

Oracle Contract Checklist for Select India Financial Services Regulations, Guidance and Circulars

- Reserve Bank of India's Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (2011), Cyber Security Framework in Banks (2016), Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks (2006) and the Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) (2018)
- Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations 2017
- Securities and Exchange Board of India Guidelines on Outsourcing of Activities by Intermediaries (Security and Exchange Board of India, 2011), Circular on Outsourcing by Depositories (Securities and Exchange Board of India, 2015) and Circular on Outsourcing of Activities by Stock Exchanges and Clearing Corporations (Securities and Exchange Board of India, 2017)

August 2022, Version 1.0
Copyright © 2022, Oracle and/or its affiliates
Public

Disclaimer

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

The information in this document was current as of August 2022.

Overview

Oracle has developed this document as a part of its continuing efforts to help financial services customers meet their unique obligations, particularly under the *Reserve Bank of India (RBI)*, the *Insurance Regulatory and Development Authority of India (IRDAI)* and the *Securities and Exchange Board of India (SEBI)* legal frameworks relating to the use of Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications (SaaS)¹. We want to make it easier for you as a financial institution to identify the sections of the Oracle Cloud services contract that pertain to the requirements of the RBI, the IRDAI and the SEBI. In this document, you will find a list of relevant *RBI*, *IRDAI* and *SEBI* regulations, guidelines and circulars, along with a reference to the relevant section(s) of the Oracle Cloud services contract and a short explanation to help you conduct your review of the Oracle Cloud services. For further guidance, please read this document in conjunction with Oracle's Compliance Advisory addressing RBI and IRDAI applicable to financial institutions.

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

- **Oracle Cloud services agreement** – an Oracle Cloud Services Agreement (CSA) or Oracle Master Agreement (OMA) with Schedule C (Cloud)
- **FSA** – The Oracle Financial Services Addendum to the Oracle Cloud Services Agreement (CSA) or Master Agreement (OMA) with Schedule C (Cloud)
- **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](#).

Regulatory Background

India's central bank, the RBI was established in 1935 "to regulate the issue of Bank notes and keeping of reserves with a view to securing monetary stability in India and generally to operate the currency and credit system of the country to its advantage...", (See <https://rbi.org.in/Scripts/AboutusDisplay.aspx#EP>). RBI has provided financial institutions that are under its regulatory authority with guidelines pertaining to cloud computing and offshoring of data in the financial services sector. The guidelines include Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (2011), Cyber Security Framework in Banks (2016), Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks (2006) and the Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) (2018).

The IRDAI was established to ensure the stability of the insurance sector, establish a regulatory framework for the insurance industry in India and to protect policyholders. The purpose of the (Outsourcing of Activities by Indian Insurers) Regulations 2017 is to provide insurers with a legal framework for assessing and managing risks associated with outsourcing arrangements and has a goal of protecting the interests of insurance policyholders from potential negative systemic effects in the insurance sector relating to the management of certain risks.

¹ Oracle Advertising SaaS services; GBU SaaS services and NetSuite services are not included in the scope of this document.

The SEBI was created to provide regulation in the securities market and to protect the interest of securities investors. SEBI has issued guidelines and published circulars regarding outsourcing by exchange intermediaries, including Guidelines on Outsourcing of Activities by Intermediaries (Security and Exchange Board of India, 2011), Circular on Outsourcing by Depositories (Securities and Exchange Board of India, 2015) and Circular on Outsourcing of Activities by Stock Exchanges and Clearing Corporations (Securities and Exchange Board of India, 2017).

**RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (2011) and Equivalent
IRDAI Outsourcing Regulations and SEBI's Outsourcing Guidelines and Circulars**

REQUIREMENT REFERENCE	DESCRIPTION	EQUIVALENT IRDAI REGULATIONS	EQUIVALENT SEBI OUTSOURCING GUIDELINES AND CIRCULARS	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT	DESCRIPTION OF ORACLE PRACTICES
Chapter 2, Section 30(a)	Penetration testing needs to be conducted at least on an annual basis.	N/A	N/A	N/A	<p>Oracle conducts penetration tests of the Oracle OCI and SaaS systems at least annually. In addition, Oracle completes third-party vulnerability scans/penetration tests annually for applicable services.</p> <p>See: Oracle Cloud Security Testing Policy.</p>
Section 2(iii)	The terms governing the contract between the bank and the service provider should be carefully defined in written agreements and vetted by bank's legal counsel on their legal effect and enforceability.	Regulation 11(i) Outsourcing arrangements shall be governed by written agreements that are legally binding for a specified period, subject to periodical renewals, if necessary, that clearly describe all important aspects of the outsourcing arrangement, including the rights and obligations of all parties.	Annexure I, Section 5 (Guidelines on Outsourcing of Activities by Intermediaries)- Outsourcing relationships shall be governed by written contracts/agreements/terms and conditions (as deemed appropriate) {hereinafter referred to as "contract"} that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities, and expectations of the parties to the contract, client confidentiality issues, termination procedures, etc.	CSA Ordering Document	Written Oracle Cloud services contract and referenced Service Specifications.

ORACLE

			by Stock Exchanges and Clearing Corporations) – Stock Exchange and clearing corporations shall ensure that there is a legally binding written contract with the service provider/Outsourcing agency.		
Section 2(iii)	Banks should ensure that the contract brings out nature of legal relationship between the parties (agent, principal or otherwise), and addresses risks and mitigation strategies identified at the risk evaluation and due diligence stages.	N/A	Annexure I, Section 5.1 (Guidelines on Outsourcing of Activities by Intermediaries)- Outsourcing arrangements shall be governed by a clearly defined and legally binding written contact between the intermediary and each of the third parties, the nature and detail of which shall be appropriate to the materiality of the outsourced activity in relation to the ongoing business of the intermediary.	CSA Ordering Document	Written Oracle Cloud services contract and referenced Service Specifications.
Section 2 (iii)	Contracts should provide for periodic renewal and re-negotiation to enable institution to retain an appropriate level of control over the outsourcing.	N/A	Section 7.2 (Circular on Outsourcing of activities by Stock Exchanges and Clearing Corporations) - Each agreement should allow for renegotiation and renewal to enable the exchange to retain an appropriate level of control over the outsourcing	Ordering Document	Written Oracle Cloud services contract and referenced Service Specifications.

ORACLE

Section 2 (iii)	Contracts should include the right to intervene with appropriate measure to meet the Bank's legal and regulatory obligations.	N/A	Section 7.2 (Circular on Outsourcing of activities by Stock Exchanges and Clearing Corporations) - Each agreement should allow for renegotiation and renewal to enable the exchange to retain the right to intervene with appropriate measures to meet its legal and regulatory obligations.	Section 8 FSA	Section 8 of the FSA sets out a contractual obligation to comply with applicable laws.
Section 2(iii)	Contractual Agreement should, in the very least, have provision for the following: (See all references to Section 2(iii)) Scope: Agreements should state the activities that are to be outsourced.	Regulation 11(i) Outsourcing arrangements shall be governed by written agreements that are legally binding for a specified period, subject to periodical renewals, if necessary, that clearly describe all important aspects of the outsourcing arrangement, including the rights and obligations of all parties.	Annexure I, Section 5 (Guidelines on Outsourcing of Activities by Intermediaries)- Outsourcing relationships shall be governed by written contracts/agreements/terms and conditions (as deemed appropriate) {hereinafter referred to as "contract"} that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities, and expectations of the parties to the contract, client confidentiality issues, termination procedures, etc. Section 5.1 (Circular on Outsourcing Activities by Stock Exchanges and Clearing Corporations) – Stock Exchange and clearing corporations	CSA Ordering Document	Written Oracle Cloud services contract and referenced Service Specifications.

			shall ensure that there is a legally binding written contract with the service provider/Outsourcing agency.		
Section 2(iii)	Performance Standards: Key performance metrics should be defined for each activity to be outsourced, as part of the overall Service Level Agreement	N/A	N/A	Sections 3.1 and 3.2 Oracle Cloud Hosting and Delivery Policies	<p>Service Availability and Service Level Agreements:</p> <p>Sections 3.1 and 3.2 of the Oracle Cloud Hosting and Delivery Policies as well as the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, as applicable.</p> <p>Oracle Cloud Infrastructure Service Level Agreement: https://www.oracle.com/cloud/sla/</p>
Section 2(iii)	Monitoring and Oversight: Provide for continuous monitoring and assessment by the bank of the service provider so that any necessary corrective measure to meet the Bank's legal and regulatory obligations.	N/A	<p>Annexure I, Section 5.2(d) (Guidelines on Outsourcing of Activities by Intermediaries)-</p> <p>Outsourcing contract provides for continuous monitoring and assessment by the intermediary of the third party so that any necessary corrective measures can be taken up immediately, i.e., the contract shall enable the intermediary to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations.</p> <p>Section 2(vii) Circular on Outsourcing by Depositories-</p> <p>An effective monitoring of the entities selected for outsourcing shall be</p>	<p>Section 3.2.2 Oracle Cloud Hosting and Delivery Policies</p> <p>Section 11 Schedule C and CSA</p>	<p>Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability.</p> <p>Section 11.1 of Schedule C and the CSA, as applicable, explains that Oracle also continuously monitors the Cloud services.</p>

			done to ensure that there is check on the activities of outsourced entity.		
Section 2(iii)	<p>Access to books and records/Audit and Inspection: This would include:</p> <ol style="list-style-type: none"> 1) Ensure that the bank has ability to access all books, records and information relevant to the outsourced activity available with the service provider. For technology outsourcing, requisite audit trail and logs for administrative activities should be retained and accessible to the Bank based on approved requests 2) Provide Bank with the right to conduct audits on the service provider whether by internal or external auditors, or by external specialists appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed by the bank 3) Include clauses to allow the Reserve Bank of India or persons authorized by it to access the bank's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. This includes information maintained in paper and electronic formats. 4) Recognize the right of the Reserve Bank to cause and inspection to be made of a service provider of a bank and its books and account by one or 	<p>Regulation 13 The insurer shall conduct periodic inspection or audit on the outsourcing service providers either by internal auditors or by Chartered Accountant firms appointed by the insurer to examine the compliance of the outsourcing agreement while carrying out the activities outsourced. Insurer shall ensure that enabling provisions for the Inspection by the Insurer shall be included in the Agreement with outsourcing service provider. Measures shall be taken to arrest the deficiencies noticed if any in the inspection or audit report.</p> <p>Regulation 18(i) Include a provision in the outsourcing agreement, giving authorized representatives of the IRDAI the right to: Examine the books, records, information, systems, and the</p>	<p>Annexure I, Section 5.2(m) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract provides for intermediary and /or the regulator or the persons authorized by it to have the ability to inspect, access all books, records, and information relevant to the outsourced activity with third party.</p> <p>Section 12.1 (Circular on Outsourcing of Activities by Stock Exchanges and Clearing Corporations) - The outsourcing arrangement should provide for the access by the regulatory authority of the records of service providers/Outsourcing agencies and other information relating to the activities that are relevant to regulatory oversight.</p>	<p>Section 2 FSA Section 1.12 Oracle Cloud Hosting and Delivery Policies Section 7 DPA</p>	<p>1) Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA. Section 1 of the FSA sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under Section 7 of the DPA.</p> <p>2) Section 1.12 of the Oracle Cloud Hosting and Delivery Policies indicates that Oracle may conduct independent reviews of Cloud services utilizing third parties in the following areas (the scope of any such reviews may vary by service and country): <ul style="list-style-type: none"> • SOC 1 (based on Statement on Standards for Attestation Engagements (SSAE) No 18) and/or SOC 2 reports • Other independent third-party security testing to review the effectiveness of administrative and technical controls. Additionally, Oracle's common shares are traded on the NYSE Stock Market and Oracle is thus subject to standard information obligations on all matters relevant to the public market. As a publicly traded company, Oracle is not permitted to report material non-public information with a single customer. However, as required by applicable law, such information is reported by Oracle as part of our public company filings with the SEC.</p> <p>Oracle Cloud Compliance Site</p> <p>3) Section 2.1 of the FSA further provides that a customer's regulator may audit Oracle as required by applicable law. Please also refer to Section 2.5 of the FSA, which expressly states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law.</p> <p>4) Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA.</p>

ORACLE

	<p>more of its officers or employees or other persons</p> <p>5) Where the controlling/Head offices of foreign banks operating in India outsource the activities related to the Indian operations, the Agreement should include clauses to allow the RBI or persons authorized by it to access the bank's documents, records of transactions and other necessary information given or store by the service provider within a reasonable time also clauses to recognize the right of RBI to cause an inspection to be made of a service provider and its books and accounts by one or more of its officers or employees or other persons</p>	<p>internal control environment in the outsourcing service provider (or sub-contractor as applicable), to the extent that they relate to the service being performed for the Insurer; and Access any internal audit reports or external audit findings of the outsourcing service Provider that concern the service being performed for the Insurer.</p>			<p>5) See Number 3 above.</p> <p>Oracle Cloud Compliance Site: https://www.oracle.com/corporate/cloud-compliance/</p>
Section 2(iii)	Contract should include a termination clause and minimum periods to execute a termination provision as deemed necessary.	N/A	Annexure I, Section 5.2(j) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract provides for termination of contract and termination rights.	Section 3.1(b) FSA Section 9.3 Schedule C Section 9.4 CSA	<p>Section 3.1(b) of the FSA expressly permits customers to terminate any affected outsourcing agreement with Oracle under certain circumstances with at least 30 days prior written notice to Oracle by the customer.</p> <p>Section 9.3 of Schedule C and Section 9.4 of the CSA, as applicable, which provides a termination right in the event of a breach of a material term of the Agreement.</p>
Section 2(iii)	Agreements should provide for maintaining confidentiality of customers information even after the contract expires or is terminated by either party.	N/A	Annexure I, Section 5.2(f) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract has unambiguous confidentiality clauses to ensure protection of proprietary and customer data during the tenure of the contract and also after	Section 4 Schedule C Section 4 CSA	Section 4 of Schedule C and of the CSA , as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services).

			the expiry of the contract.		
Section 2(iii)	Contract should include condition for default termination/early exit option for contracts. This may include circumstances when the service provider undergoes a change in ownership, becomes insolvent or goes under liquidation, received judicial indictment (whether within India or any other location), or when there has been a breach of confidentiality, security, or demonstrable deterioration in quality of services rendered.	N/A	<p>Annexure I, Section 5.2(j) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract provides for termination of the contact.</p> <p>Section 11 (Circular on Outsourcing Activities by Stock Exchanges and Clearing Corporations) - Stock exchanges and clearing corporations should include contractual provisions relating to termination of the contract and appropriate exit strategies inter-alia specifying events that may trigger termination of the service contract, what will occur on termination and strategies for managing the transfer of activity back to the stock exchange and clearing corporation or to another party.</p>	<p>Section 3.1(c) FSA</p> <p>Section 3.2 FSA</p> <p>Section 6.1 and 9.3 Schedule C</p> <p>Section 6.1 and 9.4 CSA</p>	<p>Section 3.1(c) of the FSA states that a customer may terminate any affected outsourcing agreement if impediments are identified that impact Oracle's ability to perform the cloud services.</p> <p>Section 3.2 of the FSA addresses the customer's termination rights if Oracle becomes insolvent.</p> <p>Sections 6.1 and 9.3 of Schedule C and Sections 6.1 and 9.4 of the CSA, as applicable, further explain that customers have the right to terminate for any breach of a material contract term, including a breach of the service warranty. In the service warranty, Oracle warrants that it will perform the services using commercially reasonable care and skill in all material respects as described in the Service Specifications.</p>
Section 2(iii)	In all cases of termination (early or otherwise), an appropriate handover process for data and process needs to be agreed with the service provider.	<p>Regulation 11(e) The outsourcing contract shall contain a contract termination clause specifying orderly handing over data, assets, etc.</p> <p>Regulation 12(iii)</p>	<p>Annexure I, Section 5.2(h) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract provides for transfer of information and exit strategies.</p>	<p>Section 9.1 DPA</p> <p>Section 4.1 FSA</p>	<p>Section 9.1 of the DPA 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>Section 4.1 of the FSA 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>

		In the event of termination of the outsourcing agreement, the insurer should ensure that the customer data is retrieved from the service provider and ensure there is no further use of customer data by the service provider.			
Section 2(iii)	Mandate controls to ensure customer data confidentiality and service provider's liability in case of breach of security and leakage of confidential customer related information. For e.g., use of transaction-enabled mobile banking channels necessitates encryption controls to ensure security of data in transmission.	N/A	Annexure I, Section 7 (Guidelines on Outsourcing of Activities by Intermediaries) - The intermediary shall take appropriate steps to require that third parties protect confidential information of both the intermediary and its customers from intentional or inadvertent disclosure to unauthorized persons.	Sections 4 and 5 Schedule C Section 4 and 5 CSA Section 1 Oracle Cloud Hosting and Delivery Policies Section 7 CSA Sections 6 and 8 DPA	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices.</p> <p>Section 1.5 of the Oracle Cloud Hosting and Delivery Policies in particular sets out Oracle's use of encryption technology.</p> <p>Confidentiality and Protection of "Your Content":</p> <ul style="list-style-type: none"> - Section 4 of Schedule C and of the CSA, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services) - Section 5 of Schedule C and of the CSA, as applicable - <p>Section 6 of the DPA sets out Oracle's obligation to implement and maintain appropriate technical and organisational security measures for the processing of personal information designed to prevent accidental or unlawful destruction, loss, alteration and unauthorised access or disclosure.</p> <p>Section 8 of the DPA sets out Oracle's incident management and breach notification obligations.</p> <p>Section 7 of the CSA and Schedule C, which sets forth the limitations of liabilities for direct damages.</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p>

Section 2(iii)	Confidentiality and Security: Provide for the preservation of documents and data by the service provider in accordance with the legal/regulatory obligation of the bank in this regard.	N/A	Annexure I, Section 5.2(h) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract provides for preservation of the documents and data by third party. Section 10.1 (Circular on Outsourcing of Activities by Stock Exchanges and Clearing Corporations) – Stock exchanges and clearing corporations should have adequate procedures in place that require the service provider / Outsourcing agency to protect the exchanges proprietary, member-related, and potentially market sensitive information and software from unauthorized usage.	Section 6 DPA Sections 4 and 5 Schedule C Section 4 and 5 CSA	Section 6 of the DPA sets out Oracle's obligation to implement and maintain appropriate technical and organisational security measures for the processing of personal information designed to prevent accidental or unlawful destruction, loss, alteration and unauthorised access or disclosure. Confidentiality and Protection of "Your Content": <ul style="list-style-type: none">- Section 4 of Schedule C and of the CSA, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services)- Section 5 of Schedule C and the CSA, as applicable.
Section 2(iii)	The contract should contain clauses for contingency plans and testing thereof, to maintain business continuity.	Section 11(c) Contingency planning of the outsourcing service Provider to provide business for the outsourced arrangements that are material. Regulation 16(i) Insurers shall establish and maintain adequate contingency plans where the outsourced activity is material. These include disaster	Annexure I, Section 5.2(g) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract specifies the responsibilities of the third party with respect to the contingency plans, business continuity and disaster recovery. Annexure I, Section 6 (Guidelines on Outsourcing of	Section 5 FSA Section 2 Oracle Cloud Hosting and Delivery Policies	Section 5 of the FSA indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. 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. Section 2 of the PaaS/IaaS Cloud Services Pillar Document and Section 2 of the SaaS Cloud Pillar Document also addresses the Oracle cloud service continuity policy and the Oracle cloud service backup strategy, respectively.

ORACLE

	<p>recovery plans and backup facilities to support the continuation of an outsourced activity with minimal business disruption in the event of reasonably foreseeable events that affect the ability of an outsourcing service provider to continue providing the service.</p> <p>Regulation 16(ii) In particular, contingency plans should ensure that the Insurer can readily access all the records necessary to allow it to sustain business operations, meet statutory obligations, and provide any information relating to the outsourced activity as may be required by the IRDAI.</p> <p>Regulation 16(iii) Contingency plans should also be regularly tested to ensure that they remain robust, particularly under changing operation conditions.</p>	<p>Activities by Intermediaries) - The intermediary and its third parties shall establish and maintain contingency plans, including a plan for disaster recovery and periodic testing of backup facilities.</p>			
Section 2(iii)	Agreements may include covenants limiting further sub-contracting. Agreements should provide for prior approval/consent by the bank of the use of subcontractors by the service provider for all or part of an outsourced activity. The bank should retain	N/A	Annexure I, Section 5.2(e) (Guidelines on Outsourcing of Activities by Intermediaries) -	Section 4.1 DPA Section 6.1 FSA Section 6.2 FSA	Section 4.1 of the DPA indicates 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 Oracle Cloud services contract. This section also indicates that Oracle is responsible for the

	<p>the ability of similar control and oversight over the sub service provider as the service provider.</p>	<p>Outsourcing contract includes, where necessary, conditions of sub-contracting by the third-party, i.e. the contract shall enable intermediary to maintain a similar control over the risks when a third party outsources to further third parties as in the original direct outsourcing.</p> <p>Section 2(v) of Circular on Outsourcing by Depositories - Depositories shall ensure that outsourced activities are further outsourced downstream only with the prior consent of the depository and with appropriate safeguards including proper legal documentation[and] agreement.</p> <p>Section 6.1 (Circular on Outsourcing of Activities by Stock Exchanges and Clearing Corporations) – Stock Exchanges and clearing corporations shall ensure that outsourced activities are further outsourced downstream only with the prior consent of the exchange and clearing corporation and with appropriate safeguards including proper legal</p>	<p>Section 14.2 Schedule C Section 17.2 CSA</p>	<p>performance of the Oracle affiliates and third party subprocessors' obligations in compliance with the terms of the Oracle Data Processing Agreement and applicable data protection law.</p> <p>Sections 6.1 to 6.2 of the FSA include terms applicable to Oracle's use of subcontractors and strategic subcontractors, and similar to the DPA, includes a right for a customer to object to the intended involvement of a new strategic subcontractor.</p> <p>Section 6.1 of the FSA further 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>Section 14.2 of Schedule C and Section 17.2 of the CSA, as applicable.</p>
--	--	--	---	--



			documentation/agreement.		
Section 2(iii)	Agreement should specify the resolution process, the event of default, indemnities involved and the remedies and recourse of the respective parties to the agreement.	Regulation 11(ii) The outsourcing contracts, shall have in place clauses and conditions relating to guarantee or indemnity from the outsourcing service provider towards his commitment including liability for any failure.	Annexure I, Section 5.2(b) (Guidelines on Outsourcing of Activities by Intermediaries)- Outsourcing contract provides for mutual rights obligations and responsibilities of the intermediary and third party, including indemnity by the parties. Section 7.3 (Circular on Outsourcing of Activities by Stock Exchanges and Clearing Corporations)- The agreement should provide for a dispute resolution mechanism, inter-alia specifying the resolution process, events of default, and indemnities, remedies and recourse of the respective parties in the agreements.	Section 4 FSA Section 9 FSA Section 8 CSA Section 5 OMA Section 7 CSA and Schedule C	<p>Section 4 of the FSA provides customers with the ability to order transition services and transition assistance to facilitate the transfer or the re-incorporation of the concerned function back to the customer or to a third-party provider.</p> <p>Sections 9.1, and 9.2 of the FSA.</p> <p>Section 8 of the CSA and Section 5 of the OMA</p> <p>Section 7 of the CSA and Schedule C, which sets forth the limitations of liabilities for direct damages.</p>
Section 2(iii)	Agreements should include choice of law provisions, based on the regulations of the applicable to the bank.	N/A	Annexure I, Section 5.2(k) (Guidelines on Outsourcing of Activities by Intermediaries)- Outsourcing contract addresses additional issues arising from country risks and potential obstacles in exercising oversight and management of the	Section 14 CSA	<p>Section 14 of the CSA sets out the governing law and jurisdiction of the agreement.</p>

ORACLE

			arrangements when the intermediary outsources its activities to foreign third party. For example, the contract shall include choice of law provisions and agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction.		
Section 2(iii)	An agreement should be tailored to provide for specific risks relating to cross border businesses and operations, data privacy and ownership aspects, among others.	Regulation 11(ii) Outsourcing contracts, shall include clauses and conditions such as information and asset ownership, information technology, data security and protection of confidential information.		<p>Section 3 CSA and Schedule C</p> <p>Sections 5, 6 and 8 DPA</p> <p>Sections 4 and 5 Schedule C</p> <p>Section 4 and 5 CSA</p> <p>Section 1 Oracle Cloud Hosting and Delivery Policies</p> <p>Section 7 CSA</p>	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices. Section 1.5 of the Oracle Cloud Hosting and Delivery Policies in particular sets out Oracle's use of encryption technology.</p> <p>Confidentiality and Protection of "Your Content":</p> <ul style="list-style-type: none"> - Section 4 of Schedule C and of the CSA, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services) - Section 5 of Schedule C and Section 5 of the CSA, as applicable <p>Section 5 of the DPA addresses cross-border data transfers.</p> <p>Section 6 of the DPA sets out Oracle's obligation to implement and maintain appropriate technical and organisational security measures for the processing of personal information designed to prevent accidental or unlawful destruction, loss, alteration and unauthorized access or disclosure.</p> <p>Section 8 of the DPA sets out Oracle's incident management and breach notification obligations.</p>

					<p>See Section 7 of the CSA and Schedule C, which sets forth the limitations of liabilities for direct damages.</p> <p>Section 3 of the CSA and of Schedule C.</p>
Section 2(iv)	Banks should at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider should highlight any deterioration or breach in performance standards, confidentiality, and security, and in business continuity preparedness.	N/A	N/A	Sections 6 and 8 DPA Sections 4 and 5 Schedule C Section 4 and 5 CSA Oracle Cloud Hosting and Delivery Policies Section 7 CSA	<p>This obligation does not apply to the Cloud services provider; however, 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 including the following:</p> <ul style="list-style-type: none"> • Oracle security practices • Compliance documentation <p>Customers can access these materials via the Oracle Compliance Site as well as on Oracle's Cloud consoles specified in the resources section.</p> <p>Additionally, Oracle's common shares are traded on the NYSE Stock Market, and Oracle is thus subject to standard information obligations on all matters relevant to the public market. As a publicly traded company, Oracle is not permitted to report material non-public information. However, as required by applicable law, such information is reported by Oracle as part of our public company filings with the SEC. (See Investor Relations: https://investor.oracle.com/home/default.aspx)</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p> <p>See Investor Relations Website: https://investor.oracle.com/home/default.aspx</p> <p>SaaS Cloud Services Pillar Document: https://www.oracle.com/assets/saas-public-cloud-services-pillar-3610529.pdf</p> <p>PaaS/IaaS Cloud Services Pillar Document: https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf</p> <p>Oracle Cloud Compliance Site:</p>



					<u>https://www.oracle.com/corporate/cloud-compliance/OracleCompliance Documents in Console:</u> <u>https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm</u>
Section 2(iv)	Banks should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches.	N/A	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies Section 8 DPA	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices.</p> <p>Section 8 of the DPA sets out Oracle's incident management and breach notification obligations.</p> <p>Oracle Corporate Security Practices Site: <u>https://www.oracle.com/corporate/security-practices/</u></p> <p>Oracle Cloud Compliance Site: <u>https://www.oracle.com/corporate/cloud-compliance/</u></p> <p>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.</p>
Section 2(iv)	It may be desirable if banks control the management of user ids created for use of external vendor personnel. As a contingency measure, banks may also endeavor to develop, over a period of time, reasonable level of skills/knowledge in various technology related areas like system administration, database administration, network architecture and administration, etc. to effectively engage with the vendors and also to take over these functions in the event of any contingency.	N/A	N/A	Section 5 FSA Section 2 Oracle Cloud Hosting and Delivery Policies	<p>Section 5 of the FSA 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, 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.</p> <p>Oracle Corporate Security Practices Site: <u>https://www.oracle.com/corporate/security-practices/</u></p>
Section 2(iv)	Management should include SLAs in the outsourcing contracts to agree and establish accountability for performance expectations. SLAs must clearly formalize	N/A	Annexure I, Section 5.2(a) (Guidelines on Outsourcing of	Section 3.1 and 3.2 Oracle Cloud Hosting and Delivery Policies	<p>Service Availability and Service Level Agreements:</p> <p>Sections 3.1 and 3.2 of the Oracle Cloud Hosting and Delivery Policies as well as the <u>PaaS/IaaS Cloud Services</u></p>

	<p>the performance criteria to measure the quality of service levels. Banks should develop the following towards establishing an effective oversight program: (See all rows pertaining to Section 2(iv))</p> <ul style="list-style-type: none"> • Formal Policy that defines the SLA program • SLA monitoring process • Recourse for non-performance • Escalation process 		<p>Activities by Intermediaries)- Outsourcing contract clearly defines what activities are going to be outsourced, including appropriate service and performance levels Annexure I, Section 5.2(c) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract provides for liability of third party to the intermediary for unsatisfactory performance/other breach of contract.</p>		<p>Pillar Document or the SaaS Cloud Pillar Document, as applicable.</p> <p>Oracle Cloud Infrastructure Service Level Agreement: https://www.oracle.com/cloud/sla/</p>
Section 2(iv)	<p>[With respect to SLAs and performance metrics], Banks should develop the following towards establishing an effective oversight program: Dispute Resolution</p>	N/A	<p>Annexure I, Section 5.2(i) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract provides for the mechanisms to resolve disputes arising from implementation of outsourcing contract.</p> <p>Section 7.3 (Circular on Outsourcing of Activities by Stock Exchanges and Clearing Corporations) – The agreement should provide for a dispute resolution mechanism, inter-alia specifying the resolution process, events of default, and</p>	Section 10 FSA	<p>Section 10 of the FSA addresses dispute resolution and the parties' respective obligations relating to services agreement.</p>



			indemnities, remedies and recourse of the respective parties in the agreements.		
Section 2(iv)	With respect to SLAs and performance metrics], Banks should develop the following towards establishing an effective oversight program: Conditions in which the contract may be terminated by either party	N/A	N/A	Section 8 FSA Section 3.1(b) FSA Section 9.3 Schedule C Section 9.4 CSA	Section 8 of the FSA sets out a contractual obligation to comply with applicable laws. Furthermore, Section 3.1(b) of the FSA expressly permits customers to terminate any affected outsourcing agreement if Oracle is in breach of applicable law or regulation in providing the cloud services. Section 9.3 of Schedule C and Section 9.4 of the CSA , as applicable, which provides a termination right in the event of a breach of a material term of the Agreement
Section 2(iv)	Performance expectations, under both normal and contingency circumstances, need to be defined.	N/A	N/A	Section 3.2.2 Oracle Cloud Hosting and Delivery Policies Section 11 Schedule C and CSA	Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability. Section 11.1 of Schedule C and the CSA , as applicable, explains that Oracle also continuously monitors the Cloud services.
Section 2(iv)	Provisions need to be in place for timely and orderly intervention and rectification in the event of substandard performance by the service provider.	N/A	N/A	Section 3.2.2 and 5 Oracle Cloud Hosting and Delivery Policies Section 11 Schedule C and CSA	Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability. Section 5 of the Oracle Cloud Hosting and Delivery Policies outlines the Oracle Cloud Support Policy Section 11.1 of Schedule C and of the CSA , as applicable, explains that Oracle also continuously monitors the Cloud services.
Section 2(iv)	Banks should evaluate the adequacy of internal controls environment offered by the service provider. Due consideration should be given to the implementation of following by the service provider: Information security policies and employee awareness of the same.	N/A	N/A	Section 1 Oracle Hosting and Security and Delivery Policies	Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices. Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/



	(See all rows below pertaining to Section 2(iv))				
Section 2(iv)	Controls for logical access to customer information by service provider staff, so that information may be accessed on a need-to-know basis only.	N/A	N/A	Section 1.4 Oracle Cloud Hosting and Delivery Policies	<p>Section 1.4 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle personnel access to the Services environment for the Cloud Services (including Your Content residing in the Cloud Services), Oracle enforces Role Based Access Controls (RBAC) and employs the access management principles of “need to know”, “least privilege” and “segregation of duties.”</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p>
Section 2(iv)	Physical and environmental security and controls.	N/A	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies describes Oracle's information security practices including physical security safeguards, system and data access controls, encryption and training.</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p>
Section 2(iv)	Network security and controls.	N/A	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices.</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p>
Section 2(iv)	Formal process for tracking and monitoring program changes and projects.	N/A	N/A	Section 4.1 Oracle Cloud Hosting and Delivery Policies	<p>Section 4.1 of the Oracle Cloud Hosting and Delivery Policies addresses Oracle's Cloud change management and maintenance policy.</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p>
Section 2(iv)	Process for incident reporting and problem management.	N/A	N/A	Section 8 of DPA Section 5.2 Oracle Cloud Hosting and Delivery Policies	<p>Section 8 of the DPA sets out Oracle's incident management and breach notification obligations.</p> <p>Section 5.2 of the Oracle Cloud Hosting and Delivery Policies describes Oracle's cloud customers support systems.</p>

					Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/
Section 2(iv)	Special control considerations for service providers using cloud computing as part of service.	N/A	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices.</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p>
Section 2(iv)	Outsourcing should not impede or interfere with the ability of the Bank or the Regulator in performing its supervisory function and objectives.	Regulation 11(d) The outsourcing contract shall include and express clause that the contract shall neither prevent nor impede Insurer from meeting its respective regulatory obligations, nor the IRDAI from exercising its regulatory powers of conducting inspection, investigation, obtaining information from either the Insurer or the outsourcing service provider.	Annexure I, Section 1.1 (Guidelines on Outsourcing of Activities by Intermediaries)- An activity shall not be outsourced if it would impair the supervisory authority's right to assess, or its ability to supervise the business of the intermediary Annexure I, Section 3 (Guidelines on Outsourcing of Activities by Intermediaries) - The intermediary shall ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to customer and regulators, nor impede effective supervision by the regulators. Annexure I, Section 5.2(l) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract neither prevents nor impedes the intermediary from	Sections 1 and 2 FSA	<p>Sections 1 and 2 of the FSA set out Oracle's obligations with respect to customer and customer regulators' audit rights.</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p>

			<p>meeting its respective regulatory obligations, nor the regulator from exercising its regulatory powers.</p> <p>Section 5.2 (Circular on Outsourcing activities by Stock Exchanges and Clearing Corporations) – Stock Exchange and clearing corporation shall ensure that the outsourcing arrangement does not in any way diminish its obligations and those of its board and senior management, to comply with relevant laws and regulations, guidelines and other directions.</p>		
Section 2(iv)	An institution should at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet outsourcing obligations. Such sure diligence reviews, which can based on all available information should highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.	N/A	N/A	<p>Section 1 Oracle Cloud Hosting and Delivery Policies</p> <p>Section 4 Schedule C and CSA</p> <p>Sections 7 DPA</p> <p>Section 1 FSA</p>	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policies, which describes Oracle's security practices. Section 1.5 of the Oracle Cloud Hosting and Delivery Policies in particular sets out Oracle's use of encryption technology.</p> <p>Confidentiality and Protection of "Your Content":</p> <ul style="list-style-type: none"> - Section 4 of Schedule C and of the CSA, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services) - Section 5 of Schedule C and the CSA, as applicable <p>Section 1 of the FSA sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under Section 7 of the DPA.</p>

					Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/
Section 2(iv)	Banks should also periodically commission audit and expert assessments on the security and control environment of the service provider. Such assessments and reports on the service provider may be performed and prepared by the institution's internal or external auditors, or by agents appointed by the institution.	N/A	N/A	Section 1 and 2 FSA Section 7 DPA	<p>Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA.</p> <p>Section 1 of the FSA sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under Section 7 of the DPA.</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p> <p>Oracle Cloud Compliance: oracle.com/corporate/cloud-compliance/</p>
Section 2(iv)	With respect to audits, reviews should take adequate cognizance of historical violations or issue remediation during previous audits and assessments. Copies of previous audit and assessments should be shared during RBI inspections.	N/A	N/A	Section 1 and 2 FSA Section 7 DPA	<p>Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA.</p> <p>Section 1 of the FSA sets out customer's audit and access rights and supplements the audit and inspection rights granted to customers under Section 7 of the DPA.</p> <p>Oracle provides several 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>OCI CAIQ: oracle.com/a/ocom/docs/oci-corporate-caiq.pdf</p> <p>Oracle Fusion Cloud Applications: oracle.com/a/ocom/docs/caiq-oracle-fusion-cloud-applications.pdf</p> <p>Oracle Enterprise Performance Management Cloud Applications: oracle.com/a/ocom/docs/caiq-oracle-epm-cloud-applications.pdf</p> <p>Oracle Cloud Applications: oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf</p>

					Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/ Oracle Cloud Compliance: oracle.com/corporate/cloud-compliance/
Section 2(v)	An institution may take the following steps to ensure that risks with respect to confidentiality and security of data are adequately mitigated: (See all rows pertaining to Section 2(v)) Address, agree and document specific requirements of the respective parties in outsourcing to ensure adequacy and effectiveness of security practices, including identifying obligations and liability in the event of a breach or default.	N/A	Annexure I, Section 5.2(g) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract specifies the responsibilities of the third party with respect to the IT security.	Section 1 Oracle Cloud Hosting and Delivery Policies	Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices. Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/
Section 2(v)	Discuss and agree on the instances where customer data shall be accessed and the user groups who will have access to the same. Access to a Bank's data should be strictly on a need-to-know basis.	N/A	Annexure I, Section 7.2 (Guidelines on Outsourcing of Activities by Intermediaries)- The intermediary shall prevail upon the third party to ensure that the employees of the third party have limited access to the data handled and only on a "need to know" basis and third party shall have adequate checks and balances to ensure the same.	Section 1.4 Oracle Cloud Hosting and Delivery Policies	Section 1.4 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle personnel access to the Services environment for the Cloud Services (including Your Content residing in the Cloud Services), Oracle enforces Role Based Access Controls (RBAC) and employs the access management principles of "need to know", "least privilege" and "segregation of duties." Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/
Section 2 (v)	Ensure that service provider employees are adequately aware and informed on the security and privacy policies.	N/A		Section 1.8 Oracle Cloud and Delivery Policies Section 5.2 DPA	Section 1.8 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices. Section 5.2 of the DPA addresses cross-border transfer of data. Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/

ORACLE

Section 2(vi)	Outsourcing outside of India should be agreed, in a manner that does not obstruct or hinder the ability of the bank or regulatory authorities to perform periodic audits/inspections and assessments, supervise or reconstruct activities of the bank based on books, records and necessary documentation, in a timely manner.	Regulation 18(ii) In cases where Insurer outsources to the service providers outside India, the Insurers shall ensure that the terms of the agreement are in compliance with respective local regulations governing the outsourcing service provider and laws of the country concerned and such laws and regulations do not impede the regulatory access and oversight by the Authority. All original policyholder records continue to be maintained in India.	Section 4.4 (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing arrangements shall[not] impair the ability of SEBI/SRO or auditors to exercise its regulatory responsibilities such as supervision/inspection of the intermediary.	Section 2 FSA	Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA. With respect to OCI, there are two data centers located in the India region. Customers can select the region of their choice for object storage/physical storage of documents. Although Oracle is unable to accommodate SaaS customers with physical storage of documents in India, Oracle may assist those customers with obtaining third-party storage provider services.
Section 2(vi)	Banks should principally enter into arrangement with parties operating in jurisdictions that generally uphold confidentiality clauses and arrangements.	N/A	N/A	Section 14 CSA Section 8 FSA Section 4 Schedule C and CSA	Section 14 of the CSA sets forth the governing law and jurisdiction. Section 8 of the FSA sets out a contractual obligation to comply with applicable laws. Additionally, as described in Section 4 of Schedule C and the CSA , each party may disclose the other party's Confidential Information in any legal proceeding or to a governmental entity as required by law.
Section 2(vi)	Banks may not outsource to jurisdictions where access to books, records or any other information required for audit and review purposes may be impeded due to regulatory or administrative constraints.	N/A	N/A	Section 2 FSA	Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA. Section 2.5 of the FSA , which expressly states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law.
Section 2(vi)	Banks should clarify the jurisdiction for their data and applicable regulations at the outset of an outsourcing arrangement. This information should be reviewed periodically	N/A	N/A	Oracle Cloud Hosting and Delivery Policies	The Ordering Document or the cloud customer support portal states the data center region applicable to ordered Cloud services. Oracle and Oracle affiliates may have access to data while providing support and services subject to the

ORACLE

	and in case of significant changes performed by the service provider.			Ordering Document	Oracle Cloud Hosting and Delivery Policies , the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document , as applicable.
Section 2(vii)	These guidelines are generally applicable to outsourcing within a group conglomerate, including parent or Head Office, branch or group company, whether located within or outside India. The respective roles and responsibilities of each office in the outsourcing arrangement should be documented in a formal Service Level Agreement.	N/A	N/A	Section 3.1 and 3.2 Oracle Cloud Hosting and Delivery Policies	Service Availability and Service Level Agreements: Sections 3.1 and 3.2 of the Oracle Cloud Hosting and Delivery Policies as well as the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document , as applicable.

Cyber Security Framework in Banks (Reserve Bank of India, June 2, 2016) and Equivalent IRDAI Outsourcing Regulations and SEBI's Outsourcing Guidelines and Circulars

Requirement Reference	Regulation Requirement and Description	Equivalent IRDAI Outsourcing Regulations	Equivalent SEBI Outsourcing Guidelines and Circulars	Reference to Oracle Cloud Services Contract	Description of Oracle Practices
Section 10	Availability of the same, irrespective of whether the data is stored/in transit within themselves or with customers or with the third party vendors; the confidentiality of such custodial information should not be compromised at any situation and to this end, suitable systems and processes across the data/information lifecycle need to be in place by banks.	N/A	N/A	DPA Section 6 Section 1 Oracle Cloud Hosting and Delivery Policies Section 1 CSA Section 4 OMA Schedule C Section 4 CSA Section 5 OMA Schedule C Section 5 DPA Section 8	The Oracle Cloud services contract addresses the integrity, privacy and safety of customer content as follows: Technical and organizational security measures: <ul style="list-style-type: none">- Section 6 of the DPA (Security and Confidentiality)- Section 1 of the Oracle Cloud Hosting and Delivery Policies (Oracle Cloud Security Policy) Oracle's Corporate Security Practices: oracle.com/corporate/security-practices/ Confidentiality and protection of customer content:



					<ul style="list-style-type: none"> - Section 4 of the CSA or Section 4 of the OMA Schedule C (as applicable) – specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services) - Section 5 of the CSA or Section 5 of the OMA Schedule C (as applicable) - Section 8 of the DPA (Incident Management and Breach Notification) <p>Oracle Cloud Infrastructure Availability: https://ocistatus.oraclecloud.com/#/</p>
Annex 1, Section 2.3	Continuously monitor the release of patches by various vendors/OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply the security patch as per the patch management policy of the bank.	N/A	N/A	Section 4 Oracle Cloud Hosting and Delivery Policies	<p>Section 4 of the Cloud Hosting and Delivery Policies.</p>
Annex 1, Section 7.7	Periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between (i) different VLANs in the Data Centre (ii) LAN/WAN interfaces (iii) bank's network to external network and interconnections with partner, vendor and service provider networks are to be secure configured.	N/A	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices relating to access controls and patch management.</p> <p>Section 1.12 indicates that Oracle may conduct independent reviews of Cloud services utilizing third parties in the following areas (the scope of any such reviews may vary by service and country):</p> <ul style="list-style-type: none"> • SOC 1 (based on Statement on Standards for Attestation Engagements (SSAE) No 18) and/or SOC 2 reports • Other independent third-party security testing to review the effectiveness of administrative and technical controls. <p>Section 1.3 and 1.4 of the Oracle Cloud Hosting and Delivery Policies in particular sets out Oracle's system access controls and authentication processes.</p> <p>See Oracle Critical Patch Updates relating to on-prem/customer-managed components (including customer-managed components in the cloud) at</p>

					<p>https://www.oracle.com/corporate/security-practices/assurance/vulnerability/</p> <p>Oracle's Corporate Security Practices: oracle.com/corporate/security-practices/</p>
Annex 1, Section 10.1	Implement secure mail and messaging systems, including those used by bank's partners & vendors, that include measure to prevent email spoofing, identical mail domains, protection of attachments, malicious links, etc.	N/A	N/A	MyOracle Support: support.oracle.com/portal/	<p>MyOracle Support (MOS) is a secure messaging portal available to many Oracle customers.</p>
Annex 1, Section 11.1	Banks shall carefully evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment.	N/A	N/A	N/A	<p>Oracle provides several resources to assist its customers in conducting the necessary risk assessments and due diligence, which includes Consensus Assessment Initiative Questionnaires (CAIQs), audit reports and other information regarding Oracle's operational and security practices.</p> <ul style="list-style-type: none"> • Oracle Corporate Security Practices • Compliance documentation <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p> <p>Oracle Cloud Compliance Site: oracle.com/corporate/cloud-compliance/</p> <p>OCI CAIQ: oracle.com/a/ocom/docs/oci-corporate-caiq.pdf</p> <p>Oracle Fusion Cloud Applications CAIQ: oracle.com/a/ocom/docs/caiq-oracle-fusion-cloud-applications.pdf</p> <p>Oracle Enterprise Performance Management Cloud Applications CAIQ: oracle.com/a/ocom/docs/caiq-oracle-epm-cloud-applications.pdf</p>



					<p>Oracle Cloud Applications CAIQ: oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf</p> <p>Audit Reports: customers can obtain more information about available audit reports by contacting their Oracle sales representative</p>
Annex 1, Section 11.5	Banks shall ensure and demonstrate that the service provider (including another bank) adheres to all regulatory and legal requirements of the country. Banks may necessarily enter into agreements with the service provider that amongst others provides for right to audit by the bank and inspection by the regulators of the country.	N/A	N/A	Section 2 FSA Section 8 DPA	<p>Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA.</p> <p>Section 8 of the DPA sets out Oracle's incident management and breach notification obligations.</p>
Annex 1, Section 11.6	Reserve Bank of India shall have access to all information resources (online/in person) that are consumed by banks, to be made accessible to RBI officials by the banks when sought, though the infrastructure/enabling resources may not physically be located in the premises of banks.	N/A	N/A	Section 2 of FSA	<p>Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA.</p>
Annex 1, Section 11.7	Banks have to adhere to relevant legal and regulatory requirements related to geographical location of infrastructure and movement of data out of borders.	N/A	N/A	Section 5 DPA Ordering Document	<p>Section 5 of the DPA, which addresses cross-border transfer of data.</p> <p>OCI customers select their own region.</p> <p>The region is specified in the Ordering Document for SaaS customers.</p> <p>Oracle Cloud Infrastructure Regions:</p> <p>https://www.oracle.com/cloud/data-regions/ for a list of Oracle Global Infrastructure Regions</p>



Annex 1, Section 11.8	Banks shall thoroughly satisfy about the credentials of vendor/third-party personnel accessing and managing the bank's critical assets.	N/A	N/A	Section 1.4 Oracle Cloud Hosting and Delivery Policies	Section 1.4 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle personnel access to the Services environment for the Cloud Services (including Your Content residing in the Cloud Services), Oracle enforces Role Based Access Controls (RBAC) and employs the access management principles of "need to know", "least privilege" and "segregation of duties."
Annex 1, Section 11.9	Background checks shall be mandated for all third party service providers	N/A	N/A	N/A	Part A, Section A1 of the Oracle Supplier Information and Physical Security Standards provides that unless prescribed otherwise in the agreement, Supplier will perform background checks, consistent with local laws and regulations, for all personnel. See: https://www.oracle.com/us/corporate/supplier/oracle-supplier-contractor-security-070672.pdf
Annex 1, Section 11.9	Non-disclosure agreement shall be mandated for all third- party service providers.	N/A	N/A	Section 4 CSA and Schedule C	Section 4 of the CSA and Schedule C states that each party may only share Confidential Information with subcontractors who are required to protect it against unauthorized disclosure in a manner no less protective than required under the Agreement.
Annex 1, Section 11.9	Security policy compliance agreement shall be mandated for all third-party service providers.	N/A	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies	Section 1 of the Oracle Cloud Hosting and Delivery Policies describes Oracle's information security practices including physical security safeguards, system and data access controls, encryption, and training.
Annex 1, Section 15.1 through 15.3	15.1 Develop a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information. 15.2 This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline. 15.3 Similar arrangements need to be ensured at the vendor managed facilities as well.	N/A	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies Section 6 DPA	Section 1 of the Oracle Cloud Hosting and Delivery Policies describes Oracle's information security practices including physical security safeguards, system and data access controls, encryption and training. Section 6 of the DPA sets out Oracle's obligation to implement and maintain appropriate technical and organisational security measures for the processing of personal information designed to prevent accidental or unlawful destruction, loss, alteration and unauthorised access or disclosure.

ORACLE

Annex 1, Section 19.5	Banks shall ensure such capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative & coordinated resilience testing that meet the bank's recovery time objectives.	N/A	N/A	N/A	The Risk Management Resiliency Program (RMRP) addresses Oracle's internal testing processes that are performed by Oracle. Additionally, Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. See: oracle.com/corporate/security-practices/corporate/resilience-management/disaster-recovery.html
Annex 1, Section 19.6(a)	Define incidents, method of detection, methods of reporting incidents by employees, vendors and customers and periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type, allocate and communicate clear roles and responsibilities of personnel manning/handling such incidents, provide specialised training to such personnel, post incident review, periodically test incident response plans.	N/A	N/A	Section 8 DPA	Section 8 of the DPA sets out Oracle's incident management and breach notification obligations.
Annex 1, Section 20.1	Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all-delivery channels.	N/A	N/A	Oracle Cloud Hosting and Delivery Policies	This obligation does not apply to the cloud services provider. However, Oracle encourages customers to consider Oracle Cloud Hosting and Delivery Policies .

Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks (Reserve Bank of India, November 3, 2006) and Equivalent IRDAI Outsourcing Regulations and SEBI's Outsourcing Guidelines and Circulars

REQUIREMENT REFERENCE	REGULATION REQUIREMENT/DESCRIPTION	EQUIVALENT IRDAI OUTSOURCING REGULATIONS	SEBI'S OUTSOURCING GUIDELINES AND CIRCULARS	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT	DESCRIPTION OF ORACLE PRACTICES
Section 5.5.1	The contract should clearly define what activities are going to be outsourced including appropriate service and performance standards.	N/A	N/A	CSA Ordering Document	Written Oracle Cloud services contract and referenced Service Specifications.

ORACLE

Section 5.5.1	The bank must ensure it has the ability to access all books, records and information relevant to the outsourced activity available with the service provider.	N/A	N/A	Section 2 FSA	<p>Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA.</p> <p>Where required by applicable law, including where mandated by a customer's regulator, such regulators may perform audits. The customer will promptly provide Oracle with written notice, identifying the applicable services agreement and service, and provide evidence of the regulatory notice for such an audit</p>
Section 5.5.1	The contract should provide for continuous monitoring and assessment by the bank of the service provider so that any necessary corrective measure can be taken immediately.	N/A	N/A	<p>Section 3.2.2 Oracle Cloud Hosting and Delivery Policies</p> <p>Section 11 Schedule C</p> <p>Section 11 Schedule CSA</p>	<p>Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability.</p> <p>Section 11.1 of Schedule C and the CSA, as applicable, explains that Oracle also monitors the Cloud services.</p>
Section 5.5.1	A termination clause and minimum periods to execute a termination provision, if deemed necessary, should be included.	N/A	N/A	<p>Section 3 of FSA</p> <p>Section 9.3 of Schedule C</p> <p>Section 9.4 of the CSA</p>	<p>Section 3 of the FSA expressly permits termination with applicable notice periods.</p> <p>Please also see Section 9.3 of Schedule C and Section 9.4 of the CSA, as applicable, which provides a termination right in the event of a breach of a material term of the Agreement.</p>
Section 5.5.1	The agreement should include controls to ensure customer data confidentiality and service providers liability in case of breach of security and leakage of confidential customer related information.	N/A	N/A	<p>Section 1 of Oracle Cloud Hosting and Delivery Policies</p> <p>Section 4 Schedule C and CSA</p> <p>Section 5 of Schedule C and CSA</p> <p>Sections 6 and 8 DPA</p>	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle's security practices. Section 1.5 of the Oracle Cloud Hosting and Delivery Policies in particular sets out Oracle's use of encryption technology.</p> <ul style="list-style-type: none"> • Confidentiality and Protection of "Your Content": <ul style="list-style-type: none"> - Section 4 of Schedule C and of the CSA, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services). - Section 5 of Schedule C and of the CSA, as applicable

					<p>Section 6 of the DPA sets out Oracle's obligation to implement and maintain appropriate technical and organisational security measures for the processing of personal information designed to prevent accidental or unlawful destruction, loss, alteration and unauthorised access or disclosure.</p> <p>Section 8 of the DPA sets out Oracle's incident management and breach notification obligations.</p>
Section 5.5.1	The agreement should include contingency plans to ensure continuity.	N/A	Annexure I, Section 5.2(g) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract specifies the responsibilities of the third party with respect to contingency plans.	Section 5 FSA Section 2 Oracle Cloud Hosting and Delivery Policies	<p>Section 5 of the FSA 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>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.</p>
Section 5.5.1	The contract should provide for the prior approval/consent by the bank of the use of subcontractors by the service provider for all or part of an outsourced activity.	N/A	Section 2(v) of Circular on Outsourcing by Depositories - Depositories shall ensure that outsourced activities are further outsourced downstream only with the prior consent of the depository and with appropriate safeguards including proper legal documentation/agreement.	Section 4.1 DPA Section 6.1 FSA Section 6.2 FSA Section 14.2 Schedule C Section 17.2 CSA	<p>Section 4.1 of the DPA indicates 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 Oracle Cloud services contract. This section also indicates that Oracle is responsible for the performance of the Oracle affiliates and third-party subprocessors' obligations in compliance with the terms of the Oracle Data Processing Agreement and Applicable Data Protection Law.</p> <p>Sections 6.1 to 6.2 of the FSA include terms applicable to Oracle's use of subcontractors and strategic subcontractors, and similar to the Oracle Data Processing Agreement, includes a right for a customer to object to the intended involvement of a new strategic subcontractor.</p> <p>Section 6.1 of the FSA further 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</p>

ORACLE

					<p>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>Section 14.2 of Schedule C and Section 17.2 of the CSA, as applicable.</p>
Section 5.5.1	Provide the bank with the right to conduct audits on the service provider whether by its internal or external auditors, or by agents appointed to act on its behalf and to obtain copies of any audit or review reports and finding made on the service provider in conjunction with the services performed for the bank.	N/A	N/A	Section 2 FSA	Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA.
Section 5.5.1	Outsourcing agreements should include clauses to allow the Reserve Bank of India or persons authorised by it to access the bank's documents, records of transactions, and other necessary information given to, stored, or processed by the services provider within a reasonable time.	N/A	N/A	Section 2 FSA	Section 2 of the FSA grants customer's financial services regulator audit rights to the extent required by applicable law and as specified in the FSA.
Section 5.5.1	Outsourcing agreement should also include clause to recognise the right of Reserve Bank to cause an inspection to be made of a service provider of a banks and its books and account by one or more of its officers or employees or other persons.	N/A	N/A	Section 2 FSA	Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA.
Section 5.5.1	In cases where the controlling/Head offices of foreign banks operating in India outsource the activities related to the Indian operations, the Agreement should include clauses	N/A	N/A	Section 2 FSA	Section 2 of the FSA grants customer's financial services regulator audit rights to the extent required by applicable law and as specified in the FSA, which is limited to audits of operational security processes.

	to allow the RBI or persons authorized by it to access the bank's documents, records of transactions and other necessary information given or stored or processed by the service provider within a reasonable time as also clauses to recognise the right of RBI to cause an inspection to be made of a service provider and its books and accounts by one or more of its officers or employees or other persons.				
Section 5.5.1	The outsourcing agreement should also provide that confidentiality of customer's information should be maintained even after the contract expires or gets terminated.	N/A	N/A	Section 4 Schedule C Section 4 CSA	Section 4 of Schedule C and CSA , as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services).
Section 5.5.1	The outsourcing agreement should provide for the preservation of documents and data by the service provider in accordance with the legal/regulatory obligation of the bank this regard.	N/A	Annexure I, Section 5.2(h) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract provides for preservation of the documents and data by third party.	Section 6 DPA Sections 4 and 5 Schedule C Section 4 and 5 CSA	Section 6 of the DPA sets out Oracle's obligation to implement and maintain appropriate technical and organisational security measures for the processing of personal information designed to prevent accidental or unlawful destruction, loss, alteration and unauthorised access or disclosure. Confidentiality and Protection of "Your Content": Section 4 of Schedule C and Section 4 of the CSA , as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services) Section 5 of Schedule C and of the CSA , as applicable.
Section 5.6.2	Access to customer information by staff of the service provider should be one 'need to know' basis i.e., limited to those areas where the information is required in order to perform the outsourced function.	N/A	N/A	Section 1.4 Oracle Cloud Hosting and Delivery Policies	Section 1.4 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy which describes Oracle personnel access to the Services environment for the Cloud Services (including Your Content residing in the Cloud Services), Oracle enforces Role Based Access Controls (RBAC) and employs the access management principles of "need to know", "least privilege" and "segregation of duties."
Section 5.6.3	The bank should ensure that the service provider is able to isolate	N/A	N/A	Section 6 and 8 DPA	Please refer to:

ORACLE

	<p>and clearly identify the bank's customer information, documents, records and assets to protect the confidentiality of the information. In instances, where service provider acts as outsourcing agent for multiple banks, care should be taken to build strong safeguards so that there is no comingling of information/documents, records and assets.</p>			<p>Oracle Cloud Hosting and Delivery Policies Section 4 and 5 of Schedule C and CSA</p>	<ul style="list-style-type: none"> • Technical and organization security measures: <ul style="list-style-type: none"> - Section 6 of the DPA - the Oracle Cloud Hosting and Delivery Policies as well as the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, as applicable. - Oracle Corporate Security Practices • Confidentiality and Protection of "Your Content": <ul style="list-style-type: none"> - Section 4 of Schedule C and CSA, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services) - Section 5 of Schedule C and the CSA, as applicable - Section 8 of the DPA sets out Oracle's incident management and breach notification obligations. <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p>
Section 5.6.4	The bank should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches.	N/A	N/A	<p>Section 1 Oracle Cloud Hosting and Delivery Policies Section 8 DPA</p>	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies describes Oracle's information security practices including physical security safeguards, system and data access controls, encryption, and training.</p> <p>Section 8 of the DPA sets out Oracle's incident management and breach notification obligations.</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p>
Section 5.8.1	A bank should require its service providers to develop and establish a robust framework for documenting, maintaining, and testing business continuity and recovery procedures. Banks need to ensure that the service provider periodically tests the Business Continuity and Recovery Plan and may also consider occasional joint testing	N/A	N/A	<p>Section 5 FSA Section 2 Oracle Cloud Hosting and Delivery Policies</p>	<p>Section 5 of the FSA 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>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.</p>

	and recovery exercise with its service provider.				Section 4 of the PaaS/IaaS Cloud Services Pillar Document and Section 2 of the SaaS Cloud Services Pillar Document also addresses cloud service continuity.
Section 5.8.2	In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, banks should retain an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of the bank and its services to the customers.	N/A	N/A	Section 6.1 Oracle Cloud Hosting and Delivery Policies Section 4 FSA	Section 6.1 of the Oracle Cloud Hosting and Delivery Policies states Oracle will make content available in a structured, machine-readable format for retrieval by the customer for a specified period post-termination (retrieval period). Upon expiry of the retrieval period, Oracle will delete the content from the services unless otherwise required by applicable law. Section 4 of the FSA provides customers with the ability to order transition services and transition assistance to facilitate the transfer or the re-incorporation of the concerned function back to the customer or to a third-party provider.
Section 5.8.4	The bank should ensure that the service providers ensure that service providers are able to isolate the bank's information, documents and records, and other assets. This is to ensure that in adverse conditions, all documents, records of transactions and information given to the service provider, and assets of the bank, can be removed from the possession of service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.	N/A	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	Customers' termination rights are set out in Section 9 of the CSA or Section 9 of the OMA Schedule C (as applicable) and in Section 3 of the FSA . Section 6.1 of the Oracle Cloud Hosting and Delivery Policies states Oracle will make content available in a structured, machine-readable format for retrieval by the customer for a specified period post-termination (retrieval period). Upon expiry of the retrieval period, Oracle will delete the content from the services unless otherwise required by applicable law. Section 4.3 of the FSA addresses customers who require assistance with a transition. Section 9.1 of the DPA 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.
Section 5.9.1	The bank should ensure that outsourcing agreements with the service provider contain provisions	N/A	Annexure I, Section 5.2(d) (Guidelines on Outsourcing of	Section 3.2.2 Oracle Cloud Hosting and Delivery Policies	Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability.

ORACLE

	to address their monitoring and control of outsourced activities.		Activities by Intermediaries) - Outsourcing contract provides for continuous monitoring and assessment by the intermediary of the third party so that any necessary corrective measures can be taken up immediately, i.e., the contract shall enable the intermediary to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations.	Section 11 Schedule C and CSA	Section 11.1 of Schedule C and of the CSA , as applicable, explains that Oracle also continuously monitors the Cloud services.
Section 5.9.3	Regular audits by either internal or external auditors of the bank should assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement, the bank's compliance with its risk management framework and the requirements of these guidelines.	N/A	N/A	Section 2 FSA	Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA.
Section 5.9.4	Banks should at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider should highlight any deterioration or breach in performance standards, confidentiality, and security, and in business continuity preparedness.	N/A	N/A	N/A	<p>This obligation does not apply to the Cloud services provider; however, 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 including the following:</p> <ul style="list-style-type: none"> • Oracle security practices • Compliance documentation

					<p>Customers can access these materials via the Oracle Compliance Site located at oracle.com/corporate/cloud-compliance/</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p> <p>Also see:</p> <p>Oracle corporate: oracle.com/corporate</p> <p>Oracle annual reports: investor.oracle.com/sec-filings/default.aspx</p> <p>Oracle financials: investor.oracle.com/financials/default.aspx</p>
Section 5.9.5	In the event of termination of the agreement for any reason this should be publicized as to ensure that the customers do not continue to entertain the service provider.	N/A	N/A	Termination Rights: Section 9 CSA and Schedule C Section 3 FSA	This obligation does not apply to the cloud services provider; however, Oracle encourages customers to consider our customers' termination rights, which are set out in Section 9 of the CSA or Section 9 of the OMA Schedule C (as applicable) and in Section 3 of the FSA .
Section 7.1	With respect to engagement of service providers in a foreign country, in principle, arrangements should only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements.	N/A	N/A	Section 6 DPA Section 4 CSA and Schedule C Section 5 CSA and Schedule C	<p>Section 6 of the DPA sets out Oracle's obligation to implement and maintain appropriate technical and organisational security measures for the processing of personal information designed to prevent accidental or unlawful destruction, loss, alteration and unauthorised access or disclosure.</p> <p>Section 4 of the CSA and Schedule C, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services).</p> <p>Section 5 of the CSA and Schedule C, as applicable.</p>
Section 7.2	The activities outsourced outside of India should be conducted in a manner so as not to hinder efforts to supervise or reconstruct the India activities of the bank in a timely manner.	N/A	N/A	Section 2 FSA	<p>Section 2 of the FSA grants customer's financial services regulator audit rights as required by applicable law and as specified in the FSA.</p> <p>Where required by applicable law, including where mandated by a customer's regulator, such regulators may perform audits. The customer will promptly</p>

					provide Oracle with written notice, identifying the applicable services agreement and service, and provide evidence of the regulatory notice for such an audit.
--	--	--	--	--	---

Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBS) (Reserve Bank of India, October 19, 2018) and Equivalent IRDAI Outsourcing Regulations and SEBI Outsourcing Guidelines and Circulars

Requirement Reference	Regulation Requirement and Description	Equivalent IRDAI Outsourcing Guidelines	Equivalent SEBI Outsourcing Guidelines and Circulars	Reference to Oracle Cloud Services Contract	Description of Oracle Practices
Section 7	UCBs, as owners of customer sensitive data, should take appropriate steps in preserving Confidentiality, Integrity, and Availability of the same, irrespective of whether the data is stored/in transit within themselves or with third party vendors; the confidentiality of such custodial information should not be compromised in any situation.	N/A	N/A	N/A	<p>Please refer to:</p> <ul style="list-style-type: none"> • Technical and organization security measures: <ul style="list-style-type: none"> - Section 6 of the DPA - the Oracle Cloud Hosting and Delivery Policies as well as the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, as applicable. - Oracle Corporate Security Practices • Confidentiality and Protection of "Your Content": <ul style="list-style-type: none"> - Section 4 of Schedule C and CSA, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services) - Section 5 of Schedule C and the CSA, as applicable - Section 8 of the DPA sets out Oracle's incident management and breach notification obligations. <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p>
Section 8.1	Implement secure mail and messaging systems including those used by UCB'S partners and	N/A	N/A	N/A	<u>MyOracle Support</u> (MOS) is a secure messaging portal available to many Oracle customers.

ORACLE

	vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.				
Annex 1, Section 13.1	All the outsourcing service level agreement (SLAs) signed with the vendors must clearly mention the responsibility of the UCB and vendor in case of any failure of services.	N/A	N/A	Sections 3.1. and 3.2 Oracle Cloud Hosting and Delivery Policies	<p>Service Availability and Service Level Agreements:</p> <p>Sections 3.1 and 3.2 of the Oracle Cloud Hosting and Delivery Policies, as well as the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, as applicable.</p> <p>Also see the OCI Status Site: https://ocistatus.oraclecloud.com/#/</p>
Annex 1, Section 13.2	The agreements must clearly mention the grievance redressal mechanism to resolve customer complaints.	No equivalent	No equivalent	Section 5 Oracle Cloud Hosting and Delivery Policies	<p>Section 5 of the Oracle Cloud Hosting and Delivery Policies describes the Oracle Cloud Support Policy, which is provided by Oracle as part of such Oracle Cloud Services and can be utilized by customers to raise issues relating to their cloud services.</p> <p>Oracle support for Oracle Cloud Services consists of:</p> <ul style="list-style-type: none"> • Diagnoses of problems or issues with the Oracle Cloud Services • Reasonable commercial efforts to resolve reported and verifiable errors in the Oracle Cloud Services so that those Oracle Cloud Services perform in all material respects as described in the associated Program Documentation • Support during Change Management activities described in the Oracle Cloud Change Management Policy • Assistance with technical service requests 24 hours per day, 7 days a week • 24 x 7 access to a Cloud Customer Support Portal designated by Oracle (e.g., My Oracle Support) and Live Telephone Support to log service requests • Access to community forums • Non-technical Customer service assistance during normal Oracle business hours (8:00 to 17:00) local time
Annex 1, Section 13.3	Vendors' service level agreements shall be periodically reviewed for performance in security controls.	N/A	N/A	Section 1 Oracle Cloud Hosting and Delivery Policies	<p>Section 1 of the Oracle Cloud Hosting and Delivery Policies describes Oracle's information security practices including physical security safeguards, system and data access controls, encryption and training.</p>



N/A	N/A	N/A	Annexure I, Section 2.4 (Guidelines on Outsourcing of Activities by Intermediaries) - The intermediary shall review the financial and operational capabilities of the third party in order to assess its ability to continue to meet its outsourcing obligations.	N/A	<p>This obligation does not apply to the Cloud services provider; however, 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 including the following:</p> <ul style="list-style-type: none"> • Oracle security practices • Compliance documentation <p>Customers can access these materials via the Oracle Compliance Site</p> <p>Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/</p> <p>Oracle Cloud Compliance: oracle.com/corporate/cloud-compliance/</p>
N/A	N/A	N/A	Annexure I, Section 3.3 (Guidelines on Outsourcing of Activities by Intermediaries) - The facilities /premises/data that are involved in carrying out the outsourced activity by the service provider shall be deemed to be those of the registered intermediary. The intermediary itself and Regulator or the persons authorized by it shall the right to access the same at any point of time.		Sections 1 and 2 of the FSA set out Oracle's obligations regarding customer and customer regulators' audit rights.
N/A	N/A	N/A	Annexure I, Section 5.2(g) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract specifies the	Oracle Cloud services contract Ordering Document	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.

			responsibilities of the third party with respect to insurance cover.		Oracle can specify applicable insurance coverage and limits in the Ordering Document
N/A	N/A	N/A	Annexure I, Section 5.2(g) (Guidelines on Outsourcing of Activities by Intermediaries) - Outsourcing contract specifies the responsibilities of the third party with respect to force majeure clause.	Section 13 CSA	Section 13 of the CSA addresses force majeure.
N/A	N/A	N/A	Annexure I, Section 6.4 (Guidelines on Outsourcing of Activities by Intermediaries) - Periodic tests of critical security procedures and systems and review of the back-up facilities shall be undertaken by the intermediary to confirm adequacy of the third party's systems. Section 9 (Circular on Outsourcing Activities by Stock Exchanges and Clearing Corporations) – Stock exchanges and clearing corporations should take appropriate measures to determine that its service providers/Outsourcing agencies establish and maintain emergency procedures and plan for business continuity/disaster recovery, with periodic testing of backup facilities.	Section 5 FSA Section 2 Oracle Cloud Hosting and Delivery Policies	Section 5 of the FSA indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Section 2 of the Oracle Cloud Hosting and Delivery Policies sets out Oracle Cloud Service Continuity Policy, which describes Oracle Cloud Services High Availability Strategy and Oracle Cloud Services Backup Strategy.
N/A	N/A	N/A	Annexure I, Section 7.3 (Guidelines on	Section 1 Oracle Cloud Hosting and Delivery Policies	Section 1 of the Oracle Cloud Hosting and Delivery Policies describes Oracle's information security practices



			Outsourcing of Activities by Intermediaries) - In cases where the third party is providing similar services to multiple entities, the intermediary shall ensure that adequate care is taken by the third party to build safeguards for data security and confidentiality.		including physical security safeguards, system and data access controls, encryption, and training. Oracle Corporate Security Practices Site: https://www.oracle.com/corporate/security-practices/
N/A	N/A	N/A	Section 2(vi) (Circular on Outsourcing by Depositories) - Depositories shall ensure that risk impact analysis is undertaken before any activity and appropriate risk mitigation measures like back up/restoration system are in place.	Section 2 Cloud Hosting and Delivery Policies	Section 2 of the Oracle Cloud Hosting and Delivery Policies sets out Oracle Cloud Service Continuity Policy, which describes Oracle Cloud Services High Availability Strategy and Oracle Cloud Services Backup Strategy.
N/A	N/A	N/A	Section 2(vii) (Circular on Outsourcing by Depositories) - Depositories shall strive to automate their processes and workflows to the extent possible which shall enable real time monitoring of outsourced activities.	N/A	Customers can also get real time notifications through the following: <ul style="list-style-type: none"> OCI Status: https://ocistatus.oraclecloud.com/ Fusion Cloud Applications: https://saasstatus.oracle.com/ <u>MyOracle Support</u> (MOS) is a secure messaging portal available to many Oracle customers.
N/A	N/A	N/A	Section 3.5 (Circular on Outsourcing Activities by Stock Exchanges and Clearing Corporations) In case the trading and/or clearing software is purchased from a vendor, then there must be an arrangement to keep the source code in escrow, such that in any case of any issue with the vendor, the software can be taken	Ordering Document	With respect to on premise software, a source code provision may be added to the Ordering Document, which would specify where a copy of the source code necessary to support the applicable Oracle programs is maintained or that the source code that will be placed into escrow.



			out of escrow and used to continue business.		
N/A	N/A	N/A	Section 7.1 (Circular on Outsourcing activities by Stock Exchanges and Clearing Corporations) Contractual terms and conditions governing relationships, functions, obligations and responsibilities of contracting parties, potential conflict of interests should be carefully and properly defined in written agreements.	CSA Ordering Document	<p>Written Oracle Cloud services contract and referenced Service Specifications.</p> <p>Oracle will work with the customer during the contracting process to address the insertion language in the agreement with respect to potential conflicts of interests.</p>
N/A	N/A	Section 11 (iii) The insurer shall ensure that the outsourcing service provider shall not sub-contract the whole or a substantial portion of the Outsourced activity. Where sub-contracting is allowed partially it should be with the prior consent of the Insurer and the additional risk which flows due to subcontracting shall be factored in at the time of due diligence.	N/A	Sections 6.1 and 6.2 FSA Section 4.1 DPA	<p>Sections 6.1 to 6.2 of the FSA include terms applicable to Oracle's use of subcontractors and strategic subcontractors, and similar to the Section 4.1 of the DPA. Oracle customers provide general approval of the engagement of subcontractors and subprocessors.</p>
N/A	N/A	Section 14(iv) All the outsourcing service providers engaged by insurers are subject to the provisions of the Insurance Act, 1938, IRDA Act 1999, Rules, Regulations and any other order issued thereunder.	N/A	Section 8 FSA	<p>Section 8 of the FSA sets out a contractual obligation to comply with applicable laws.</p>

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

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