ORACLE

Advisory: Oracle Cloud Applications (SaaS) and Select Kenyan Regulatory Guidelines

Description of Oracle Cloud Applications (SaaS) corporate security practices in the context of certain Central Bank of Kenya (CBK) prudential and cybersecurity guidelines.

August 2023, Version 1.0

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in assessing your use of Oracle cloud services in the context of the guidelines applicable to you as a financial institution under the Central Bank of Kenya (CBK) prudential guidelines and/or cybersecurity guidelines. This document may also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document. The information in this document is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations referenced in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied on in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

The CBK prudential guidelines and cybersecurity guidelines referenced in this document are subject to periodic changes or revisions by the CBK. The current versions of the guidelines are available at:

- Central Bank of Kenya (CBK) Prudential Guidelines for Institutions Licenced under the Banking Act
- Guideline on Cybersecurity for Payment Service Providers (PSPs)

This document is based on information available at the time of drafting, it is subject to change at the sole discretion of Oracle and may not always reflect changes in the regulations.

Table of Contents

Introduction

The Central Bank of Kenya (CBK) is a principal financial services regulator in Kenya, responsible for the prudential regulation and supervision of certain financial institutions, including banks, microfinance institutions, and payment service providers.

Key guidelines issued by the CBK relating to cybersecurity, outsourcing arrangements, and risk management include:

- Prudential Guidelines on Outsourcing (Prudential Guidelines)
- Guideline on Cybersecurity for Payment Service Providers (Cybersecurity Guidelines)

While Oracle itself is not regulated or supervized by the CBK, it recognizes that some of its customers operating in Kenya may be required to comply with the Prudential Guidelines and/or the Cybersecurity Guidelines and wishes to support those customers in meeting their compliance objectives.

Document Purpose

This document is intended to provide relevant information about Oracle Cloud Applications (SaaS) to assist you in determining the suitability of Oracle Cloud Applications (SaaS), having regard to the Prudential Guidelines and the Cybersecurity Guidelines.

The information in this document applies to the following Oracle Cloud Applications:[1]

- Enterprise Resource Planning (ERP)
- Enterprise Performance Management (EPM)
- Supply Chain Management & Manufacturing (SCM)
- Human Capital management (HCM)

Note: Oracle Netsuite and Advertising SaaS Services are not included in the scope of this document.

The information contained in this document does not constitute legal advice. Customers are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by Oracle regarding their specific legal and regulatory requirements.

About Oracle Cloud

Oracle's mission is to help people see data in new ways, discover insights, and unlock endless possibilities. Oracle provides several cloud solutions tailored to customer needs. These solutions provide customers with the benefits of the cloud, including global, secure, and high-performance environments to run all their workloads. The cloud solutions discussed in this document are Oracle Cloud Applications (SaaS).

Oracle Cloud Applications (SaaS) provide comprehensive and connected SaaS suite. By delivering a modern user experience and continuous innovation, Oracle is committed to our customers' success with continuous updates and innovation across the entire business: finance, human resources, supply chain, manufacturing, advertising, sales, customer service, and marketing. For more information on Oracle Cloud Applications, see https://www.oracle.com/applications.

The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On-premises customers are in full control of their technology infrastructure. For example, they have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers

use components that are partially under the management of the cloud service providers. As a result, the management of security in the cloud is a shared responsibility between cloud customers and the cloud service provider.

Oracle provides best-in-class security technology and operational processes in support of Oracle's secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle Cloud Applications (SaaS). By design, Oracle provides security functions for cloud infrastructure and operations (e.g., cloud operator access controls, infrastructure security patching, etc.), and customers are responsible for securely configuring and using their cloud resources. For more information, please refer to the cloud service documentation.

The following figure illustrates this division of responsibility at high level.

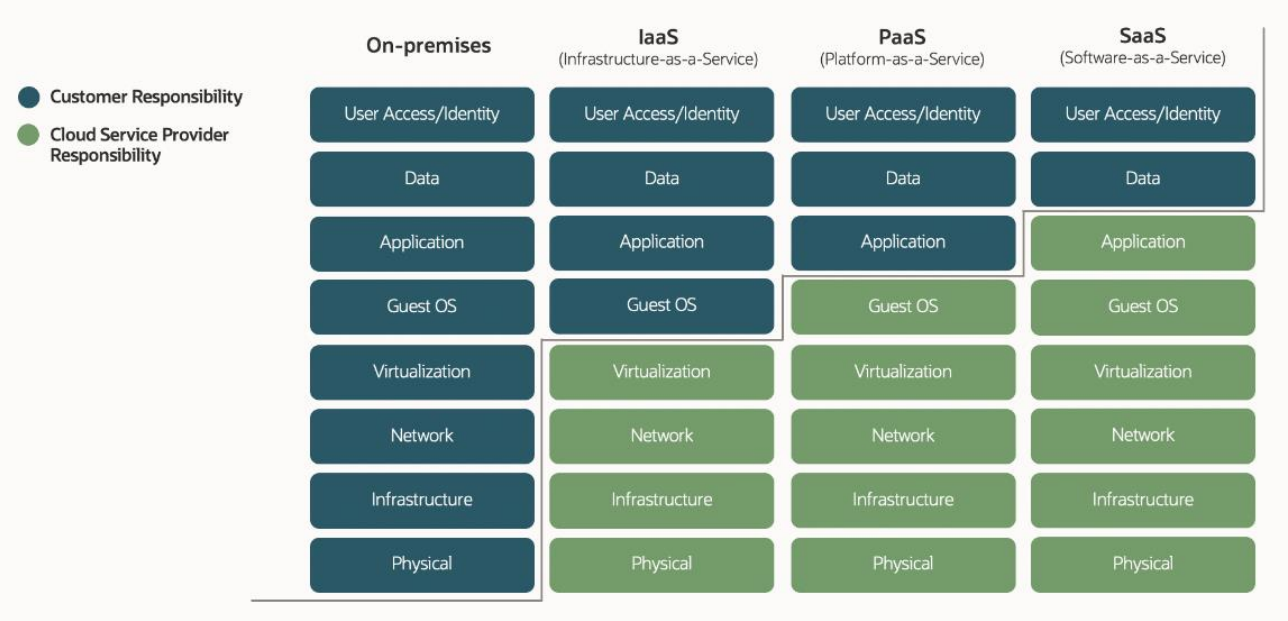

Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers

Overview of the Prudential Guidelines and Cybersecurity Guidelines

This section provides an overview of select provisions of the Prudential Guidelines and the Cybersecurity Guidelines that relevant financial services institutions in Kenya should consider.

Financial services institutions are responsible for determining the suitability of a cloud service in the context of these requirements and their needs. They are also responsible for ensuring that their use of the cloud service and internal business processes meet these requirements. However, Oracle provides certain features and functions that may help you meet the requirements.

There are two parts to this section:

- Part 1 –Sets out relevant information about Oracle and Oracle Cloud Solutions.
- Part 2 –Addresses certain provisions of the Prudential Guidelines and Cybersecurity Guidelines by reference to Oracle Cloud Applications (SaaS) services and operational and security practices.

Part 1 – About Oracle and Oracle Cloud Solutions

Is Oracle a regulated entity under the supervision of the CBK?

No. Oracle is not under the direct supervision of CBK. However, Oracle may assist regulated customers by providing some of the information and resources that may support a regulated customer's ability to comply with regulatory guidelines.

Does Oracle have a specific cloud contract for the financial services sector?

Yes. In addition to its comprehensive cloud hosting and delivery policies, data protection commitments, and security terms, Oracle offers the Financial Services Addendum (FSA) as an add-on to the Oracle Cloud Services Agreement (CSA) or to the Oracle Master Agreement (OMA), as applicable. The FSA addresses various topics typically requested by regulated customers in the financial services sector, including audit rights for customers and their regulators, expanded termination rights, exit and transition assistance services, business continuity, and subcontracting arrangements.

What customer data will Oracle process in the context of the provision of a contracted Oracle cloud service?

Oracle cloud services typically handle two types of customer data:

- Customer account information that is needed to operate the customer's cloud account. This information is primarily used for customer account management, including billing. Oracle is a controller with regard to the use of personal information that it gathers from the customer for purposes of account management and handles such information in accordance with the terms of the Oracle General Privacy Policy.
- Customer content that customers choose to store within Oracle cloud services, which may include personal information gathered from the customer's data subjects, such as its users, end customers, or employees.

It is important to note that Oracle does not have a direct relationship with the customer's data subjects. The customer is the controller in these situations and is responsible for data collection and data use practices. Oracle is the processor that acts on the instructions of the customer and handles personal information contained in customer content in accordance with the general processing terms of the Oracle Services Privacy Policy and the Oracle Data Processing Agreement.

Does Oracle have access to customer content?

Under the SaaS model, authorized Oracle employees can access customer content in limited circumstances. This access is audited, and logged. Oracle customers are responsible for administering their own access rights with regard to their cloud services environment.

Oracle Database Vault and Break Glass, as optional service for Oracle Fusion, provide additional security by restricting administrative access to systems and services. As such, Oracle Support representatives can access a customer's cloud environment only after customer approvals and relevant authorization have been obtained. For more information, see Oracle Break Glass,

How is customer content protected against access by unauthorized third parties, including other Oracle customers?

Oracle provides secure and reliable product offerings and services, and prioritizes protecting their integrity and security. Oracle cloud services are designed and operated following a defense-in-depth model. This model starts with a default-deny 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. This provides a foundation for ensuring that tenants are isolated from one another.

Access controls are implemented to govern access to and use of resources. These controls include following a least-privilege model designed as a system-oriented approach where user permission and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.

How does Oracle manage availability risks?

Oracle deploys its cloud services on a resilient computing infrastructure designed to maintain service availability and continuity if an adverse event affects the services. Oracle cloud service data centres align with Uptime Institute and

Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Ddata centres housing Oracle cloud infrastructure services use redundant power sources and maintain backup generators in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.

Oracle periodically makes backups of a customer's production data and stores such backups at the primary site used to provide the Oracle cloud services. Backups may also be stored at an alternative location for retention purposes. For more information, see section 2 of the Oracle Cloud Hosting and Delivery Policies at oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf.

How does Oracle handle security incidents?

Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed data has been accessed by an unauthorized entity. The Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (LoBs). In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, Oracle will promptly notify impacted customers or third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle services. Information about malicious attempts or suspected incidents and incident history are not shared externally.

Does Oracle provide audit rights to customers and their regulators?

Yes. Customers and their financial services regulators have the unrestricted right to access and audit Oracle's compliance with its obligations under their cloud services agreement as specified in the FSA. Such audit rights include the right to conduct emergency audits. In addition, Oracle grants customers and their financial services regulators the same rights of access and audit in respect of Oracle strategic subcontractors. Such audit rights and related terms are set out in the FSA.

What compliance documentation does Oracle provide?

Oracle provides information about frameworks for which an Oracle line of businesshas 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 Applications. Such attestations include CSA Star, SOC, and ISO/IEC 27001, 27017, and 27018. These attestations are generally specific to a certain cloud service and may also be specific to a certain data centre or geographic region.

Additionally, Oracle provides general information and technical recommendations for the use of its cloud services in the form of "advisories." These advisories are provided to help customers determine the suitability of using specific Oracle cloud services and implement specific technical controls to help meet compliance obligations.

For more information, see oracle.com/cloud/compliance/.

Oracle also provides a descriptions of its security practices for some of itscloud services in a Consensus Assessment Initiative Questionnaire (CAIQ). The CAIQs are publicly available at https://www.oracle.com/corporate/security-practices/cloud/, and customers can download to review that cloud services security practices to determine the risks associated with its use

Part 2 – Summary of select Prudential Guidelines and Cybersecurity Guidelines

Prudential Guidelines – Guideline on Outsourcing (CBK/PG/16) – 4.5.5.1. – Due Diligence

"In considering or renewing an outsourcing arrangement, appropriate due diligence should be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement."

Customers are solely responsible for conducting their own due diligence when considering the outsourcing of services.

Oracle provides several resources to assist existing and prospective customers in conducting necessary due diligence, including access to security questionnaires, audit reports, and other information about Oracle's operational and security practices.

For more information, see:

Oracle Cloud Compliance site - https://www.oracle.com/corporate/cloud-compliance/

Cloud Services Hosting and Delivery Policies – http://www.oracle.com/corporate/cloud-services-hostingand-delivery-policies

Oracle Corporate Security Practices - https://www.oracle.com/corporate/security-practices/cloud/

Cybersecurity Guidelines –3.4 (vii) – Security Incident Reporting

"Make it mandatory for their outsourced providers to report security incidents/breaches within a certain timeframe in line with best practice. Typically, 48 hours is a good benchmark."

Oracle's Information Security Incident Reporting and Response Policy defines the requirements for reporting and responding to incidents. This policy authorizes the Oracle Global Information Security organization to provide overall direction for security event and incident preparation, detection, investigation, and resolution within Oracle's Lines of Business.

In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, Oracle will promptly notify any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities.

See Oracle Cloud Hosting and Delivery Policies, Pillar Documents and Service Descriptions for specific details about Oracle incident notifications:

http://www.oracle.com/corporate/cloud-services-hostingand-delivery-policies

Cybersecurity Guidelines –3.4 (ix) – Service Levels and Performance

"Ensure that Service Level Agreements should have robust provisions in relation to security, service availability, performance metrics and penalties."

Oracle commits to deliver cloud services at the agreed level of availability, and offers tools and services to support the monitoring obligations of its customers.

Also, Oracle Cloud Applications use a combination of tools, portals, and reports to provide customers insight and transparency regarding how their environments are performing and meeting various industry standards.

Customers can access metrics on the service availability for their ordered Oracle cloud services through the customer notifications portal, where available, or upon request.

For more information, see the Oracle Cloud Application (SaaS) status page here: https://saasstatus.oracle.com/

Prudential Guidelines – Guideline on Outsourcing (CBK/PG/16) –4.5.6.4. – Risk Management

"Every outsourcing agreement should address the risks and risk mitigation strategies identified at the risk evaluation and due diligence stages."

Customers are solely responsible for ensuring that all identified risks are satisfactorily addressed within the service agreement.

The provision of Oracle Cloud Application (SaaS) services and the relationship between Oracle and its customers are governed by the terms set out in a contract agreement, which addresses different risk areas within the lifecycle of the contract.

Also, Oracle has protective measures for identifying, analyzing, measuring, mitigating, responding to, and monitoring risk specific to its cloud services. Risk assessments are performed annually across Oracle cloud services to identify threats and risks that could impact the integrity, confidentiality, or availability of the system. Risks are reviewed, assigned an owner, and remediated in line with the Oracle cloud services risk management assessment program. The results of internal audits, external audits, customer audits, and other compliance activity findings are collated as inputs into Oracle's risk assessment process.

For more information, see Oracle Cloud Security Practices, Oracle Corporate Security Practices and the Risk Management Resiliency Program (RMRP).

Prudential Guidelines – Guideline on Outsourcing (CBK/PG/16) –4.5.7. (b) – Data Confidentiality and Security

"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."

Oracle Cloud provides customers with the capability to restrict access to information stored or processed in their application and cloud tenancy in accordance with Oracle's policies and confidentiality commitments. Additionally, the Oracle Cloud services contract addresses the availability, integrity and privacy of customers' content through technical and organization security measures.

Also, the Oracle Identity and Access Management on SaaS applications enables the capabilities of role-based access control (RBAC), ensuring the access management principles of "need to know," "least privilege," and "segregation of duties".

The Data Processing Agreement for Oracle Services describe Oracle's commitments regarding the processing of personal information.

Prudential Guidelines – Guideline on Outsourcing (CBK/PG/16) –4.5.7. (a) – Access Management

"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".

Customers are responsible for the user access provisioning in their use of Oracle SaaS Cloud Applications.

The Oracle Logical Access Controls Policy and standard describes logical access control requirements for Oracle systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined 'users' with access to Oracle systems. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles:

- Need to know: Does the user require this access for his job function?
- Segregation of duties: Will the access result in a conflict of interest?
- Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?

Oracle reviews and revalidates Oracle administrative user access for least privilege and separation of duties on a quarterly cadence.

Also, Oracle Cloud Applications adhere to documented security standards that defines access requirements and processes, which includes segregation of privileged access.

For more information, see Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Applications and Oracle Cloud Security Practices

Prudential Guidelines – Guideline on Outsourcing (CBK/PG/16) –4.5.6.1 – Outsourcing Agreements

"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 provision of Oracle Cloud Application (SaaS) services and the relationship between Oracle and its financial services customers may be governed by the terms set out in the following contractual documents:

The **Oracle Cloud Services Agreement (CSA)** covers:

- Description of the services
- Governing law and jurisdiction
- Start date and end date of the agreement
- Notice period and procedures

The **Ordering Document** covers:

- Description of the cloud services
- Service-period term
- Fees
- Data center region (for SaaS cloud services)

The Oracle **Financial Services Addendum (FSA)** covers:

- Audit rights for customers and financial services regulators
- Termination rights
- Exit provision including data retrieval, transition period, and transition services
- Business continuity
- Strategic subcontractors
- Compliance with law applicable to Oracle's provision of services
- Assistance with regulatory obligations, including the provision of necessary information requested by the customer's competent authority

The **Data Processing Agreement (DPA)** for Oracle services covers key data privacy requirements for services engagements, such as:

- Allocation of responsibilities between the customer and Oracle
- Assistance with handling privacy inquiries and requests from individuals
- Subprocessor management and due diligence
- Cross-border data transfers
- Security and confidentiality
- Audit rights
- Incident management and breach notification
- Return and deletion of personal information

For more information, see Oracle cloud services contracts.

Prudential Guidelines – Guideline on Outsourcing (CBK/PG/16) –4.5.6.6. (h) – Audit Rights

"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."

Customers and their financial services regulators have the right to assess and audit Oracle's compliance with its obligations under their cloud services agreement as specified in the FSA.

In addition, Oracle grants customers and their financial services regulators the same rights of access and audit of Oracle strategic subcontractors.

Such audit rights and related terms are covered by the FSA.

Audit reports about Oracle cloud services are periodically published by Oracle's third-party auditors.

Prudential Guidelines – Guideline on Outsourcing (CBK/PG/16) – 4.5.6.6. (f) – Business Continuity

"Some of the key provisions of the contract include: contingency plans to ensure business continuity"

Customers are solely responsible for creating their internal business continuity plans.

Oracle maintains its own business continuity program with the objective of maintaining, in the event of a disruption, Oracle's internal operations that are used to provide the cloud services. Oracle monitors, tests and reviews the implementation and adequacy of its business continuity program annually. Upon request by a customer, Oracle will provide a guided summary of its program and applicable test information, material modifications to the program within the last 12 months, and pertinent program governance areas, along with confirmation that an internal review of these governance areas was performed within the last 12 months.

For more information, see Oracle Risk Management Resiliency Business Continuity

Prudential Guidelines – Guideline on Outsourcing (CBK/PG/16) –4.5.6.6. (d) – Termination Rights

"A termination clause and minimum periods to execute a termination provision, if deemed necessary, should be included."

Customers have the right to terminate Oracle cloud services in the following situations, as set out in the cloud services agreement:

1. Termination due to regulatory requirements
    - Termination requested based on express instruction issued by the regulator.
    - Oracle is in a breach of applicable law or regulation in providing the relevant cloud services.
    - Impediments affecting Oracle's ability to perform the cloud services are identified.
    - There are material changes affecting the cloud services or Oracle which result in an adverse impact on the provision of the cloud services.
    - There are weaknesses regarding the management and security of Your Content or Confidential Information.
2. Termination due to insolvency
    - Oracle has become insolvent or resolved to go into liquidation.
    - A proposal is made for entering into any compromise or arrangement with any or all of Oracle's creditors.
    - A receiver is appointed over all or substantially all the assets of Oracle.

Also, Oracle supports its customers when a contract is terminated, by providing the following:

- Transition period and services - The FSA provides customers with the ability to order transition services and transition assistance to facilitate the transfer or the re-incorporation of the concerned function back to the customer or to a third-party provider.
- Data retrieval - For a period of 60 days upon termination, Oracle makes available, by means of secure protocols and in a structured, machine-readable format, customers' content residing in the production cloud services environment, or keep the cloud service system accessible, for the purpose of data retrieval. Oracle provides reasonable assistance to customers to retrieve their content from the production services environment and will provide help to understand the structure and format of the exported file.
- Data deletion - Following expiry of the retrieval period, Oracle deletes the data (unless otherwise required by applicable law).

For more information, see:

FSA section 3: Additional Termination Rights.

CSA section 9: Customer Termination Rights

FSA section 4: Exit Provision.

DPA section 9.1

Cloud Services Hosting and Delivery Policies: Section 6.1 – Termination of Oracle cloud services

Prudential Guidelines – Guideline on Outsourcing (CBK/PG/16) –4.5.6.6. (g) – Subcontractors

"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."

Customers are solely responsible for implementing a subcontracting risk appetite framework that is proportional to their business strategy.

Oracle may use subprocessors or subcontractors (collectively "subcontractors") to deliver some of its cloud services. Oracle reviews all of its subcontractors that provide services to Oracle as part of its cloud services according to a published criteria (see the following details) to determine the status of such subcontractors. Oracle publishes lists of its subprocessors and strategic subcontractors to customers through My Oracle Support.

Oracle notifies customers of any new strategic subcontractor or new third-party subprocessor, and customers have a 30-day period to object to Oracle's use of such strategic subcontractor or third-party subprocessor. If the parties are not able to adequately address the customer's objections, the customer has the right to terminate the relevant cloud services.

Oracle strategic subcontractor criteria

To determine whether a proposed subcontractor qualifies as a strategic subcontractor, , Oracle considers the following criteria:

- Whether a failure in the subcontractor's performance would materially impair Oracle's obligations under the cloud services agreement
- Oracle's ability to easily replace the subcontractor
- Frequency of the subcontractor's engagement
- Whether the subcontractor may have access to customer data
- Impact to the relevant Oracle cloud services if the subcontractor must be changed

For more information, see FSA section 5: Strategic subcontractors and other subcontractors

Conclusion

Oracle is committed to helping customers operate globally in a fast-changing business environment, and meet their obligations under the CBK prudential guidelines and requirements. Oracle Cloud Applications (SaaS) services and capabilities provide some features that may help customers meet their compliance objectives.