availability due to changes in market conditions and due to natural disasters

	STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Supplier SLA reporting is Oracle Confidential.
	STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Oracle makes equivalent information available periodically in the form of various third-party audit and testing reports. These include, but are not limited to SOC 1, SOC 2, ISO, and third-party security assessments/penetration tests. Internal audits and assessments are not available to customers.
	STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?	As part of Fusion Cloud Applications, Oracle will provide Customer with access to a customer notifications portal. This portal may provide metrics on system availability for Cloud Services purchased under the ordering document.
	STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?	Fusion Cloud Applications customers are responsible for data management policies and service level conflicts of interest in their environment.
	STA-07.8	Do you review all service level agreements at least annually?	Third-party supplier agreements, policies and processes are reviewed no less than annually as part of the SOC and ISO audit programs.
Supply Chain Management, Transparency, and Accountability: Third Party Assessment	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	Oracle suppliers and partners are required to protect the data and assets Oracle entrusts to them. These Supplier Information and Physical Security Standards detail the security controls that Oracle's suppliers and partners are required to adopt when accessing Oracle or Oracle customer facilities, networks and/or information systems, handling Oracle confidential information, or controlling custody of Oracle hardware assets. Suppliers and partners are responsible for compliance with these standards, including ensuring that all personnel and subcontractors are bound by contractual terms consistent with the requirements of Oracle's standards. These standards cover a wide range of requirements in the following critical areas: • Personnel/human resources security • Business continuity and disaster recovery • Information security organization, policy, and procedures • Compliance and assessments • Security incident management and reporting • IT security standards • Baseline physical and environmental security
	STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	Oracle's Supplier Security Management Policy requires all lines of business which utilize third party providers to maintain a program which manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each particular supplier's goods or services are leveraged.

Supply Chain Management, Transparency, and Accountability: Third Party Audits	STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	Oracle's Supplier Security Management Policy requires all lines of business which utilize third party providers to maintain a program which manages risk for those suppliers. These programs are required to include a variety of assurance and oversight activities such as an annual review, where appropriate per the risk to data confidentiality, availability or integrity introduced by the way each particular supplier's goods or services are leveraged.
	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Audit reports about Oracle Cloud Services are periodically published by Oracle's third-party auditors. Reports may not be available for all services or all audit types or at all times. Customers may request access to available audit reports for a particular Oracle Cloud service via their Oracle account representative. 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.
Additional Comments for Control Domain above:			
Threat and Vulnerability Management: Antivirus / Malicious Software	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	Oracle deploys anti-virus/anti-malware software on systems that are used by Oracle Fusion Cloud Applications. Oracle Fusion Cloud Applications Support and Operations Staff, along with all Oracle employees and contractors who provide Cloud Support, are required to use company approved laptop or desktop computers that have been equipped with additional controls that include antivirus and malware protection, disk encryption, VPN software, asset inventory management software, and logging software to reduce threat vectors and data privacy risks. All bastion hosts are configured to meet the Windows Server Security & Hardening Guide and the Enterprise Linux Security Standard and Hardening Guide (internal to Oracle). Hardening includes but is not limited to: • Updating the OS with the latest approved security patches • Disabling unnecessary services and policies • Installing antivirus software • Editing registry settings • Disabling copy/paste and over 20 other functions to reduce data loss • Setting inactivity timeouts • Restricting the number of Remote Desktop sessions per user to 1

	TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	Security detection systems, including the Network Intrusion Detection Systems (IDS), Anti-malware, and D-DoS system are configured to auto-update at least every 24 hours.
Threat and Vulnerability Management: Vulnerability / Patch Management	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Oracle regularly performs penetration testing and security assessments against Oracle Cloud infrastructure, platforms, and applications in order to validate and improve the overall security of Oracle Cloud Services.
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Application-layer vulnerability scans are performed on a regular cadence that are aligned with industry commonly accepted practices.
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Operating Systems-level vulnerability scans are performed on a regular cadence that are aligned with industry commonly accepted practices
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	Oracle may provide information which summarizes that point-in-time penetration testing and environment vulnerability scans are performed regularly, with a summary of findings. Oracle does not provide the details of identified weaknesses because sharing that information would put all customers using that product or service at risk. Please see the Oracle Cloud Security Testing Policy for information about customer testing of Oracle Cloud services: https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm
	TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	Oracle Fusion Cloud Applications have a robust patch management solution that ensures vulnerabilities are evaluated, and patches are deployed across the environment based upon criticality. Oracle Fusion Cloud Applications vulnerability severity is assessed based upon Common Vulnerability Scoring System (CVSS) scoring, and remediation SLAs timelines are based upon the assigned severity and possible business impact.
	TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	The Oracle Cloud Hosting and Delivery Policies describe the customer (tenant) security obligations. Also, the Oracle Data Processing Agreement includes the responsibilities of the data controller (tenant/customer) versus data processor (Oracle). Please see the Oracle Hosting and Delivery Policies located at http://www.oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf and the Oracle Data Processing Agreement at http://www.oracle.com/us/corporate/contracts/cloud-data-processing-agreement-1965922.pdf

Threat and Vulnerability Management: Mobile Code	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience. Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at: **Fostering security innovations.** Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help enable organizations to implement and manage consistent security policies across the hybrid cloud data center: database security and identity management, and security monitoring and analytics. **Reducing the incidence of security weaknesses in all Oracle products.** Oracle Software Security Assurance key programs include Oracle's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups, and the use of automated analysis and testing tools. **Reducing the impact of security weaknesses in released products on customers.** Oracle has adopted transparent security vulnerability disclosure and remediation policies. The company is committed to treating all customers equally, and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs.
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile device security and good practice.
Additional Comments for Control Domain above:			

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