ORACLE

Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Infrastructure

October 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

The answers provided in this document are for the architecture, boundaries, and components underlying Oracle Cloud Infrastructure. These answers are provided in the same context as the Cloud Security Alliance Security, Trust, Assurance and Risk (CSA STAR) based on criteria to assess the Cloud Control Matrix (CCM) Version 3.1.

The scope is applicable to the following Oracle services:

Archive Storage,
Audit,
Block Volume,
Compute,
Container Engine for Kubernetes,
Database – Bare Metal,
Database – Exadata,
Database – Virtual Machine,
Distributed Denial of Service (DDoS) Protection,
Digital Assistant,
Email Delivery,
Events,
FastConnect,
File Storage,
Functions,
Health Checks,
Identity and Access Management (IAM),
Key Management,
Load Balancing,
Monitoring,
Networking – Virtual Cloud Networks (VCN),
Notifications,
Object Storage,
Registry,
Resource Manager,
Streaming,
Web Application Firewall (WAF)

Located in the following regions, availability domains and points of presence:

Commercial Regions

Australia East: Sydney, Australia,
Australia Southeast: Melbourne, Australia,
Brazil East: Sao Paulo, Brazil,
Canada Southeast: Toronto, Canada,
Germany Central: Frankfurt am Main, Federal Republic of Germany,
India West: Mumbai, India,
Japan Central: Osaka, Japan,
Japan East: Tokyo, Japan,
Netherlands Northwest: Amsterdam, Netherlands,
Saudi Arabia West: Jeddah, Saudi Arabia,
South Korea Central: Seoul, Republic of Korea,
Switzerland North: Zurich, Switzerland,
United Kingdom South: London, United Kingdom,
United States East: Ashburn, Virginia, United States,
United States West: Phoenix, Arizona, United States.

Government regions

United Kingdom Government South: London, United Kingdom,
United States Department of Defense East: Ashburn, Virginia, United States,
United States Department of Defense North: Chicago, Illinois, United States,
United States Department of Defense West: Phoenix, Arizona, United States,
United States Government East: Ashburn, Virginia, United States,
United States Government West: Phoenix, Arizona, United States.

Office facilities and security/network operating centers:

Bangalore, India,
Dublin, Ireland,
Hyderabad, India,
Kaunas, Lithuania,
Nashua, New Hampshire, United States,
Seattle, Washington, United States.

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 comprehensive 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	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

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
Supply Chain Metrics		and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	• 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 described 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?	The OCI Console provides customers with system security data.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?	OCI provides customers with access to a customer notifications portal. This portal will 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?	Tenants 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 OCI 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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	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. Customer may request access to available audit reports for a particular Oracle Cloud service via Sales. 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: STA-3.2 As part of the Oracle Cloud Infrastructure offering, OCI will provide customers with capacity analytics on request. STA-07.4 As part of Cloud Service offering, OCI provides access to a customer notifications portal. The portal will provide metrics on system availability for Cloud Services purchased under the ordering document.			
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/malware software on systems used by OCI services, however customers are responsible for implementing anti-malware solutions in their own environment
	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 NIDS, Anti-malware, and DDoS system are configured to auto-update at least every 24 hours. Customers are responsible for configuring the update settings for their systems.
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?	OCI performs Host, Network and Application scans on a regularly scheduled frequency. Scans are performed no less than monthly, and after significant project launches or major network changes. Customers are responsible for vulnerability scans of their own applications. Additional information on OCI's security testing policy can be found here: https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Operating system-layer vulnerability scans are performed on systems that are operated by OCI. Additional information on vulnerability testing can be found here: https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm
	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?	OCI has a robust patch management solution that ensures vulnerabilities are evaluated, and patches are deployed across the environment based upon criticality. OCI 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 obligation with regard to the applications and workload operating on OCI. OCI does not have access to, or control of customer (tenant) data.
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.

Control Domain	Question ID	Consensus Assessment Question	Oracle Response
			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: n/a			

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

Consensus Assessment Initiative Questionnaire (CAIQ) CAIQ for Oracle Cloud Infrastructure
October 2020