Oracle Contract Checklist for Saudi Arabian Monetary Authority Cyber Security Framework

January 2023

Disclaimer

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their use of Oracle services. Please also note that the relevant contract(s) between you and Oracle determine(s) the scope of services provided and the related legal terms and this document is provided for reference purposes only, and is not part of, and does not otherwise create or amend, any agreement, warranties, representations or other obligations between you and Oracle. Oracle disclaims any terms or statements contained herein that seek to impose legal or operational requirements on Oracle for the delivery of the services. Customers acknowledge that they remain solely responsible for meeting their legal and regulatory requirements.

The information in this document was current as of January 2023.

Overview

Oracle has developed this document as a part of its continuing efforts to help financial services customers in the Kingdom of Saudi Arabia meet their obligations, particularly under Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework relating to the use of Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications (SaaS)[1]. We want to make it easier for you as a financial institution to identify the sections of the Oracle Cloud services contract that may help you address the requirements in the SAMA Cyber Security Framework. In this document, you will find a list of specific requirements in Article 3.4 (Third Party Cyber Security) of the SAMA Cyber Security Framework, along with a reference to the relevant section(s) of the Oracle Cloud services contract and a short explanation to help you conduct your review of the Oracle Cloud services. For further guidance, please read this document in conjunction with Oracle's Compliance Advisory addressing SAMA Cyber Security Framework applicable to financial institutions.

The Oracle Cloud services contract includes the following customer-specific components, all of which are referenced in this document:

- **Oracle Cloud services agreement** – an Oracle Cloud Services Agreement (CSA) or Oracle Master Agreement (OMA) with Schedule C (Cloud)
- **FSA** – The Oracle Financial Services Addendum to the Oracle Cloud Services Agreement CSA or OMA with Schedule C
- **Ordering Document** – Oracle Cloud services order
- **Services Specifications** – Service-specific components, including the **Oracle Cloud Hosting and Delivery Policies** with applicable **Services Pillar Document(s)** and the **Oracle Data Processing Agreement (DPA)**.

Regulation Background

SAMA is the central bank of the Kingdom of Saudi Arabia and the supervisory authority for banks, payment providers, insurance companies, finance companies and credit bureaus operating within the Kingdom. In May 2017, SAMA issued the Cyber Security Framework, designed to enable SAMA-regulated financial institutions to effectively identify, and address risks related to cyber security. The Framework is based on SAMA requirements and international standards, including standards of the Basel Committee on Banking Supervision (the "Basel Framework"). It's stated objectives are to create a common approach for addressing cyber security, to achieve an appropriate maturity level of cyber security controls, and to ensure cyber security risks are properly managed. For more information, see https://www.sama.gov.sa/en-US/RulesInstructions/Pages/Cybersecurity.aspx.

For more information on financial services regulations in other jurisdictions please visit https://www.oracle.com/cloud/compliance/.

[1] Oracle Global Business Units, NetSuite, and Advertising products are not included in the scope of this document.

NO.	REFERENCE	REGULATION REQUIREMENT/DESCRIPTION	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT	ORACLE EXPLANATION
		3.4 Third Party Cyber Security		
Contract and Vendor Management				
1.	3.4.1(1)	The cyber security requirements should be defined, approved, implemented and communicated within the contract and vendor management processes.	• DPA Section 7 • Oracle Cloud Hosting and Delivery Policies Section 1 • Oracle PaaS and IaaS Public Cloud Services Pillar Document Section 1 • Oracle SaaS Public Cloud Services Pillar Document Section 1	The Oracle Cloud services contract addresses the technical and organizational security measures applicable to customer content as follows: • **Section 7 of the DPA** (Security and Confidentiality) • **Section 1 of the Oracle Cloud Hosting and Delivery Policies** (Oracle Cloud Security Policy) • **Section 1 of the Oracle PaaS and IaaS Public Cloud Services Pillar Document** and **Section 1 of the Oracle SaaS Public Cloud Services Pillar Document** • Oracle's Corporate Security Practices: **oracle.com/corporate/security-practices/**
2.	3.4.1(2)	The compliance with contract and vendor management process should be monitored.	• Oracle Cloud Hosting and Delivery Policies Section 3.2.2 • CSA Section 11.1 • OMA Schedule C Section 11.1	**Section 3.2.2 of the Cloud Hosting and Delivery Policies** states that Oracle will provide customers with access to a customer notifications portal for monitoring the availability of services. **Section 11.1 of the CSA** or **Section 11.1 of the OMA Schedule C** (as applicable) confirms that Oracle continuously monitors the services.
3.	3.4.1(3)	The effectiveness of the cyber security controls within the contract and vendor management	• Oracle Cloud Hosting and Delivery Policies	The Oracle Cloud services contract sets out the various notifications that customers are entitled to receive, which will help enable them to monitor

		process should be measured and periodically evaluated.	Sections 1.12, 3.2.2, 4.1, 4.3 and 5.2.1 • FSA Section 6.2.2 • DPA Section 2.8 • DPA Section 9.2 • FSA Section 7 • FSA Section 1	the outsourced services. These include the reporting and notification obligations, which are set out in the **Oracle Cloud Hosting and Delivery Policies** (see **Sections 1.12, 3.2.2, 4.1, 4.3** and **5.2.1**), the **FSA** (see **Section 6.2.2**) and the **DPA** (see **Section 2.8** and **Section 9.2**). Additionally, **Section 7 of the FSA** states that Oracle provides support for cloud services through a cloud customer support portal. Service notifications and alerts relevant to cloud services are posted on this portal and include notification of circumstances that can reasonably be expected to have a material impact on the provision of the services. Customers can also monitor the services by exercising their audit and access rights set out in **Section 1 of the FSA**.
4.	3.4.1(4)	These contract and vendor management processes should cover: a. whether the involvement of the cyber security function is actively required (e.g., in case of due diligence); b. the baseline cyber security requirements which should be applied in all cases; c. the right to periodically perform cyber security reviews and audits.	• Oracle Cloud Hosting and Delivery Policies Section 1 • DPA Section 7 • FSA Section 1 • DPA Section 8	**Section 1 of the Oracle Cloud Hosting and Delivery Policies** describes Oracle's information security practices including physical security safeguards, system and data access controls, encryption and training. **Section 7 of the DPA** sets out Oracle's obligation to implement and maintain appropriate technical and organisational security measures for the processing of personal information designed to prevent accidental or unlawful destruction, loss, alteration and unauthorised access or disclosure. **Section 1 of the FSA** sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under **Section 8 of the DPA.**
5.	3.4.1(5)	The contract management process should cover requirements for: a. executing a cyber security risk assessment as part of the procurement process; b. defining the specific cyber security requirements as part of the tender process;	• Oracle Cloud Hosting and Delivery Policies Section 5 • CSA Section 9 • OMA Schedule C Section 9	Oracle provides information to assist its customers in conducting the necessary risk assessments and due diligence. These include Consensus Assessment Initiative Questionnaires (CAIQs), audit reports and other information regarding Oracle Cloud operational and security practices, which can be accessed at: • OCI CAIQ: **oracle.com/a/ocom/docs/oci-corporate-caiq.pdf**

		c. evaluating the replies of potential vendors on the defined cyber security requirements; d. testing of the agreed cyber security requirements (risk-based); e. defining the communication or escalation process in case of cyber security incidents; f. ensuring cyber security requirements are defined for exiting, terminating or renewing the contract (including escrow agreements if applicable); g. defining a mutual confidentiality agreement.	• FSA Sections 3 and 4 • CSA Section 4 • OMA Schedule C Section 4	• Oracle Fusion Cloud Applications CAIQ: **oracle.com/a/ocom/docs/caiq-oracle-fusion-cloud-applications.pdf** • Oracle Enterprise Performance Management Cloud Applications CAIQ: **oracle.com/a/ocom/docs/caiq-oracle-epm-cloud-applications.pdf** • Oracle Cloud Applications CAIQ: **oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf** • Oracle Cloud Compliance: **oracle.com/corporate/cloud-compliance/** Audit Reports: Customers can obtain more information about available audit reports by contacting their Oracle sales representative. **Section 5 of the Oracle Cloud Hosting and Delivery Policies** describes the process for engaging Oracle Cloud support, which among other things provides assistance with technical service requests. The parties' termination rights are set out in **Section 9 of the CSA** or **Section 9 of the OMA Schedule C** (as applicable) and **Section 3 of the FSA.** Provisions relating to data retrieval, transition period and transition assistance, post-termination, are set out **Section 4 of the FSA**. **Section 4 of the CSA** or **Sections 4 OMA Schedule C** (as applicable) set out the parties' mutual obligation of confidentiality.
6.	3.4.1(6)	The vendor management process (i.e., service level management) should cover requirements for: a. periodic reporting, reviewing and evaluating the contractually agreed cyber security requirements (in SLAs).	• Oracle Cloud Hosting and Delivery Policies Section 3.2 • Oracle PaaS and IaaS Public Cloud Services Pillar Document Section 3.6	**Sections 3.2 of the Oracle Cloud Hosting and Delivery Policies** describes the target availability levels for cloud service as specified in **Section 3.6 of the Oracle PaaS and IaaS Public Cloud Services Pillar Document** and **Section 3.2 of the Oracle SaaS Public Cloud Services Pillar Document**.

			• Oracle SaaS Public Cloud Services Pillar Document Section 3.2	
Outsourcing				
7.	3.4.2(1)	The cyber security requirements within the outsourcing policy and process should be defined, approved, implemented and communicated within Member Organization.	See Article 3.4.1(1) above.	See Article 3.4.1(1) above.
8.	3.4.2(2)	The cyber security requirements regarding the outsourcing policy and process should be measured and periodically evaluated.	See Article 3.4.1(3) above.	See Article 3.4.1(3) above.
9.	3.4.2(3)	The outsourcing process should include: a. the approval from SAMA prior to material outsourcing; b. the involvement of the cyber security function; c. compliance with the SAMA circular on outsourcing.	N/A	Oracle provides various materials through My Oracle Support and the Oracle Cloud Console that may assist customers in their outsourcing-related submissions to regulators. In addition, as required by applicable law or regulation, Oracle will provide customers and their regulators with necessary information (including summaries of reports and documents) regarding the activities outsourced to Oracle. Oracle provides a detailed contract checklist to help customers identify the sections of the Oracle Cloud services contract that pertain to the requirements in the SAMA circular on outsourcing. For more information see, https://www.oracle.com/a/ocom/docs/contract-checklist-sama-rules-on-outsourcing.pdf
Cloud Computing				
10.	3.4.3(1)	The cyber security controls within the cloud computing policy for hybrid and public cloud services should be defined, approved and implemented and communicated within Member Organization.	See Article 3.4.1(1) above.	See Article 3.4.1(1) above. In addition, Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of “attestations.” These attestations can assist in your compliance and reporting, providing

				independent assessment of the security, privacy and compliance controls of the applicable Oracle cloud services. In reviewing these third-party attestations, it is important that you consider they are generally specific to a certain cloud service and may also be specific to a certain data center or geographic region. Such attestations include CSA STAR, SOC, and ISO/IEC 27001, 27017, and 27018.
11.	3.4.3(2)	The compliance with the cloud computing policy should be monitored.	See Article 3.4.1(2) above.	See Article 3.4.1(2) above.
12.	3.4.3(3)	The cyber security controls regarding the cloud computing policy and process for hybrid and public cloud services should be periodically measured and evaluated.	See Article 3.4.1(3) above.	See Article 3.4.1(3) above.
13.	3.4.3(4)(a)	The cloud computing policy for hybrid and public cloud services should address requirements for: the process for adopting cloud services, including that: 1. a cyber security risk assessment and due diligence on the cloud service provider and its cloud services should be performed; 2. the Member Organization should obtain SAMA approval prior to using cloud services or signing the contract with the cloud provider; 3. a contract should be in place, including the cyber security requirements, before using cloud services;	• See Article 3.4.1(5) above. • See Article 3.4.2(3) above. • Oracle Cloud services contract	See Article 3.4.1(5) above regarding information, Oracle makes available, to assist customers in conducting the necessary risk assessments and due diligence. Ordered cloud services are documented in the Ordering Document. See also, Article 3.4.2(3) above regarding assistance to customers in their outsourcing-related submissions to regulators. Contractual terms governing the outsourcing relationship and obligations between the parties are documented in the written Oracle Cloud services contract.
14.	3.4.3(4)(b)	The cloud computing policy for hybrid and public cloud services should address requirements for:	• Ordering Document	Oracle operates within various regions across the globe, including in Jeddah, Saudi Arabia. Each region is composed of one or more physically

		data location, including that: 1. in principle only cloud services should be used that are located in Saudi Arabia, or when cloud services are to be used outside Saudi Arabia that the Member Organization should obtain explicit approval from SAMA;	• Oracle Cloud Hosting and Delivery Policies Section 4.1.3	isolated and fault-tolerant data centers (also named availability domains). Customers may choose Jeddah as their data center region during their initial Oracle account setup, either in the Ordering Document (SaaS) or during account setup (OCI). For more information, visit: • Oracle Cloud Regions: **oracle.com/cloud/architecture-and-regions** • Oracle Cloud Region in Jeddah: **oracle.com/middleeast/news/announcement/oracle-second-generation-cloud-region-2020-07-20/** • OCI Regions and Availability Domains: **docs.oracle.com/iaas/Content/General/Concepts/regions.htm** The overview of the **Oracle Cloud Hosting and Delivery Policies** confirms that a customer's content will be stored in the data centre region applicable to the services and that Oracle may replicate customer content to other locations within the applicable data centre region in support of data durability. **Section 4.1.3 of the Oracle Cloud Hosting and Delivery Policies** states that Oracle may migrate services deployed in data centres retained by Oracle between production data centres in the same data centre region as deemed necessary by Oracle or in the case of disaster recovery. For data centre migrations for purposes other than disaster recovery, Oracle will provide a minimum of 30 days' notice to the customer.
15.	3.4.3(4)(c)	The cloud computing policy for hybrid and public cloud services should address requirements for: data use limitations, including that: 1. the cloud service provider should not use the Member Organization's data for secondary purposes;	• CSA Section 11.2 • OMA Schedule C Section 11	**Section 11.2 of the CSA** or **Section 11 of OMA Schedule C** (as applicable) describes Oracle use of data from cloud services, including the use of such data for cloud services analyses. Customer's data shall not be used for secondary purposes beyond that specified in the agreement.

16.	3.4.3(4)(d)	The cloud computing policy for hybrid and public cloud services should address requirements for: security, including that: 1. the cloud service provider should implement and monitor the cyber security controls as determined in the risk assessment for protecting the confidentiality, integrity and availability of the Member Organization's data;	• DPA Section 7 • Oracle Cloud Hosting and Delivery Policies Section 1 • Oracle PaaS and IaaS Public Cloud Services Pillar Document Section 1 • Oracle SaaS Public Cloud Services Pillar Document Section 1 • CSA Section 4 • OMA Schedule C Section 4 • CSA Section 5 • OMA Schedule C Section 5 • DPA Section 9	The Oracle Cloud services contract addresses the integrity, privacy and safety of customer content as follows: • Technical and organizational security measures: - **Section 7 of the DPA** (Security and Confidentiality) - **Section 1 of the Oracle Cloud Hosting and Delivery Policies** (Oracle Cloud Security Policy) - **Section 1 of the** Oracle PaaS and IaaS Public Cloud Services Pillar Document and **Section 1 of the** Oracle SaaS Public Cloud Services Pillar Document - Oracle's Corporate Security Practices: oracle.com/corporate/security-practices/ • Confidentiality and protection of customer content: - **Section 4 of the CSA** or **Section 4 of the OMA Schedule C** (as applicable) – specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services) - **Section 5 of the CSA** or **Section 5 of the OMA Schedule C** (as applicable) - **Section 9 of the DPA** (Incident Management and Breach Notification)
17.	3.4.3(4)(e)	The cloud computing policy for hybrid and public cloud services should address requirements for: data segregation, including that: 1. the Member Organization's data is logically segregated from other data held by the cloud service provider, including that the cloud service provider should be	• Oracle Cloud Hosting and Delivery Policies Section 1.7	**Section 1.7 of the Oracle Cloud Hosting and Delivery Policies** explains that customer data hosted in the Oracle Cloud Services environments are logically or physically segregated from the content of other customers. All Oracle Public Cloud networks are segregated from Oracle's Corporate networks.

		able to identify the Member Organization's data and at all times should be able to distinguish it from other data.		
18.	3.4.3(4)(f)	The cloud computing policy for hybrid and public cloud services should address requirements for: business continuity, including that: 1. business continuity requirements are met in accordance with the Member Organization's business continuity policy;	• FSA Section 5 • Oracle Cloud Hosting and Delivery Policies Section 2	**Section 5 of the FSA** confirms that Oracle will maintain a business continuity program with the objective of maintaining Oracle's internal operations used in the provision of cloud services and will monitor, test and review the implementation and adequacy of the program annually. **Section 2 of the Oracle Cloud Hosting and Delivery Policies** describes Oracle's service continuity strategy and data back-up strategy.
19.	3.4.3(4)(g)	The cloud computing policy for hybrid and public cloud services should address requirements for: audit, review and monitoring, including that: 1. the Member Organization has the right to perform a cyber security review at the cloud service provider; 2. the Member Organization has the right to perform a cyber security audit at the cloud service provider; 3. the Member Organization has the right to perform a cyber security examination at the cloud service provider;	• FSA Section 1 • DPA Section 8 • Oracle Cloud Hosting and Delivery Policies Section 3.2.2 • CSA Section 11.1 • OMA Schedule C Section 11.1	**Section 1 of the FSA** grants customers and their auditors, full access to all relevant business premises and data used for providing the cloud services, as well as unrestricted rights of inspection and auditing related to the cloud services, in each case as specified in the FSA. **Section 8 of the DPA** grants customers the right to audit Oracle's compliance with its obligations under the DPA. **Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies** indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability. **Section11.1 of the CSA or Section 11.1 of OMA Schedule C** (as applicable) explains that Oracle also continuously monitors the Cloud services.
20.	3.4.3(4)(h)	The cloud computing policy for hybrid and public cloud services should address requirements for: exit, including that: 1. the Member Organization has termination rights;	• CSA Section 9 • OMA Schedule C Section 9 • FSA Section 3 • CSA Section 9.5	Customers' termination rights are set out in **Section 9 of the CSA** or **Section 9 of the OMA Schedule C** (as applicable) and in **Section 3 of the FSA**. **Section 9.5 of the CSA** or **Section 9.4 of OMA Schedule C** (as applicable) states Oracle will make personal information and content available for retrieval by the customer at the end of the services period. This section also states Oracle will, except as may be required by law, delete, or otherwise

		2. the cloud service provider has to return the Member Organization's data on termination; 3. the cloud service provider has to irreversibly delete the Member Organization's data on termination.	• OMA Schedule C Section 9.4 • Oracle Cloud Hosting and Delivery Policies Section 6.1 • DPA Section 10.1	render unrecoverable any of customer content that remains in the services at the end of such retrieval period. **Section 6.1 of the Oracle Cloud Hosting and Delivery Policies** states Oracle will make content available in a structured, machine-readable format for retrieval by the customer for a specified period post-termination (retrieval period). Upon expiry of the retrieval period, Oracle will delete the content from the services unless otherwise required by applicable law. **Section 10.1 of the DPA** confirms that, on termination of an arrangement, Oracle will promptly return or delete any remaining copies of personal information, except as otherwise stated in the Oracle Cloud services contract.