ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Applications

February, 2021 | 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 Cloud Applications delivered as SaaS services deployed at Oracle data centers or third-party data centers retained by Oracle, with the exception of Oracle Cloud at Customer Services:

Human Capital Management (HCM)

- Taleo Business Edition
- Taleo Enterprise Edition

Supply Chain & Manufacturing

- Logistics
  - Transportation Management
  - Warehouse Management
- Blockchain
- Internet of Things (IOT)

	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 located 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 27001, 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 Oracle 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?	Oracle 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 has deployed antivirus or anti-malware software on the following services: Taleo Enterprise Cloud Transportation Management Warehouse Management Blockchain IOT Commerce Configure-Price-Quote DataFox Service Oracle 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, and asset inventory management 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

	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 weekly.
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 Cloud Applications have a robust patch management solution that ensures vulnerabilities are evaluated, and patches are deployed across the environment based upon criticality. Oracle 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

CAIQ for Oracle Cloud Applications