

# Oracle Contract Checklist for Select South African Financial Services Directives and Guidance

- **Prudential Authority directive and guidance on cloud computing and offshoring of data in the financial services sector (Directive 3 of 2018 and Guidance Note 5 of 2018)**
- **Office of the Registrar of Banks guidance to banks in relation to the outsourcing functions within a bank and cyber resilience (Guidance Note 5 of 2014 and Guidance Note 4 of 2017)**
- **Financial Services Board of the Republic of South Africa directive on outsourcing of insurance business, (Directive 159.A.i)**

July 2022, Version 1.0

Copyright © 2022, Oracle and/or its affiliates

Public

## 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 with assessing your use of Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications (SaaS) in the context of the requirements applicable to you under the South African Cloud Regulations and Guidance (as defined on p.4). This may also help you to assess Oracle as a cloud service provider. You remain responsible for making your own independent assessment of the information in this document as 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 discussed in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied upon 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 South African Cloud Regulations and Guidance are subject to periodic changes or revisions by the Prudential Authority (PA), the Office of the Registrar of Banks and the Financial Services Board of the Republic of South Africa (FSB).

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

## Table of Contents

---

<b>Disclaimer .....</b>	<b>2</b>
<b>Introduction .....</b>	<b>3</b>
<b>Document Purpose .....</b>	<b>4</b>
<b>About Oracle Cloud Infrastructure.....</b>	<b>5</b>
<b>The Cloud Shared Management Model .....</b>	<b>5</b>
<b>Select South African Financial Services Directives and Guidance Notes.....</b>	<b>6</b>

## Introduction

The Financial Sector Regulation (FSR) Act was signed into law in 2017 to reorganize the supervisory and regulatory structure of the financial services sector in South Africa. The FSR Act created a “twin peaks” approach to regulation of the financial services industry by forming the Prudential Authority (PA) and the Financial Sector Conduct Authority (FSCA). The PA regulates commercial banks, mutual banks, co-operative banks, insurers, co-operative financial institutions, financial companies, and market infrastructures under the supervision of the South African Reserve Bank (SARB), while the FSCA serves as a market conduct regulator.

Since its creation, the PA has issued a directive and guidance note pertaining to cloud computing and offshoring of data in the financial services sector referred to as Directive 3 of 2018 (D3/2018) and Guidance Note 5 of 2018 (G5/2018), (collectively “PA Regulations”). Prior to the creation of the PA, the Office of the Registrar of Banks issued guidance to banks in relation to the outsourcing functions within a bank and cyber resilience by way of Guidance Note 5 of 2014 (G5/2014) and Guidance Note 4 of 2017 (G4/2017). G5/2014 and G4/2017 were not replaced by the PA Regulations, but rather should be interpreted and applied in conjunction with the PA Regulations.

Additionally, in 2012, the Financial Services Board (FSB) implemented Directive 159.A.i, which specifies the rules applicable to outsourcing by insurers in South Africa.

All of the above regulations shall collectively be referred to as the “South African Cloud Regulations and Guidance” throughout this document.

For more information, see <https://www.resbank.co.za/en/home> and <https://www.fsca.co.za/Enforcement-Matters/Directives/Forms/DispForm.aspx?ID=436>.

The current versions of PA’s directive on cloud computing and offshoring of data is available at: <https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-directives/2018/8749>.

The current versions of the PA’s and the Office of the Registrar’s guidance notes on cloud computing and offshoring of data and guidance on the outsourcing functions within banks and cyber resilience, respectively, are available at <https://www.resbank.co.za/en/home/publications/guidance-notes/banks-guidance-notes>.

The current version of the Financial Services Board of the Republic of South Africa directive on outsourcing insurance business is available at: <https://www.fsca.co.za/Enforcement-Matters/Directives/Forms/DispForm.aspx?ID=436>.

## Document Purpose

This document is intended to provide relevant information related to OCI and SaaS cloud services to assist you in determining the suitability of using OCI and SaaS in relation to the South African Cloud Regulations and Guidance. Additionally, we want to make it easier for you as a financial institution to identify the sections of the Oracle Cloud services contract that pertain to such requirements. In certain sections of this document, you will find a list of specific requirements under the South African Cloud Regulations and Guidance 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.

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 CSA or OMA 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 \(DPA\)](#)

## About Oracle

Oracle’s mission is to help people see data in new ways, discover insights, unlock endless possibilities. Oracle provides a number of cloud solutions tailored to customers’ needs. These cloud offerings provide customers the benefits of the cloud including global, secure, and high-performance environments to run all their workloads.

## About Oracle Cloud Infrastructure

Oracle Cloud Infrastructure (OCI) is a set of complementary cloud services that enable customers to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance compute capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from on-premises network. OCI delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information on Oracle OCI, see <https://docs.oracle.com/en-us/iaas/Content/home.htm>.

## About Oracle Cloud Applications

Oracle Cloud Applications (SaaS) is the world’s most complete, connected SaaS suite. By delivering a modern user experience and continuous innovation, Oracle is committed to the success of your organization with continuous updates and innovations across the entire business: finance, human resources, supply chain, manufacturing, advertising, sales, customer service, and marketing. For more information about Oracle Cloud Applications, see <https://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 the cloud customers and the cloud service provider.

Oracle provides best-in-class security technology and operational processes to 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 services. By design, Oracle provides security functions for cloud infrastructure and operations (e.g., cloud operator access controls, infrastructure security patching), 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.

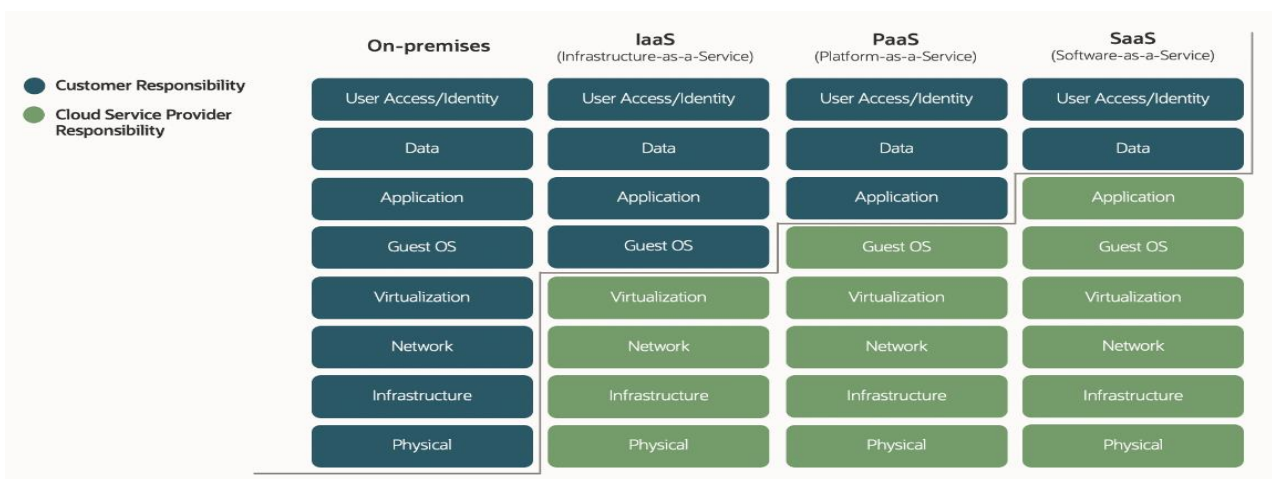


Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud provider

## Select South African Financial Services Directives and Guidance Notes

There are three main South African regulatory authorities that include five financial services directives and guidance notes that govern the provision of cloud services applicable to financial services customers in South Africa (collectively referred to as the “South African Cloud Regulations and Guidance”):

1. Prudential Authority directive and guidance on cloud computing and offshoring of data in the financial services sector D3/2018 and G5/2018, respectively
2. Office of the Registrar of Banks guidance to banks in relation to the outsourcing functions within a bank and cyber resilience G5/2014 and G4/2017
3. Financial Services Board of the Republic of South Africa directive on outsourcing of insurance business, Directive 159.A.i

This section provides an overview of certain South African Cloud Regulations and Guidance rules that financial services customers may need to consider. Omitted portions have been identified as general guidance for financial institutions on establishing an internal strategy and cybersecurity governance programs and are not specific to the use of OCI and/or SaaS services.

Customers are solely responsible for determining the suitability of using OCI and SaaS in the context of the South African Cloud Regulations and Guidance. However, the Oracle practices and resources below may assist you in the evaluation of OCI and SaaS services within the shared management model.

### PA Directive 3 of 2018 (Cloud Computing and Offshoring of Data) (D3/2018) and FSB Directive 159.A.i

TOPIC REF.	REGULATION REQUIREMENT/DESCRIPTION	FSB DIRECTIVE 159.A.I EQUIVALENT	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
D3/2018 2.2.9	The use of cloud computing/or offshoring of data must not in any way infringe on the bank's supervisors or prevent any regulatory mandated access to information, nor must it [have] impact on its regulator's ability to fulfil their duties.	7.7.15	Sections 1 and 2 (2.1, 2.4, 2.5) FSA	<p><b>Section 1 of the FSA</b> 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.</p> <p><b>Section 2.4 of the FSA</b> explicitly acknowledges the information gathering and investigatory powers of resolution authorities.</p> <p><b>Section 2.1 of the FSA</b> further provides that a customer's regulator may audit Oracle as required by applicable law.</p> <p><b>Section 2.5 of the FSA</b>, which expressly states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law.</p>
D3/2018 2.2.11	Banks must ensure that their intellectual property rights and contractual rights to data are not compromised, despite any cloud computing and/or offshoring of data arrangements which may be in place.	7.7.13	Section 3.1 CSA  Section 3 Schedule C OMA	Customers retain ownership of their Content under the Oracle written cloud services contract, as described in <b>Section 3.1 of the CSA and Section 3 of Schedule C of the OMA</b> .
D3/2018 2.2.11	Data must always be in a usable, readable, and portable state, even when the contract is terminated.	N/A	Section 9.5 CSA  Section 9.1 DPA  Section 6.1	<p><b>Section 9.5 of the CSA</b> addresses availability of Content following the end of the Service Period.</p> <p><b>Section 9.1 of the DPA</b> confirms that, on termination of an arrangement, Oracle will promptly return or delete any remaining copies of personal information,</p>

			Oracle Cloud Hosting and Delivery Policies	except as otherwise stated in the Oracle Cloud services contract.  <b>Section 6.1 of the Oracle Cloud Hosting and Delivery Policies</b> 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.
D3/2018 2.2.12	Any cloud computing and/or offshoring of data arrangements must not impact on banks' ability to conduct forensic audits or investigations.	N/A	Sections 1 and 2 (2.1, 2.4, 2.5) FSA  Section 7 DPA	<b>Section 1 of the FSA</b> sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under <b>Section 7 of the DPA</b> .  <b>Section 2 of the FSA</b> sets out the customer's regulator's audit and access rights.  Additionally, Oracle will allow its banking customers and their regulatory authorities to audit Oracle records relating to invoices and payments for the services under the following circumstances: (i) to investigate or identify suspected fraud or material accounting mistakes; (ii) to fulfil any request by or comply with the requirements of any governmental or regulatory body (including Regulator) in the course of carrying out its regulatory functions; (iii) to verify the accuracy of the charges and any other amounts payable or receivable by the bank under an applicable agreement; and/or (iv) to verify Oracle's compliance with its obligations under an applicable agreement or any ordering document.
D3/2018 2.2.13	All cloud computing and/or offshoring of data arrangements must be contained in a documented, legally binding agreement.	7.6	CSA  Ordering Document	Oracle's written cloud services contract and Ordering Document specifies the rights and obligations of the parties relating to Oracle's cloud services.

### PA Guidance Note 5 of 2018 (Cloud Computing and Offshoring of Data) (G5/2018) and FSB Directive 159.A.i

TOPIC REF.	REGULATION REQUIREMENT/DESCRIPTION	FSB DIRECTIVE 159.A.I EQUIVALENT	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
G5/2018 4.1.1	Banks's data strategy/framework should include among other things where (in which jurisdictions) data may be stored (data residency).	N/A	Ordering Document Overview Section  Oracle Cloud Hosting and Delivery Policies	The Ordering Document or the cloud customer support portal states the data center region in which customer's content will be stored.  As indicated in the overview section of the Oracle Cloud Hosting and Delivery Policies, customer Content will be stored in the data center region applicable to such services.
G5/2018 4.3.2 (c)	The bank should develop and maintain operational and strategic oversight mechanisms which enable the ongoing assessment of performance against agreed service levels, the viability of the service and/or service provider, identification of a change in the relationship and a timely response to arising issues and emerging risks.	7.7.8 7.7.9	Section 3.2.2 Oracle Cloud Hosting and Delivery Policies Section 11  Schedule C OMA  Section 11 CSA  OCI Status: <a href="https://ocistatus.oraclecloud.com">https://ocistatus.oraclecloud.com</a>  Fusion Cloud Applications:	<b>Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies</b> states that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability.  <b>Section 11.1 of Schedule C of the OMA and Section 11.1 of the CSA</b> , as applicable, explains that Oracle also continuously monitors the Cloud services.  Oracle also offers multiple tools and services to support the monitoring obligations of its customers: <ul style="list-style-type: none"> <li>• OCI Status: <a href="https://ocistatus.oraclecloud.com/">https://ocistatus.oraclecloud.com/</a></li> <li>• Fusion Cloud Applications: <a href="https://saasstatus.oracle.com/">https://saasstatus.oracle.com/</a></li> </ul>

			<a href="https://saasstatus.oracle.com/">https://saasstatus.oracle.com/</a>	
G5/2018 4.3.2 (d)	Banks should manage services and service providers proactively by regularly receiving timely and sufficient information to enable effective oversight.	7.7.8 7.7.9	Section 3.2.2 Oracle Cloud Hosting and Delivery Policies	<b>Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies</b> indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability.  <b>See also Row above.</b>
G5/2018 4.3.2(e)	Oversight of service provider should include monitoring the alignment of the cloud computing and/or data offshoring service providers environmental requirements compared to those required by the bank. This includes performance, capacity security, resilience, and recoverability requirements.	7.7.8	Sections 2 and 3.4 Oracle Cloud Hosting and Delivery Policies  Section 5 FSA  Section 2 of the SaaS Cloud Services Pillar Document:  <a href="https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf">https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf</a>  Section 4 of the PaaS/IaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf">https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf</a>	<b>Section 3.4 of the Oracle Cloud Hosting and Delivery Policy</b> provides that Oracle uses a variety of software tools to monitor the availability and performance of the Oracle Cloud Services and the operation of infrastructure and network components.  <b>Section 5 of the FSA</b> indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Upon customer's request, Oracle will make available to the customer via web conference or on Oracle premises, in a guided manner, a summary of the Business Continuity Program (BCP) and applicable test information, material modifications to the BCP within the last 12 months and pertinent BCP governance areas, and confirmation that an internal review of these governance areas was performed within the last 12 months.  Additionally, please see the Oracle Cloud Service Continuity Policy in <b>Section 2 of the Oracle Cloud Hosting and Delivery Policies</b> .  <b>Section 4 of the PaaS/IaaS Cloud Services Pillar Document</b> and <b>Section 2 of the SaaS Cloud Services Pillar Document</b> also addresses cloud service continuity.
G5/2018 4.3.2 (f)	Responsibility for day-to-day operations and strategic management of the services should be clearly allocated.	7.7.2	CSA or OMA w/ Schedule C Ordering Document  Section 1 Oracle Cloud Hosting and Delivery Policies	Oracle's written cloud services contract and Ordering Document detail the parties' respective responsibilities under the agreement with respect to the cloud services.  <b>Section 1 of the Oracle Cloud Hosting and Delivery Policies</b> contains the Oracle Cloud Security Policy which describes Oracle's security practices.
G5/2018 4.4.1(c)	Services provided by third parties outside of the control of the bank should be covered in the assessment of the bank's audit universe and related assurances testing scheduled in order to assess all material aspects of the IT security control environment, both at the bank and at third parties, over time.	7.7.8	Section 1 FSA Section 3.4.2 Oracle Cloud Hosting and Delivery Policies  Oracle Cloud Compliance Site: <a href="https://www.oracle.com/corporate/cloud-compliance/">https://www.oracle.com/corporate/cloud-compliance/</a>	<b>Section 1 of the FSA</b> sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under <b>Section 7 of the DPA</b> .  <b>Section 3.4.2 of the Oracle Cloud Hosting and Delivery Policies</b> allows customers to conduct certain functional testing for Oracle Cloud services in their test environment..  Oracle provides information regarding compliance frameworks for which its lines of business have achieved applicable third-party attestations or certifications. These attestations provide independent assessment of the security, privacy, and compliance controls of the applicable Oracle Cloud services and can assist with compliance and reporting.
G5/2018 4.5.1(g)	Responsibility should be assigned for managing risks identified in the cloud	7.7.4	CSA or OMA w/ Schedule C	Oracle written cloud services contract and the Ordering Document describes the parties' respective responsibilities with respect to the cloud services.



	computing and/or the offshoring data initiative.		<p>Section 2 DPA</p> <p>Oracle Corporate Security Practices Site:  <a href="https://www.oracle.com/corporate/security-practices/">https://www.oracle.com/corporate/security-practices/</a></p> <p>Oracle Cloud Compliance Site:  <a href="https://www.oracle.com/cloud/compliance/">https://www.oracle.com/cloud/compliance/</a></p>	<p><b>Section 2 of the DPA</b> describes the responsibilities of Oracle and the customer with respect to the processing of personal information and the bank's instructions.</p> <p>Additionally, Oracle provides a number of resources to assist its customers in conducting the necessary risk assessments and due diligence. Oracle provides customers with access to security questionnaires (CAIQ), audit reports and other information regarding Oracle's operational and security practices.</p>
G5/2018 4.5.3	The impact of using different jurisdictions should be considered in light of the bank's data strategy as well as the potential impact on the role of the supervisor and its access to data.	N/A	<p>Ordering Document</p> <p>Sections 1 and 2 FSA</p>	<p><b>The Ordering Document or the cloud customer support portal</b> states the data center region applicable to ordered Cloud services.</p> <p><b>Section 1 of the FSA</b> sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under <b>Section 7 of the DPA</b>.</p> <p><b>Section 2 of the FSA</b> sets out the customer's regulator's audit and access rights.</p>
G5/2018 4.7.4 (a)	With respect to information security, banks should obtain assurance from third parties involved and contractually agree that third parties will adhere to the information security requirements defined by the bank. The information security requirements should, deal with patch management, authentication, authorization, and administration.		<p>Sections 1 and 4 Oracle Cloud Hosting and Delivery Policies</p> <p>Oracle Corporate Security Practices:  <a href="https://www.oracle.com/corporate/security-practices/">oracle.com/corporate/security-practices/</a></p> <p><a href="#">Section 4 DPA</a></p>	<p><b>Section 1 of the Oracle Cloud Hosting and Delivery Policies</b> contains the Oracle Cloud Security Policy which describes Oracle's Cloud security practices. <b>Section 4 of the Hosting and Delivery Policies</b> also describe Oracle's practices regarding change/patch management and access controls (<b>Sections 1.3, 1.4</b>).</p> <p><b>Section 4 of the DPA</b> states that to the extent Oracle engages third party subprocessors and/or Oracle affiliates to process personal information, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Services Agreement.</p>
G5/2018 4.7.4 (b)	Banks should agree [to] data loss and breach processes with any third party involved, and ensure they are aligned with the bank's risk appetite and legal as well as regulatory obligations.	7.7.4	<p>Section 8 DPA</p> <p>Section 2 Oracle Cloud Hosting and Delivery Policies</p> <p>SaaS Cloud Services Pillar Document:  <a href="https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf">https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf</a></p> <p>PaaS/IaaS Cloud Services Pillar Document:  <a href="https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf">https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf</a></p>	<p><b>Section 8 of the DPA</b> sets out Oracle's incident management and breach notification obligations.</p> <p><b>Section 2 of the Oracle Cloud Hosting and Delivery Policies</b> sets out Oracle Cloud Service Continuity Policy, which describes Oracle Cloud Services High Availability Strategy and Oracle Cloud Services Backup Strategy, as well as the <b>PaaS/IaaS Cloud Services Pillar Document</b> or the <b>SaaS Cloud Services Pillar Document</b>, as applicable.</p>
G5/2018 4.7.4 (c)	Contractual agreements should clearly define accountability and penalties in cases where controls are breached, including who would be responsible for losses resulting from a data breach.		<p>Section 7 CSA  Section 7 Schedule C OMA</p>	<p><b>Section 7 of the CSA and Section 7 of Schedule C of the OMA</b>, which sets forth the limitation of liabilities.</p>

<p>G5/2018 4.7.5 (a)</p>	<p>The contractual agreement with any third party involved should specify how the bank will verify adherence to the agreed information security requirements. This may include third-party assurance audits, as well as any other security testing requirements such as vulnerability scanning and penetration testing.</p>	<p>N/A</p>	<p>Section 3.4.2 Oracle Cloud Hosting and Delivery Policies</p>	<p><b>Section 1 of the FSA</b> sets out customer’s audit and access rights and supplements the audit and inspection rights granted to customers under <b>Section 7 of the DPA</b>.</p> <p><b>Section 2 of the FSA</b> sets out the customer’s regulator’s audit and access rights.</p> <p><b>Section 3.4.2 of the Oracle Cloud Hosting and Delivery Policies</b> allows customers to conduct certain functional testing for Oracle Cloud services in their test environment.</p> <p>Oracle conducts penetration tests of the Oracle OCI and SaaS systems at least annually. A commercial vulnerability scanning tool scans external IP addresses and internal nodes monthly. Identified exploitable threats and vulnerabilities are investigated and tracked to resolution. In addition, Oracle completes third-party vulnerability scans/penetration tests annually for applicable services. The summary reports are available upon request for entities that have signed a non-disclosure agreement with Oracle.</p>
<p>G5/2018 4.7.5(b)</p>	<p>Banks should obtain a copy of the information security policy of any third parties involved in order to determine whether it contains adequate provisions for security standards and controls which would be in line with the bank’s service level agreement (SLA) with the third party.</p>		<p>Section 3 Oracle Cloud Hosting and Delivery Policies</p> <p>Oracle Corporate Security Practices: <a href="https://www.oracle.com/corporate/security-practices/">https://www.oracle.com/corporate/security-practices/</a></p>	<p>Included in Oracle’s Corporate Security Program are security policies to protect the covered entity’s information systems and the non-public information stored on those information systems, from unauthorized access, use or other malicious acts.</p> <p><b>Section 3 of the Oracle Cloud Hosting and Delivery Policies</b> describes Oracle’s use of a variety of software tools to monitor the availability and performance of the Oracle Cloud Services and the operation of infrastructure and network components.</p>
<p>G5/2018 4.7.6(a)</p>	<p>Banks should be aware of whether a third party is certified or audited in terms of any of information security technology, control frameworks or standards and should obtain assurances through obtaining copies of audit/assurance reports on adherence.</p>	<p>7.7.7</p>	<p>Oracle Compliance Site: <a href="https://www.oracle.com/cloud/compliance/">https://www.oracle.com/cloud/compliance/</a></p>	<p>Oracle also provides information about frameworks for which an Oracle LOB has achieved a third-party attestation or certification on its compliance site.</p>
<p>G5/2018 4.7.6 (b)</p>	<p>Banks should consider leading standards and control frameworks, including National Institute of Standards and Technology (NIST), the Cloud Security Alliance (CSA) and the Information Systems Audit and Control Association (ISACA).</p>		<p>Oracle Cloud Compliance Site: <a href="https://www.oracle.com/cloud/compliance/">https://www.oracle.com/cloud/compliance/</a></p> <p>OCI CAIQ: <a href="https://www.oracle.com/a/ocom/docs/oci-corporate-caiq.pdf">oracle.com/a/ocom/docs/oci-corporate-caiq.pdf</a></p> <p>Oracle Fusion Cloud Applications: <a href="https://www.oracle.com/a/ocom/docs/caiq-oracle-fusion-cloud-applications.pdf">oracle.com/a/ocom/docs/caiq-oracle-fusion-cloud-applications.pdf</a></p> <p>Oracle Enterprise Performance Management Cloud Applications: <a href="https://www.oracle.com/a/ocom/docs/caiq-oracle-epm-caiq.pdf">oracle.com/a/ocom/docs/caiq-oracle-</a></p>	<p>Oracle provides a number of resources to assist its customers in conducting the necessary risk assessments and due diligence. Oracle provides customers with access to security questionnaires (CAIQ), audit reports and other information regarding Oracle’s operational and security practices.</p>

			<p><a href="#">epm-cloud-applications.pdf</a></p> <p>Oracle Cloud Applications: <a href="#">oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf</a></p>	
G5/2018 4.7.6(c)	Agreed security requirements should include physical security standards at the third party's data centres which should not be less stringent than the physical security measure that would have been in place had the data been hosted by the bank's own data centres.		<p>Sections 1. 3.1 and 3.2 Oracle Cloud Hosting and Delivery Policies</p> <p>Sections 6 and 8 DPA</p> <p>SaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf">https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf</a></p> <p>PaaS/IaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf">https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf</a></p> <p>Oracle Corporate Security Practices: <a href="https://www.oracle.com/corporate/security-practices/corporate-physical-environmental.html">https://www.oracle.com/corporate/security-practices/corporate-physical-environmental.html</a></p>	<p><b>Section 1 of the Oracle Cloud Hosting and Delivery Policies</b> describes <b>Oracle's Cloud security practices, particularly Section 1.2 of the Oracle Cloud Hosting and Delivery Policies</b>, which describes Oracle's Physical Security Safeguards.</p> <p>The Oracle Cloud services contract addresses the accessibility, availability, integrity, privacy and safety of customer's content as follows:</p> <p><b>Technical and organization security measures:</b></p> <p><b>Section 6 – Security and Confidentiality – of the Oracle Data Processing Agreement, the Oracle Cloud Hosting and Delivery Policies</b>, as well as the <b>PaaS/IaaS Cloud Services Pillar Document</b> or the <b>SaaS Cloud Pillar Document</b>, as applicable.</p> <p>Oracle cloud service data centers are designed to help protect the security and availability of customer data.</p> <p>Oracle cloud service data centers 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. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.</p>
G5/2018 4.7.7 (a)	Access rights to information in the cloud or offshored data should be restricted in line with the bank's user access management policies which, for instance, include administrator access to operating systems as well as databases.	N/A	<p>Section 1 Oracle Cloud Hosting and Delivery Policies</p> <p>Oracle Corporate Security Practices: <a href="https://www.oracle.com/corporate/security-practices/corporate-access-control.html">https://www.oracle.com/corporate/security-practices/corporate-access-control.html</a></p>	<p><b>Section 1 of the Oracle Cloud Hosting and Delivery Policies</b> describes Oracle's security practices. <b>Section 1.3 of the Oracle Cloud Hosting and Delivery Policies</b> in particular sets out Oracle's system access controls and authentication processes.</p> <p><b>Section 1.4 of the Oracle Cloud Hosting and Delivery Policies</b> describes Oracle's access controls for personnel with access to the Cloud Services environment. Oracle enforces Role Based Access Controls (RBAC) and employs the following access management principles:</p> <ul style="list-style-type: none"> <li>• Need to know</li> <li>• Least privilege</li> <li>• Segregation of duties.</li> </ul> <p><b>Oracle Corporate Security Practices</b></p>
G5/2018 4.7.7 (b)	Third parties involved in either cloud computing and/or data offshoring arrangements should develop and implement adequate user access privilege controls in order to restrict access to the bank's data, systems and infrastructures. This should be done on a least-privilege basis.	N/A	<p>Section 1.4 Oracle Cloud Hosting and Delivery Policies</p>	<p><b>Section 1.4 of the Oracle Cloud Hosting and Delivery Policies</b> describes Oracle's access controls for personnel with access to the Cloud Services environment. Oracle enforces Role Based Access Controls (RBAC) and employs the following access management principles:</p> <ul style="list-style-type: none"> <li>• Need to know</li> <li>• Least privilege</li> </ul>

				<ul style="list-style-type: none"> <li>Segregation of duties.</li> </ul>
G5/2018 4.7.8 (a)	Banks should determine the level of encryption required in line with the classification of the data involved in the cloud computing. [T]he deployment model followed is also relevan[t] in determining the appropriate level of encryption. The deployment model followed determines the appropriate level of encryption and subsequent encryption should be commensurate with the materiality of the data and risks involved.	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies	<p><b>Section 1 of the Oracle Cloud Hosting and Delivery Policies</b> contains the Oracle Cloud Security Policy which describes Oracle's security practices.</p> <p><b>Section 1.5 of the Oracle Cloud Hosting and Delivery Policies</b> in particular sets out Oracle's use of encryption technology.</p>
G5/2018 4.7.8 (b)	Banks should use different classifications, but for any personal, private or confidential data in a multitenant and/or community/public cloud environment, banks should consider encrypting data in transit as well as in storage.	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies	<p><b>Section 1 of the Oracle Cloud Hosting and Delivery Policies</b> contains the Oracle Cloud Security Policy which describes Oracle's security practices.</p> <p><b>Section 1.5 of the Oracle Cloud Hosting and Delivery Policies</b> in particular sets out Oracle's use of encryption technology.</p>
G5/2018 4.7.8 (c)	Where encryption is required, data should [be] encrypted before it is moved to the cloud and/or offshored, and the same level of encryption services should be used for data at rest and in motion.	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies	<p>Encryption of customer content prior to being moved to the cloud is the customer's responsibility.</p> <p><b>Section 1 of the Oracle Cloud Hosting and Delivery Policies</b> contains the Oracle Cloud Security Policy which describes Oracle's security practices.</p> <p><b>Section 1.5 of the Oracle Cloud Hosting and Delivery Policies</b> in particular sets out Oracle's use of encryption technology.</p>
G5/2018 4.7.8 (d)	Access to encryption keys should be restricted in line with the bank's key management policies and procedures. Where third parties are involved, key management should be subjected to the same level of control outlined in the bank's policies and procedures.	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies  Ordering Document	<p><b>Section 1 of the Oracle Cloud Hosting and Delivery Policies</b> contains the Oracle Cloud Security Policy which describes Oracle's security practices.</p> <p><b>Section 1.5 of the Oracle Cloud Hosting and Delivery Policies</b> in particular sets out Oracle's use of encryption technology.</p> <p>Customers have the ability to generate and hold encryption keys for certain Oracle Cloud Services provided under an applicable Ordering Document.</p>
G5/2018 4.7.8 (f)	Where third parties are used, they should inform the bank of changes within their cryptosystems.	N/A	Oracle Corporate Security Practices:  <a href="https://oracle.com/corporate/security-practices/">oracle.com/corporate/security-practices/</a>  Updates to Cloud Services Policies:  <a href="https://go.oracle.com/LP=82034!">https://go.oracle.com/LP=82034!</a>	Oracle notifies customers of changes to its Security Practices and other applicable policies via Oracle's notification process, where feasible, under which customers may register to receive notifications of such changes.
G5/2018	The contractual agreement with any third party involved in cloud computing	N/A	Section 8 DPA	<b>Section 8 of the DPA</b> sets out Oracle's incident management and breach notification obligations.

4.7.9 (a)	and data offshoring should refer to the incident management process between the parties and set out the roles and responsibilities of the respective parties.			
G5/2018 4.7.9 (b)	The incident management process should include incident notifications, responses, remediation, documentation, timelines, addressing the risk of the incident, escalation and formally closing incidents.	N/A	Section 8 DPA	<b>Section 8 of the DPA</b> sets out Oracle's incident management and breach notification obligations. Oracle provides notification within 24 hours of a confirmed Personal Information Breach as specified in <b>DPA, Section 8.2.</b>
G5/2018 4.7.9 (c)	The contractual agreement with the third party should define the types of incidents (for instance data breaches and security violations), events and the actions to be initiated after each incident.	N/A	Section 8 DPA	<b>Section 8 of the DPA</b> sets out Oracle's incident management and breach notification obligations.
G5/2018 4.7.9 (d)	Banks should be informed when their data may have been seized or accessed by a foreign country, even if it is through appropriate legal processes in that country.	N/A	Section 10 DPA	<b>Section 10 of the DPA.</b> Oracle will promptly inform customers of requests to provide access to Personal Information, unless otherwise required by law.
G5/2018 4.7.10 (b)	As part of defining and agreeing on security standards, the security configuration baseline to prevent cross-contamination with other customer environments should be considered.	N/A	Section 1.7 Oracle Cloud Hosting and Delivery Policies	<b>Section 1.7 of the Oracle Cloud Hosting and Delivery Policies</b> describes the logical and physical segregation of Oracle's content from the content of other customers hosted in the Oracle Cloud Services environments.
G5/2018 4.7.11 (b)	As part of defining and agreeing on security standards, the security configuration baseline to harden virtualised operating systems should be defined, where applicable.	N/A	Oracle Security Practices site: <a href="https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html">https://www.oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html</a>	Oracle's information-asset classification determines corporate data-security requirements for Oracle-managed systems. Oracle policies and standards provide global guidance for appropriate controls designed to protect the confidentiality, integrity, and availability of corporate data in accordance with the data classification. Required mechanisms are designed to be commensurate with the nature of the corporate data being protected.
G5/2018 4.7.11 (c)	The agreed security standards should further address hypervisor vulnerability management, patch management and release management – specifically when new vulnerabilities are discovered.	N/A	Oracle Corporate Security Practices, Critical Patch Update Program: <a href="https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html">https://www.oracle.com/corporate/security-practices/assurance/vulnerability/security-fixing.html</a>  !	Oracle Lines of Businesses review security bulletins and perform periodic vulnerability scans and apply the required patches, as needed. Additionally, commercial vulnerability scanning tools are used to scan external IP addresses and internal nodes monthly.  Also, Oracle completes third-party vulnerability scans/penetration tests annually for applicable services. The summary reports are available upon request for entities that have signed a non-disclosure agreement with Oracle.

G5/2018 4.8.3 (a)	The terms of contractual agreement should allow a bank to modify the manner in which the cloud computing and/or data offshoring activities are performed, specifically where banks may need to amend processes to meet compliance requirements.	N/A	Section 3.1 FSA	<b>Section 3.1 of the FSA</b> provides a process for the parties to address modifications needed to meet regulatory requirements.
G5/2018 4.8.3(b)	Where a bank makes use of a third party in the use of cloud computing and/or data offshoring, the bank should ensure that it contractually agrees on the compliance requirements with the service provider to ensure ongoing compliance with laws and regulations where the data shall be hosted.	7.7.5	Section 8 FSA	<b>Section 8 of the FSA</b> imposes obligations on both parties related to compliance with applicable laws.
G5/2018 4.9.1	Contractual arrangements must be in place to ensure access to data to all relevant parties, including the bank's regulatory authorities such as the relevant departments of the SARB, the Financial Sector Conduct Authority (FSCA) and the Financial Intelligence Centre (FIC).	7.7.10 7.7.15	Sections 1 and 2 FSA	<b>Section 1 of the FSA</b> , which grants audit rights to customer and <b>Section 2 of the FSA</b> , which grants similar audit rights to customer's regulators.
G5/2018 4.9.2(a)	The contractual agreement should include the right of supervisory institutions to access information, which included conducting on-site visits at the service provider's facilities, where considered necessary.	7.7.15	Section 2 FSA	<b>Section 2 of the FSA</b> , which grants customer's regulators a right of audit and access for on-site visits.
G5/2018 4.9.2(c)	The contractual agreement should provide for the mutual exchange of information (potentially through the right transparency clause) and, by request, the provision of relevant information to the bank's supervisors. Where a bank is unable to present data to its supervisor upon request, for any reason whatsoever, the PA may request the termination of the relationship with the service provider and take further steps as deemed necessary.	7.7.15	Section 2 FSA Section 3.1 FSA Section 7 DPA	<b>Section 2</b> and <b>Section 3 of the FSA</b> . Additionally, <b>Section 7 of the DPA</b> describes Oracle's customers' audit rights.
G5/2018 4.9.2(d)	Banks should ensure that data is not stored in jurisdictions that may inhibit effective access to data for South African supervisors.	N/A	Ordering Document  OCI Regions site: <a href="https://www.oracle.com/cloud/cloud-regions/">https://www.oracle.com/cloud/cloud-regions/</a>	Oracle operates within various regions across the globe. Each region is composed of one or more physically isolated and fault-tolerant data centers (also named availability domains), including a data center located in the Oracle Cloud Johannesburg Region.  When customers set up their Oracle account, they choose a data region in which to initially locate their tenancy and their content is hosted within that region unless customers choose to move their content outside of the region.  The Ordering Document or the Oracle Cloud Console states the data center region in which customer's content will be stored.

G5/2018 4.9.3 (a)	The contractual agreement with the third party should contain a right to audit clause which clearly defined and satisfies the assurance requirements of the bank's board, audit charter, external auditors and any regulators that have jurisdiction over the bank.	7.7.15	Section 1 and 2 FSA	<p><b>Section 1 of the FSA</b> sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under <b>Section 7 of the DPA</b>.</p> <p><b>Section 2 of the FSA</b> sets out the customer's regulator's audit and access rights.</p>
G5/2018 4.9.3 (b)	The right to audit clause is listed for inclusion in outsourcing contracts.	7.7.15	Section 1 and 2 FSA	<p><b>Section 1 of the FSA</b> sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under <b>Section 7 of the DPA</b>.</p> <p><b>Section 2 of the FSA</b> sets out the customer's regulator's audit and access rights.</p>
G5/2018 4.10.1(a)	Before entering into a contract with a third party, banks should assess whether third party has sufficient capacity to effectively manage on a continuous basis, such as considering the potential increased services that third party may have to provide in the foreseeable future including the relevant metrics for capacity, such as storage capacity, bandwidth requirements, increased number of users, and transactions per second requirements.	N/A	<p>OCI Program Documentation: <a href="https://docs.oracle.com/en-us/iaas/Content/home.htm">https://docs.oracle.com/en-us/iaas/Content/home.htm</a></p> <p>Oracle Fusion Cloud Applications Suite Documentation: <a href="https://docs.oracle.com/en/cloud/saas/">https://docs.oracle.com/en/cloud/saas/</a></p> <p>Investor Relations: <a href="https://investor.oracle.com/financials/default.aspx">https://investor.oracle.com/financials/default.aspx</a></p>	<p>Oracle provides products and services that address enterprise information technology (IT) environments. These include applications and infrastructure offerings that are delivered worldwide through various flexible and interoperable IT deployment models. Customers can find technical information, user guides and detailed information on the features and functionality of OCI and SaaS services in the applicable Program Documentation:</p> <p>Oracle's customers include businesses of many sizes, government agencies, educational institutions, and resellers. Oracle markets and sells to customers directly through its worldwide sales force and indirectly through the Oracle Partner Network. Using Oracle technologies, our customers build, deploy, run, manage, and support their internal and external products, services, and business operations. Information about Oracle's business operations and organization structure is available on Oracle's website <a href="http://oracle.com/corporate">oracle.com/corporate</a> and in its annual reports. As of fiscal year 2021, Oracle had \$40 billion total GAAP revenue and 133,000 employees serving 430,000 customers in 175 countries.</p>
G5/2018 4.10.1(b)	Before entering into a third-party contract, banks should consider whether the information communications infrastructure between the bank and the third party is sufficient to manage the current and future requirements on a continual basis.	N/A	Section 1.5 Oracle Cloud Hosting and Delivery Policies	<b>Section 1.5 of the Oracle Cloud Hosting and Delivery Policies</b> explains that customer access to Oracle Cloud Services is through a secure communication protocol provided by Oracle.
G5/2018 4.10.2(c)	Business continuity requirements, such as recovery time and recovery objectives (RTOs and RPOs), should be identified through a business impact assessment, documented and, where third parties are involved, agreed with third parties.	N/A	<p>Section 5 FSA</p> <p>Section 2 Oracle Cloud Hosting and Delivery Policies</p> <p>Section 2.2 SaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf">https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf</a></p> <p>Section 2 PaaS/IaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/paas-">https://www.oracle.com/assets/paas-</a></p>	<p><b>Section 5 of the FSA</b> indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services.</p> <p>Additionally, please see the Oracle Cloud Service Continuity Policy in <b>Section 2 of the Oracle Cloud Hosting and Delivery Policies</b>.</p> <p><b>Section 2.2 of the SaaS Cloud Pillar Document</b> describes the Recovery Time Objectives and the Recovery Point Objectives relating to Oracle Cloud services.</p> <p><b>Section 2 of the PaaS/IaaS Cloud Services Pillar Document</b> addresses recovery related to Oracle Cloud services.</p>

			<a href="#">iaas-pub-cld-srvs-pillar-4021422.pdf</a>	
G5/2018 4.10.2(d)	Disaster recovery and business continuity plans should be developed to maintain continuity of the bank's operations, including matters related to the recovery from an incident, plans for communicating incidents, and the frequency of testing the adequacy and effectiveness of these plans.	7.7.14	Section 5 FSA  Section 2 Oracle Cloud Hosting and Delivery Policies	<b>Section 5 of the FSA</b> indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services.  Additionally, <b>Section 2 of the Oracle Cloud Hosting and Delivery Policies</b> describes Oracle's computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services and Oracle cloud services backup strategy.
G5/2018 4.10.2(e)	Resilience should be designed/built into the bank's cloud computing and/or data offshoring arrangements.	N/A	Section 5 FSA  Section 2 Oracle Cloud Hosting and Delivery Policies	<b>Section 5 of the FSA</b> indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services.  Additionally, Section 2 of the Oracle Cloud Hosting and Delivery Policies describes Oracle's computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services and Oracle cloud services backup strategy.
G5/2018 4.10.2(g)	Banks should have access to the audit or assurance reports of the third party's business continuity program, including disaster recovery testing, process audits and control audits at least for activities/functions managed on their behalf.	7.7.14	Sections 1.9 and 5 FSA	<b>Section 5 of the FSA</b> indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Upon customer's request, Oracle will make available to the customer via web conference or on Oracle premises, in a guided manner, a summary of the Business Continuity Program (BCP) and applicable test information, material modifications to the BCP within the last 12 months and pertinent BCP governance areas, and confirmation that an internal review of these governance areas was performed within the last 12 months.
G5/2018 4.10.2(h)	The third party's business continuity program should ideally be certified or mapped to internationally recognized standards such as ISO 22301 (business continuity management systems).	N/A	Section 5 FSA	<b>Section 5 of the FSA</b> indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services.  Oracle's business continuity program is aligned to ISO 22301.
G5/2018 4.10.2(i)	The roles and responsibilities of the bank and any third party in the event of disruption should be clearly defined in the contractual arrangements.	N/A	Section 5 FSA  Section 2 Oracle Cloud Hosting and Delivery Policies	<b>Section 5 of the FSA</b> indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services.  Additionally, please see the Oracle Cloud Service Continuity Policy in <b>Section 2 of the Oracle Cloud Hosting and Delivery Policies</b> , which explains that for Oracle Cloud Services which enable customers to configure backups in accordance with their own policies, customers are responsible for performing backups and restores of their data, non-Oracle software, and any Oracle software that is not provided by Oracle as part of their services under the Ordering Document. Additionally, customers are encouraged to develop a business continuity plan to ensure continuity of their own operations in the event of a disaster.
G5/2018 4.10.2(k)	Contingency plans pertaining to outsourced activities should be	N/A	SaaS Cloud Services Pillar Document:	<b>OCI: Section 2 of the Oracle PaaS and IaaS Public Cloud Services Pillar Document</b> states that customers may



	reviewed regularly, but not less than once a year.		<a href="https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf">https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf</a>  PaaS/IaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf">https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf</a>	<p>be able to configure their ordered OCI services with disaster recovery capabilities. For any such postprovisioning configuration customers are responsible for designing and implementing a cloud architecture that meets their own requirements for availability, business continuity and disaster recovery. Customers are also responsible for designing, developing and implementing procedures for recovering their applications in accordance with their own recovery plans and periodically testing such plans to help meet availability commitments and requirements of their customers.</p> <p><b>SaaS:</b></p> <p><b>Section 2 of the Oracle SaaS Public Cloud Services Pillar Document</b> sets out disaster recovery services practices for SaaS public cloud services, which are intended to provide service restoration capability in the event of a major disaster, as declared by Oracle.</p>
G5/2018 4.11.1(a)	Banks should document the hardware, software and procedural requirements for moving from an existing service provider to another service provider or in-house.	N/A	Section 4.3 FSA	<b>Section 4.3 of the FSA</b> addresses customers who require assistance with a transition.
G5/2018 4.11.1(b)	Banks need to ensure that an exit from a cloud computing and/or offshoring of data arrangement does not affect their compliance with any legislative requirement.	N/A	Section 9 CSA Schedule C OMA  Section 6.1 Oracle Cloud Hosting and Delivery Policies  Section 3 and 4 FSA  Section 9.1 DPA	<p>Customers' termination rights are set out in <b>Section 9 of the CSA or Section 9 of the OMA Schedule C (as applicable) and in Section 3 of the FSA.</b></p> <p><b>Section 6.1 of the Oracle Cloud Hosting and Delivery Policies</b> states Oracle will make content available in a structured, machine-readable format for retrieval by the customer for a specified period posttermination (retrieval period). Upon expiry of the retrieval period, Oracle will delete the content from the services unless otherwise required by applicable law.</p> <p><b>Section 4.3 of the FSA</b> addresses customers who require assistance with a transition.</p> <p><b>Section 9.1 of the DPA</b> confirms that, on termination of an arrangement, Oracle will promptly return or delete any remaining copies of personal data, except as otherwise stated in the Oracle Cloud services contract.</p>
G5/2018 4.11.2(b)	The contractual agreement should stipulate the roles and responsibilities for both parties at the termination of the agreement, including the circumstances when a bank enters into a SARB resolution.	N/A	Section 9 CSA Schedule C OMA  Section 6.1 Oracle Cloud Hosting and Delivery Policies  Section 3 and 4 FSA  Section 9.1 DPA	<p>Customers' termination rights are set out in <b>Section 9 of the CSA or Section 9 of the OMA Schedule C (as applicable) and in Section 3 of the FSA.</b></p> <p><b>Section 6.1 of the Oracle Cloud Hosting and Delivery Policies</b> states Oracle will make content available in a structured, machine-readable format for retrieval by the customer for a specified period posttermination (retrieval period). Upon expiry of the retrieval period, Oracle will delete the content from the services unless otherwise required by applicable law.</p> <p><b>Section 4.3 of the FSA</b> addresses customers who require assistance with a transition.</p> <p><b>Section 9.1 of the DPA</b> confirms that, on termination of an arrangement, Oracle will promptly return or delete any remaining copies of personal data, except as otherwise stated in the Oracle Cloud services contract.</p>

G5/2018 4.11.2 (c)	The contractual agreement should define the manner in which the agreement is to be terminated as well as the guarantees provided to enable the bank to resume performance of the outsourced and/or offshored activities or to transfer those activities to another service provider upon termination of the agreement.	7.7.16 7.7.20	Section 9 CSA Schedule C OMA  Section 6.1 Oracle Cloud Hosting and Delivery Policies  Section 3 and 4 FSA  Section 9.1 DPA	<p>Customers' termination rights are set out in <b>Section 9 of the CSA or Section 9 of the OMA Schedule C (as applicable) and in Section 3 of the FSA.</b></p> <p><b>Section 6.1 of the Oracle Cloud Hosting and Delivery Policies</b> 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.</p> <p><b>Section 4.3 of the FSA</b> addresses customers who require assistance with a transition.</p> <p><b>Section 9.1 of the DPA</b> confirms that, on termination of an arrangement, Oracle will promptly return or delete any remaining copies of personal data, except as otherwise stated in the Oracle Cloud services contract.</p>
G5/2018 4.11.2(d)	The contractual agreement should include a clause to the effect that, upon the termination of the contract, a bank's data be promptly and completely removed and returned to the bank, transferred to another service provider or destroyed, depending on the nature of the data involved. The contractual arrangements should include sufficient assurance once its data has been removed, transferred or destroyed at the termination of the agreement.	N/A	Section 9.5 CSA  Section 9.1 DPA  Section 4.1 FSA  Section 6.1 Oracle Cloud Hosting and Delivery Policies	<p><b>Section 9.5 of the CSA</b> states that at the end of such retrieval period, and except as may be required by law, Oracle will delete or otherwise render unrecoverable any of customer's content that remains in the cloud services environment. Oracle's data deletion practices are described in more detail in the Service Specifications.</p> <p><b>Section 9.1 of the DPA</b> confirms that, on termination of an arrangement, Oracle will promptly return or delete any remaining copies of personal data, except as otherwise stated in the Oracle Cloud services contract.</p> <p><b>Section 4.1 of the FSA</b> addresses customer's right to retrieve its Content at the end of the cloud services period or upon termination of the agreement along with the assistance Oracle will provide to customer in this situation.</p> <p><b>Section 6.1 of the Oracle Cloud Hosting and Delivery Policies</b> 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.</p>
G5/2018 4.11.3(a)	Any cloud computing and/or data offshoring services should be organized in such a way that they do not become a barrier to the resolution or orderly wind-down of a bank or create additional complexity in a resolution.	N/A	Section 4 FSA	<b>See Section 4 of the FSA</b> for terms that address the orderly wind-down of the contract and assistance that Oracle can provide in the event of expiration or termination of the contract.
G5/2018 4.11.3(c)	The contractual agreement for a cloud computing and/or data offshoring arrangement, specifically any default clause, may not entitle the service provider to unilaterally cancel the agreement in the event that a recovery or resolution action is taken.	N/A	Section 9 FSA	<b>Section 9 of the FSA</b> addresses the parties' rights and responsibilities in the event of a Resolution Event, including suspension of Oracle's termination rights and obligation to continue provision of the cloud services during the standstill period.
G5/2018 4.11.4(c)	The bank should have contingency plans in place to continue with its operations in case of an unforeseen event, irrespective of whether a cloud	7.7.14	Section 5 FSA	<b>Section 5 of the FSA</b> indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services.

	environment had been deployed. The bank's risk management processes should determine the level and extent of contingency plans to be instituted. The operational requirements can be addressed on a case-by-case basis given the existing circumstances.			
G5/2018 4.12.1(b)	Data produced for regulatory reporting purposes should be reconcilable with source data and banks should be able to prove that the integrity of such data has been preserved, which includes data reported to all regulated authorities.	N/A	<p>Sections 6 and 8 DPA</p> <p>Sections 4 and 5 Schedule C OMA</p> <p>Section 4 and 5 CSA</p> <p>Oracle Cloud Hosting and Delivery Policies (particularly Sections 1, 3.1 and 3.2)</p> <p>SaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf">https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf</a></p> <p>PaaS/IaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf">https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf</a></p> <p>Oracle Corporate Security Practices: <a href="https://www.oracle.com/corporate/security-practices/">oracle.com/corporate/security-practices/</a></p>	<p>Although it is the customer's responsibility to ensure that the integrity of their data is preserved, Oracle's policies and standards are designed to ensure confidentiality and file integrity management.</p> <p><b>Section 1 of the Oracle Cloud Hosting and Delivery Policies</b> describes Oracle's Cloud security practices.</p> <p><b>Section 1.2 of the Oracle Cloud Hosting and Delivery Policies</b> describes Oracle's Physical Security Safeguards.</p> <p>The Oracle Cloud services contract addresses the accessibility, availability, integrity, privacy and safety of customer's content as follows:</p> <p><b>Technical and organization security measures:</b></p> <ul style="list-style-type: none"> <li>- <b>Section 6 – Security and Confidentiality – of the Oracle Data Processing Agreement</b></li> <li>- the <b>Oracle Cloud Hosting and Delivery Policies</b> as well as the <b>PaaS/IaaS Cloud Services Pillar Document</b> or the <b>SaaS Cloud Pillar Document</b>, as applicable.</li> <li>- <b>Oracle Corporate Security Practices</b></li> </ul> <p><b>Confidentiality and Protection of "Your Content":</b></p> <p><b>Section 4 of Schedule C of the OMA</b> and <b>Section 4 of the CSA</b> references Oracle's obligation to protect the confidentiality of Customer Content for as long as it resides in the Services.</p> <p><b>Section 5 of Schedule C</b> and <b>Section 5 of the CSA</b>, as applicable.</p> <p><b>Section 8 of the DPA</b> sets out Oracle's incident management and breach notification obligations.</p>
G5/2018 4.12.2(a)	The contractual agreement with the third parties responsible for cloud computing and/or the offshoring of data must clearly prescribe the access that the bank, regulatory authorities and law enforcement agencies would have in order to conduct forensic audits and investigations.	7.7.14	<p>Sections 1 and 2 FSA</p>	<p><b>Section 1 of the FSA</b> sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under <b>Section 7 of the DPA</b>.</p> <p><b>Section 2 of the FSA</b> sets out the customer's regulator's audit and access rights.</p>
G5/2018 4.12.2(b)	The contractual agreement should prescribe the manner in which forensic evidence is made available to the bank as well as the controls in place as proof that such evidence has not been tampered with.	N/A	<p>Section 1 and 2 FSA</p> <p>Section 7 DPA</p>	<p><b>Section 1 of the FSA</b> sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under <b>Section 7 of the DPA</b>.</p> <p><b>Section 2 of the FSA</b> sets out the customer's regulator's audit and access rights.</p> <p>Additionally, Oracle will allow its banking customers and their regulatory authorities to audit Oracle records relating to invoices and payments for the</p>

				services under the following circumstances : (i) to investigate or identify suspected fraud or material accounting mistakes; (ii) to fulfil any request by or comply with the requirements of any governmental or regulatory body (including Regulator) in the course of carrying out its regulatory functions; (iii) to verify the accuracy of the charges and any other amounts payable or receivable by the bank under an applicable agreement; and/or (iv) to verify Oracle's compliance with its obligations under an applicable agreement or any ordering document.
G5/2018 4.12.2(c)	The contractual agreement should define the roles and responsibilities for both parties in terms of forensic data. This should, for instance, include who is responsible for logging which data.	N/A	Section 1.14 Oracle Hosting and Delivery Policies	<b>Section 1.14 of the Oracle Cloud Hosting and Delivery Policies</b> addresses retention of security logs.
G5/2018 4.12.2(d)	The contractual agreement should also determine which forensic tools are available to a bank directly or via a third party.	N/A	No equivalent	Oracle will work closely with the bank to assist in forensic investigations, including with its use of forensic tools.
G5/2018 4.12.2(e)	The contractual agreement should stipulate both parties' responsibilities related to discovery searches, litigation holds, preservation of evidence and expert testimony. A bank should be able to provide adequate assurance to investigative and regulatory authorities that all data requested has been retrieved.	N/A	No equivalent	Upon Oracle's receipt of a request for preservation of evidence, litigation hold, or for retrieval of information, Oracle will determine its obligations under local law and regulations and cooperate with the requestor to implement, or to assist the requestor in implementing, the request consistent with those obligations.
G5/2018 4.12.2(f)	The contractual agreement should stipulate the duration during which forensic data would be available to the bank.	N/A	Section 1.14 Oracle Hosting and Delivery Policies	Upon Oracle's receipt of a request for forensic data, Oracle will work with the customer to determine the type of data that is needed to complete the inquiry and discuss the availability of such data.  <b>Section 1.14 of the Oracle Cloud Hosting and Delivery Policies</b> addresses the time period for which Oracle retains security logs.
G5/2018 4.12.2(g)	The contractual agreement with the third party should require assurance that the bank's data is preserved as recorded, which includes both the primary data and secondary information, such as metadata and logs.	N/A	Section 1.14 Oracle Hosting and Delivery Policies	<b>Section 1.14 of the Oracle Cloud Hosting and Delivery Policies</b> addresses the time period for which Oracle retains security logs provided that the data is part of the Services.
G5/2018 4.12.3(b)	Banks should consider the availability of records if required for forensic audits which may, specifically in a multitenant environment, be commingled and migrated among multiple servers located across national boundaries, which may make it impossible to identify specific data.	N/A	Section 1.5 FSA	This obligation does not apply to cloud service providers. However, <b>Section 1.5 of the FSA</b> seeks to protect all customer data by stating that, in the course of a customer audit, no access will be granted to data or services environments belonging to any other Oracle customer, nor any information whose disclosure might threaten Oracle networks or systems or other Oracle customers' service environments.
G5/2018 4.12.3(c)	A bank should consider that where a court or government grants access to a third party's servers, such local	N/A	N/A	Upon Oracle's receipt of a request for confidential information from an authorized third-party, including government or law enforcement agencies

	authorities might have access to the bank's forensic data. This should not include a bank's customer data, which should be encrypted, with the bank restricting access to the encryption keys.			or non-governmental attorneys or others through an informal request or a formal legal process, Oracle's Legal Department will determine whether Oracle is legally obligated to provide such information in accordance with local laws and regulations in addition to Oracle's internal Third-Party Information Access Request Policy and Oracle's Information Protection Policy. Once Oracle has determined the scope of its legal obligations with respect to such access requests, Oracle will work with the third-party to provide the requested confidential information in an appropriate manner, if legally required to do so. Oracle employs robust data security controls, including encryption for data at rest and in transit. Services specific information about encryption and key management controls is available to customers in the Privacy and Security Feature documentation on My Oracle Support and the Cloud security portal.
G5/2018 4.13.1(a)	The importance of a comprehensive contractual agreement, including SLAs cannot be overemphasized.	7.7.3	CSA  Ordering Document  Oracle Cloud Hosting and Delivery Policies (particularly Sections 1, 3.1 and 3.2) SaaS Cloud Services Pillar Document:  <a href="https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf">https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf</a>  PaaS/IaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf">https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf</a>	Oracle's written cloud services contract and Ordering Document specifies Oracle's written cloud services contract and Ordering Document specifies the rights and obligations of the parties relating to Oracle's cloud services  Oracle addresses Service Availability and Service Level Agreements in <b>Sections 3.1 and 3.2 of the Oracle Cloud Hosting and Delivery Policies</b> as well as the <b>PaaS/IaaS Cloud Services Pillar Document</b> or the <b>SaaS Cloud Pillar Document</b> , as applicable.
G5/2018 4.13.1(b)	The contract and SLAs should be reviewed by bank's legal counsel and relationship should not start before the contact has been signed by all parties.	N/A	Ordering Document	The Services Period for the cloud services commences on the date stated in the Ordering Document which becomes effective upon the execution by both parties.
G5/2018 4.13.1(c)	The contractual agreement with the third parties should define the third party's contractual obligations as guardian of a bank's data.	7.7.11	Sections 4 and 5 CSA Section 6 of DPA Oracle Cloud Hosting and Delivery Policies  SaaS Cloud Services Pillar Document:  <a href="https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf">https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf</a>  PaaS/IaaS Cloud Services Pillar Document:	The Oracle Cloud services contract addresses the integrity, privacy and safety of customer's content as follows:  <u>Technical and organization security measures:</u>  - <b>Section 6 – Security and Confidentiality – of the Oracle Data Processing Agreement</b>  - the <b>Oracle Cloud Hosting and Delivery Policies</b> as well as the <b>PaaS/IaaS Cloud Services Pillar Document</b> or the <b>SaaS Cloud Pillar Document</b> , as applicable.  - <b>Oracle Corporate Security Practices</b>  <u>Confidentiality and Protection of Customer Content:</u>

			<p><a href="https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf">https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf</a></p> <p><u>Section 2 DPA</u></p> <p>Oracle Corporate Security Practices:</p> <p>oracle.com/corporate/security-practices/</p>	<p><b>Section 4 of Schedule C of the OMA</b> and <b>Section 4 of the CSA</b>, as applicable (specifically, Oracle’s obligation to protect the confidentiality of “Your Content” for as long as it resides in the Services)</p> <p><b>Section 5 of Schedule C</b> and <b>Section 5 of the CSA</b>, as applicable.</p> <p><b>Section 2 of the DPA</b> describes the responsibilities of Oracle and the customer with respect to the processing of personal information and the bank’s instructions.</p>
G5/2018 4.13.1(d)	Banks should ensure that the contractual agreement provides all elements relevant to the cloud computing and/or data offshoring arrangement, including sufficient protection of data applicable to the nature of services being offered, deployment of services structurally and geographically, and compliance with the laws in the various jurisdictions where the data will be hosted or stored.	7.7.5	<p>Section 8 FSA</p> <p>Section 1 Oracle Cloud Hosting and Delivery Policies</p> <p>Ordering Document</p> <p>See Row Above</p>	<p><b>Section 8 of the FSA</b> addresses the parties’ obligation to comply with applicable laws.</p> <p><b>Section 1 of the Oracle Cloud Hosting and Delivery Policies</b> describes Oracle’s information security practices including physical security safeguards, system and data access controls, encryption and training.</p> <p><b>Ordering Document</b></p> <p><b>See Row Above.</b></p>
G5/2018 4.13.2(a)	The contractual agreement with any third party involved in the cloud computing and/or data offshoring arrangements should clearly state that the bank retains ownership rights to the data.	N/A	<p>Section 3.1 CSA</p> <p>Section 3.1 OMA Schedule C</p>	<p><b>Section 3.1 of the CSA</b> and <b>OMA Schedule C</b> confirms that each party retains ownership rights to their IP.</p>
G5/2018 4.13.2(b)	Both the bank and third party should understand how the data ownership rights are affected by the different laws in the countries which will host the data.	N/A	<p>Section 14 CSA</p>	<p><b>Section 14 of the CSA</b> sets out the governing law and jurisdiction of the agreement.</p>
G5/2018 4.13.3	Banks should obtain assurance from service provider that data, including all copies and backups are stored only in geographic locations permitted by the contractual agreements in line with the bank’s regulatory and legislative requirements.	N/A	<p>Ordering Document</p> <p>Oracle Cloud Console</p> <p>Cloud Regions around the globe:</p> <p><a href="https://www.oracle.com/cloud/data-regions/#emea">https://www.oracle.com/cloud/data-regions/#emea</a>.</p>	<p>Oracle operates within various regions across the globe. Each region is composed of one or more physically isolated and fault-tolerant data centers (also named availability domains). When customers set up their Oracle account, they choose a data center region in which to initially locate their tenancy and their content is hosted within that region unless customers choose to move their content outside of the region.</p> <p>The Ordering Document or the Oracle Cloud Console states the data center region in which customer’s content will be stored. See <b>Section 2.2 of the Oracle Cloud Hosting and Delivery Policies</b>.</p>
G5/2018 4.13.4	The contractual agreement should clearly state which activities may be subcontracted by a third party and that such arrangements would be subject to full compliance with the primary contractual agreement, including meeting regulatory and compliance requirements stipulated therein. The primary contract should clearly state that the service provider remains liable for performance in terms of the contract despite any subcontracting arrangements.	7.7.12	<p>Section 6.1 of the FSA</p> <p>Section 4 DPA</p> <p>Oracle Strategic Subcontractors:</p> <p><a href="https://support.oracle.com/epmos/faces/DocumentDisplay?id=2667492.2">https://support.oracle.com/epmos/faces/DocumentDisplay?id=2667492.2</a></p>	<p><b>Section 6.1 of the FSA</b> indicates that all subcontractors with access to customer content will be subject to the same level of data protection and security as Oracle under the terms of the Oracle Cloud services contract. In addition, under this section, Oracle agrees to enter into written agreements with subcontractors reflecting obligations that are consistent with Oracle’s obligations under the relevant terms of the Oracle Cloud services contract. Any such subcontracting will not diminish Oracle’s responsibility towards its customers under Oracle Cloud services contracts and Oracle will appropriately oversee a subcontractor’s performance.</p> <p><b>Section 4 of the DPA</b> states that to the extent Oracle engages third party subprocessors and/or Oracle affiliates to</p>

				process personal information, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Services Agreement.
G5/2018 4.13.5	The service provider shall provide an undertaking to treat the bank's data with the utmost confidentiality. Access should be restricted on a least-privilege basis.	7.7.11	Section 1.4 Oracle Cloud Hosting and Delivery Policies Sections 4 and 5 CSA and OMA Section 6 DPA	<p><b>Section 1.4 of the Oracle Cloud Hosting and Delivery Policies</b> describes Oracle's access controls for personnel with access to the Cloud Services environment. Oracle enforces Role Based Access Controls (RBAC) and employs the following access management principles:</p> <ul style="list-style-type: none"> <li>• Need to know</li> <li>• Least privilege</li> <li>• Segregation of duties.</li> </ul> <p><b>Sections 4 and 5 of the CSA/ Sections 4 and 5 of the OMA Schedule C</b>, which set out Oracle's obligation to keep confidential and protect confidential information.</p> <p><b>Section 6 of the DPA</b> sets out Oracle's obligation to implement and maintain appropriate technical and organizational security measures for the processing of personal information designed to prevent accidental or unlawful destruction, loss, alteration and unauthorized access or disclosure.</p>
G5/2018 4.13.6(a)	The bank is responsible for ensuring that the contractual agreement with the service provider ensures that it is able to meet its data breach notification or other legal reporting requirements.	N/A	Section 8 DPA	<b>Section 8 of the DPA</b> sets out Oracle's incident management and breach notification obligations.
G5/2018 4.13.6(b)	The contractual agreement should define roles and responsibilities in case of a data breach, including cooperative processes to be implemented during the investigation and any follow-up actions.	N/A	Section 8 DPA	<b>Section 8 of the DPA</b> sets out Oracle's incident management and breach notification obligations.
G5/2018 4.13.6(c)	The contractual agreement should define the penalties payable by the third party for data breaches where the third party did not adhere to the terms of the agreement or was negligent in any other way.	N/A	Section 7 CSA Section 7 Schedule C OMA	<b>Section 7 of the CSA and Section 7 of Schedule C of the OMA</b> sets forth the limitations of liabilities.
G5/2018 4.13.7	The use of cloud computing or offshoring data should not inhibit the bank's ability to meet its data retention legal requirement.	N/A	<a href="https://docs.oracle.com/en/solutions/oci-best-practices/back-your-data1.html#GUID-4CF0554F-4AF2-4875-8FB3-FE0974EF1380">https://docs.oracle.com/en/solutions/oci-best-practices/back-your-data1.html#GUID-4CF0554F-4AF2-4875-8FB3-FE0974EF1380</a>  Section 6.1 Oracle Cloud Hosting and Delivery Policies  Section 9.1 DPA  Section 9.5 CSA	<p>Customers are responsible for implementing data backup strategies that meet their business requirements.</p> <p><b>Section 6.1 of the Oracle Cloud Hosting and Delivery Policies</b> 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.</p> <p><b>Section 9.1 of the DPA</b> confirms that, on termination of an arrangement, Oracle will promptly return or delete any remaining copies of personal data, except as otherwise stated in the Oracle Cloud services contract.</p> <p><b>Section 9.5 of the CSA</b> addresses availability of Content following the end of the Service Period.</p>

**Guidance Note 5 of 2014 from the Office of the Registrar of Banks (Outsourcing functions within Banks) and FSB Directive 159.A.i**

TOPIC REF.	REGULATION REQUIREMENT/DESCRIPTION	FSB DIRECTIVE 159.A.I EQUIVALENT	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
G5/2014 6.5.1	The importance of a comprehensive outsourcing agreement, including SLAs cannot be overemphasised and all outsourcing arrangements should be contained in a documented, legally binding agreement or contract.	N/A	<p>CSA</p> <p>Ordering Document</p> <p>Oracle Cloud Hosting and Delivery Policies (particularly Sections 1, 3.1 and 3.2)</p> <p>SaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf">https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf</a></p> <p>PaaS/IaaS Cloud Services Pillar Document: <a href="https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf">https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf</a></p>	<p>Oracle’s written cloud services contract and Ordering Document specifies the rights and obligations of the parties relating to Oracle’s cloud services.</p> <p>Oracle addresses Service Availability and Service Level Agreements in <b>Sections 3.1 and 3.2 of the Oracle Cloud Hosting and Delivery Policies</b> as well as the <b>PaaS/IaaS Cloud Services Pillar Document</b> or the <b>SaaS Cloud Pillar Document</b>, as applicable.</p>
G5/2014 6.5.2	The contract and SLAs should at a minimum include, access to assets, audit, business continuity, start and end dates, confidentiality, privacy, security, customer complaints, termination, dispute resolution, establishment and monitoring performance, foreign based services, incentive compensation review, indemnification, insurance, limitation of liability, notification of inability to perform, offshoring arrangements, ownership and licenses, fee structure and pricing, provisions for amendment and periodic reviews, remedies for non-performance, reporting, responsibilities for providing, receiving and retaining information, compliance with laws and regulations, rights of regulatory and supervisory authorities, including unrestricted rights to access information and subcontracting	7.7.1	See Adjacent Column	<p><b>Terms relating to the following topics may be found at the following references:</b></p> <p><b>Access to Assets:</b> Section 1 (customer’s audit rights) and Section 2 (regulators’ audit rights) of the FSA.</p> <p><b>Audit:</b> Section 1 (customer’s audit rights) and Section 2 (regulators’ audit rights) of the FSA.</p> <p><b>Business Continuity:</b> Section 5 of the FSA and Section 2 Oracle Cloud Hosting and Delivery Policies</p> <p><b>Start and End Dates:</b> Ordering Document</p> <p><b>Confidentiality, Privacy and Security:</b> Sections 6 and 8 DPA, Sections 4 and 5 Schedule C, Section 4 and 5 CSA, Oracle Cloud Hosting and Delivery Policies (particularly Sections 1, 3.1 and 3.2)</p> <p><b>Customer Complaints:</b> Section 5 of the Oracle Cloud Hosting and Delivery Policy</p> <p><b>Termination:</b> Section 8 FSA, Section 3.1(b) FSA, Section 9.3 Schedule C OMA, Section 9.4 CSA</p> <p><b>Dispute Resolution:</b> Section 10 of the FSA</p> <p><b>Monitoring:</b> Section 3.2.2 Oracle Cloud Hosting and Delivery Policies, Section 11 Schedule C OMA and Section 11 CSA</p> <p><b>Foreign based services:</b> If applicable, Ordering Document would set forth the service location</p> <p><b>Incentive compensation review:</b> If applicable, Ordering Document</p> <p><b>Indemnification:</b> Section 8 of CSA and Section 5 of OMA</p> <p><b>Insurance:</b> Oracle Cloud services contract and Ordering Document</p>



				<p><b>Limitation of Liability:</b> Section 7 of Schedule C of the OMA and the CSA</p> <p><b>Notifications:</b> Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies</p> <p><b>Offshoring Arrangements:</b> Ordering Document</p>
G5/2014 6.5.3	A bank that outsources a material business activity or function must ensure that its outsourcing agreement includes an indemnity to the effect that any subcontracting by a third-party service provider, including liability for any failure on the part of the subcontractor.	7.7.12 7.7.17	Section 6.1 FSA Section 8 CSA Section 5 OMA	<p><b>Section 6.1 of the FSA</b> indicates that any such subcontracting will not diminish Oracle's responsibility towards its customers under Oracle Cloud services contracts and Oracle will appropriately oversee a subcontractor's performance.</p> <p><b>Section 8 of the CSA</b> and <b>Section 5 of the OMA</b>.</p>
G5/2014 6.5.4	A bank that outsources a material business activity or function must ensure that the outsourcing agreement, specifically any default clause, does not entitle the service provider to unilaterally cancel the agreement in the event that a recovery or resolution action is taken.	7.7.20	Section 4 FSA Section 9.1 and 9.2 FSA	<p><b>Section 4, Exit Provision (Exit Provision)</b> and <b>Section 9.1, Suspension of Termination Right of the FSA</b> describes the customer's right to exercise a stay of termination of the cloud services following the occurrence of a resolution event, with proper notice to Oracle.</p> <p>Under <b>Section 9.2 of the FSA</b>, Oracle will continue to perform the cloud services during a Resolution Event and will provide assistance as requested by customer or its Resolution Authority.</p>
G5/2014 6.9.1	Bank's management must ensure that the contracts and/or SLAs are structured in such a way to ensure that the bank is able at all times to provide the Office of the Registrar of Banks with the necessary information on the outsourced material business activities or functions regardless of whether activity is outsourced, offshored or insourced. The outsourcing agreement should include the right for the Office to access information, which includes conducting onsite visits at the service provider should the Office consider it necessary in its role as prudential supervisor.	7.7.15	Sections 1 and 2 FSA	<p><b>Section 1 of the FSA</b> sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under <b>Section 7 of the DPA</b>.</p> <p><b>Section 2 of the FSA</b> sets out the customer's regulator's audit and access rights.</p>
G5/2014 6.10.1	The bank must have access to the services provider by the bank's internal and external auditors, as well as access by external person conducting independent reviews for assessment by management in order to identify and deal with any weakness in a service providers performance that may have an adverse impact on the service provided to the bank.	7.7.8	Sections 1 and 2 FSA	<p><b>Section 1 of the FSA</b> sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under <b>Section 7 of the DPA</b>.</p> <p><b>Section 2 of the FSA</b> sets out the customer's regulator's audit and access rights.</p>

### Guidance Note 4 of 2017 from the Office of the Registrar of Banks (Cyber Resilience) (G4/2017) and FSB Directive 159.A.i


TOPIC REF.	REGULATION REQUIREMENT /DESCRIPTION	FSB DIRECTIVE 159.A.I EQUIVALENT		DESCRIPTION OF ORACLE PRACTICES
G4/2017 2.3.4	With regards to security testing, specifically also referring to penetration testing, when using third-	N/A	Section 3.4.2 Oracle Cloud Hosting and Delivery Policies	<b>Section 3.4.2 of the Oracle Cloud Hosting and Delivery Policies</b> allows customers to conduct certain functional


	parties banks are required to make use of reputable external service providers for such testing which may, for instance, be evidenced through certification or accreditation.		Oracle Cloud Security Testing Policy: <a href="https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm">https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm</a>	testing for Oracle Cloud services in their test environment on certain Cloud Services.  Oracle conducts penetration tests of the Oracle OCI and SaaS systems at least annually. A commercial vulnerability scanning tool scans external IP addresses and internal nodes monthly. Identified exploitable threats and vulnerabilities are investigated and tracked to resolution. In addition, Oracle completes third-party vulnerability scans/penetration tests annually for applicable services. The summary reports are available upon request for entities that have signed a non-disclosure agreement with Oracle.
No equivalent	No equivalent	7.7.6, Contract must specify the Rand value of the remuneration or consideration payable by the insurer to the other person, or if the Rand value is not fixed or determined on entering into the contract, the bases in which remuneration or consideration payable will be calculated.	Oracle Ordering Document	<b>Section A of the Oracle Ordering Document</b> sets for the applicable fees for the cloud services.
No equivalent	No equivalent	Section 7.7.18, Written contract must set out any warranties or guarantees to be furnished and insurance to be secured by the other person in respect to its ability to fulfil its contractual obligations.	Section 6 CSA and Schedule OMA C  Oracle Cloud services contract  Ordering Document	<b>Section 6 of the CSA and OMA Schedule C.</b>  Oracle generally takes out and maintains certain insurance coverages. Through insurance and/or operating cash, Oracle has the ability to pay the limits on liability set out in the Oracle Cloud services contracts.  Oracle can specify applicable insurance coverage and limits in the Ordering Document.
No equivalent	No equivalent	Section 7.7.19, Written contract must provide for a dispute resolution process.	Section 10 FSA	<b>Section 10 of the FSA</b> addresses dispute resolution and the parties' respective obligations relating to services agreement.


---

## 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](https://blogs.oracle.com)

 [facebook.com/oracle](https://facebook.com/oracle)

 [twitter.com/oracle](https://twitter.com/oracle)

---

Copyright © 2022, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

---

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120