ORACLE

Oracle Contract Checklist for the Central Bank of Kenya's Guideline on Outsourcing (CBK/PG/16)

December 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 December 2023.

Overview

Oracle has developed this document to help financial services institutions operating in Kenya review Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications in the context of the Guideline on Outsourcing (CBK/PG/16) (the **Guideline**) under the Central Bank of Kenya's Prudential Guidelines for Institutions Licensed Under the Banking Act of January 2013. We want to make it easier for you as a regulated institution to identify the sections of the Oracle Cloud services contract that may help you address applicable requirements under the Guideline. Please note that Oracle Advertising SaaS and NetSuite services are not included in the scope of this document.

In this document, you will find a list of the specific requirements under the Guideline relating to contractual arrangements, along with references to the relevant sections of the Oracle Cloud services contract and a short explanation to help you conduct your review of the Oracle Cloud services.

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

- **Oracle Cloud services agreement** – the Oracle Cloud Services Agreement (**CSA**) or Oracle Master Agreement (**OMA**) with Schedule C (Cloud)
- **FSA** – the Oracle Financial Services Addendum to the CSA or OMA, as applicable
- **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)** (Oracle SaaS Public Services Pillar Document, Oracle PaaS and IaaS Public Cloud Services Pillar Document, and Oracle Global Business Unit (GBU) Cloud Services Pillar Document, as applicable) and the **Oracle Data Processing Agreement** (**DPA**).

Regulatory Background

The Central Bank of Kenya is responsible for promoting financial stability in Kenya through regulation, supervision and licensing of financial institutions under its mandate. As part of its supervisory function, the Central Bank issues prudential guidelines concerning the operations of financial institutions.

In January 2013, the Central Bank issued its Prudential Guidelines for Institutions Licensed Under the Banking Act, which includes the Guideline on Outsourcing (CBK/PG/16) (the **Guideline**). The Guideline applies to all licensed banks that wish to outsource their activities and covers a number of areas including outsourcing policies, governance, risk management, business continuity, data security, and arrangements with service providers.

For information on financial services regulations and guidelines in other countries, please visit https://www.oracle.com/corporate/cloud-compliance/.

Guideline on Outsourcing (CBK/PG/16)

NO.	GUIDELINE PROVISION	DESCRIPTION	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT	ORACLE EXPLANATION
The Outsourcing Agreement				
1.	4.5.6.1 4.5.6.3	Outsourcing arrangements should be governed by a clearly written contract, the nature and detail of which should be appropriate to the materiality of the outsourced activity in relation to the ongoing business of the regulated entity. The terms and conditions governing the contract between the institution and the service provider should be carefully defined in written agreements.	Oracle Cloud services contract	The cloud services arrangement is governed by the written Oracle Cloud services contract, which includes all applicable terms and conditions.
2.	4.5.6.5	The agreement should be sufficiently flexible to allow the institution to retain an appropriate level of control over the outsourced activity and the right to intervene with appropriate measures to meet legal and regulatory obligations.	FSA Section 4	Customers retain a level of control of the contracted services including by virtue of their monitoring and audit rights under the Cloud services contract, which enable customers to assess the performance of the services. Section 4 of the FSA sets out a customer's right to terminate the services in certain circumstances if required by applicable law or regulation, including where termination is based on instructions from a financial services regulator.
3.	4.5.6.6	The agreement should also bring out the nature of legal relationship between the parties, that is, whether agent-principal or otherwise.	CSA Section 18.1 OMA General Terms Section 16.1	Under the Oracle Cloud services contract, the relationship between the parties is one of customer-service provider. Section 18.1 of the CSA or Section 16.1 of the OMA General Terms, as applicable, states that Oracle is an independent contractor and no partnership, joint venture, or agency relationship exists between the parties.
4.	4.5.6.6 (a)	The contract should clearly define what activities are going to be outsourced including appropriate service and performance standards.	Ordering Document Cloud Hosting and Delivery Policies Section 3	The services ordered are documented in the Ordering Document. Section 3 of the Cloud Hosting and Delivery Policies references the target availability levels for cloud service as specified in the relevant Cloud Service Pillar documentation (or in the relevant Cloud Services Service Description).
5.	4.5.6.6 (b)	The institution must ensure it has the ability to access all books, records and information relevant to the outsourced activity in the service provider.	FSA Section 1	A customer's audit and access rights are set out in Section 1 of the FSA. These include access to relevant business premises, devices, systems, networks, information and data used for providing the cloud services, including related financial information, and rights of inspection and auditing related to the cloud services in each case as set out in the FSA.
6.	4.5.6.6 (c)	The contract should provide for continuous monitoring and assessment by the institution of the service provider so that any necessary corrective measure can be taken immediately.	FSA Section 1	Customers can monitor the availability of Oracle cloud services by visiting the following sites: • Oracle Cloud Infrastructure: https://ocistatus.oraclecloud.com/ • Fusion Cloud Applications: https://saasstatus.oracle.com/ Information on monitoring the availability of certain other Oracle Cloud Application

				services is available upon request. Also, customers have access and audit rights as set out in Section 1 of the FSA.
7.	4.5.6.6 (d)	A termination clause and minimum periods to execute a termination provision, if deemed necessary, should be included.	CSA Section 9 OMA Schedule C Section 9 FSA Section 3	A customer's termination rights and the related notice periods are set out in Section 9 of the CSA or Section 9 of Schedule C to the OMA (as applicable) and in Section 3 of the FSA.
8.	4.5.6.6 (e)	The contract should include controls to ensure customer data confidentiality and service providers' liability in case of breach of security and leakage of confidential customer related information.	CSA Sections 4 and 5 OMA Schedule C Sections 4 and 5 Cloud Hosting and Delivery Policies Section 1 DPA Section 7	Sections 4 and 5 of the CSA or Sections 4 and 5 of the OMA Schedule C (as applicable) set out Oracle's obligation to keep confidential and protect confidential information. Section 1 of the 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.
9.	4.5.6.6 (f)	The contract should include contingency plans to ensure business continuity.	FSA Section 5.1 Cloud Hosting and Delivery Policies Section 2	Section 5.1 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 Cloud Hosting and Delivery Policies describes Oracle's service continuity strategy and data back-up strategy.
10.	4.5.6.6 (g)	The contract should provide for the approval by the institution of the use of subcontractors by the service provider for all or part of an outsourced activity.	FSA Sections 6.1 and 6.2 DPA Sections 5.1 and 5.3	Section 6.1 of the FSA and Section 5.1 of the DPA contain general written authorisations for Oracle to engage subcontractors, Oracle affiliates and third party subprocessors to assist in the performance of the services. Section 6.2 of the FSA sets out a process whereby a customer may object to the intended involvement of a strategic subcontractor in the provision of the services and, if the matter cannot be resolved, the customer may terminate the relevant services. Section 5.3 of the DPA sets out a customer's right to object to the intended involvement of a new Oracle affiliate or third party subprocessor.
11.	4.5.6.6 (h)	Provide the institution with the right to conduct audits on the service provider, whether by its internal or external auditors or by agents appointed to act on its behalf, and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed for the institution.	FSA Section 1 DPA Section 8	Section 1 of the FSA sets out a customer's audit and access rights in respect of the ordered services. Section 1.2 It includes a process for requesting that a third party conduct an audit on the customer's behalf. Section 1.9 references a customer's ability to request copies of attestations and audit reports. Section 8 of the DPA sets out the customer's right to audit Oracle's compliance with its obligations under the DPA and provides the process for requesting such audits.

12.	4.5.6.6 (i)	A clause to allow the Central Bank or persons authorized by it to access the institution's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. The Agreement should further provide that in the event these are not made accessible to the Central Bank within a reasonable time, the Central Bank may pursue any or all of the remedial actions and administrative sanctions provided for under the Banking Act.	FSA Section 2	Section 2 of the FSA sets out the audit and access rights of a customer's financial services regulator, or any person appointed to act on its behalf, in respect of the ordered services.
13.	4.5.6.6 (j)	A clause to recognize the right of the Central Bank to cause an inspection to be made of a service provider of a bank and its books and account by one or more of its officers or employees or other persons.	FSA Section 2.1	Section 2.1 of the FSA specifies that the audit and access rights of a financial services regulator, or any person appointed to act on its behalf, includes the right to conduct an inspection.
14.	4.5.6.6 (k)	There should be dispute resolution mechanism between parties involved in outsourcing contract.	FSA Section 10	Section 10 of the FSA sets out the process for resolving disputes between the parties.
15.	4.5.6.6 (l)	Details of pricing and fee structure of outsourcing contract should be provided.	Ordering Document	The fees applicable to the ordered services are set out in the Ordering Document.
Confidentiality and Security				
16.	4.5.7 (a)	Access to customer information by staff of the service provider should be limited to those areas where the information is required in order to perform the outsourced function.	Cloud Hosting and Delivery Policies Section 1	Section 1 of the Cloud Hosting and Delivery Policies describes the security practices that apply to customer content. These practices include physical access controls, system access controls, data access controls, user encryption, and data and network segregation. Section 1.4 confirms that for service components managed by Oracle, access to customer content is restricted to authorized Oracle staff.
17.	4.5.7 (b)	The institution should ensure that the service provider is able to isolate and clearly identify the institution's customer information, documents, records and assets to protect the confidentiality of the information.	Cloud Hosting and Delivery Policies Section 1.7 CSA Sections 4 and 5 OMA Schedule C Sections 4 and 5	Section 1.7 of the Cloud Hosting and Delivery Policies confirms that customer content is logically or physically segregated from the content of other customers hosted in the Oracle Cloud Services environments, and that all Oracle Public Cloud networks are segregated from Oracle's corporate networks. Oracle's obligations to protect the confidentiality of customer information are further set out in Sections 4 and 5 of the CSA or Sections 4 and 5 of the OMA Schedule C (as applicable).
18.	4.5.7 (c)	The institution should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches.	FSA Section 1 Oracle Cloud Compliance site Oracle Corporate	Customers can exercise their audit and access rights under Section 1 of the FSA to monitor the ordered services. There is also information available to customers that may assist them in conducting any necessary due diligence or risk assessments, including the information contained in the

			Security Practices Cloud Hosting and Delivery Policies DPA Section 9	Oracle Cloud Compliance site, the Oracle Corporate Security Practices and the Cloud Hosting and Delivery Policies. Section 9 of the DPA sets out Oracle's commitment to notify customers of a security breach involving customer content that is transmitted, stored or otherwise on Oracle systems or the cloud services environments.
19.	4.5.7 (d)	The institution should immediately notify CBK in the event of any breach of security and leakage of confidential customer related information. In these eventualities, the institution would be liable to its customers for any damage.	See Row 18	See Row 18 above for information about Oracle's security breach notification obligation.
Business Continuity Management				
20.	4.5.8 (a)	The institution should require its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. Institutions need to ensure that the service provider periodically tests the Business Continuity and Recovery Plan and may also consider occasional joint testing and recovery exercises with its service providers.	FSA Section 5.1 Risk Management Resiliency Program	Section 5.1 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. Upon 30 days' notice and no more than once per calendar year, Oracle will make available to a customer via web conference or on Oracle premises, in a guided manner, a summary of Oracle's business continuity program and applicable test information, material modifications to the program within the last 12 months and pertinent governance areas, and confirmation that an internal review of these governance areas was performed within the last 12 months. Information about Oracle's Risk Management Resiliency Program can be found here.
21.	4.5.8 (b)	In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, institutions should retain an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of the institution and its services to the customers.	FSA Sections 4.2 and 4.3	The FSA contains provisions that aim to ensure an orderly transition of the services in the event of termination of the Cloud services contract. Section 4.2 of the FSA states that Oracle will, upon written request, continue to make services under the contract available for up to an additional 12 months from termination subject to certain conditions. Section 4.3 of the FSA explains that if a customer requires assistance with a transition, either to another service provider or to the customer's own organisation, Oracle will enter into good faith negotiations regarding the provision of such transition assistance services.
22.	4.5.8 (c)	In establishing a viable contingency plan, institutions should consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency and the costs, time and resources that would be involved.	See row 21	See row 21 above for information about how Oracle can assist customers with transitioning the services to another service provider or to the customer's own organisation.

23.	4.5.8 (d)	Outsourcing often leads to the sharing of facilities operated by the service provider. The institution should ensure that service providers are able to isolate the institution's information, documents and records, and other assets. This is to ensure that in adverse conditions, all documents, records of transactions and information given to the service provider, and assets of the institution, can be removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.	Cloud Hosting and Delivery Policies Section 1.7	Section 1.7 of the Cloud Hosting and Delivery Policies confirms that customer content is logically or physically segregated from the content of other customers hosted in the Oracle Cloud Services environments, and that all Oracle Public Cloud networks are segregated from Oracle's corporate networks.
Monitoring and Control of Outsourced Activities				
24.	4.5.9.4	The institution should ensure that outsourcing agreements with the service providers contain provisions to address their monitoring and control of outsourced activities.	See row 7	See row 7 above for information about a customer's ability to monitor the ordered services.
25.	4.7.4	The governing law of the arrangement should also be clearly specified.	CSA Section 15 OMA General Terms Section 13	The governing law of the contract is set out in Section 15 of the CSA or Section 13 of the OMA General Terms (as applicable).

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