ORACLE

Business / Technical Brief

Advisory: Oracle Cloud Application Services and Select India Financial Services Regulations, Guidance and Circulars

Addressing a selection of India regulations, guidance, and circulars for Financial Services Companies when Using Oracle Cloud Application Services

March 2023, Version 1.0

Disclaimer

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

This document is for informational purposes only and is intended solely to assist you in assessing your use of Oracle Cloud application services in the context of the requirements applicable to you as a financial institution under the Reserve Bank of India (RBI), Insurance Regulatory and Development Authority (IRDAI) and Securities and Exchange Board of India (SEBI) guidelines, regulations, and circulars (collectively, the "India Regulatory Framework"). This may also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document. The information in this document is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

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

The India Regulatory Framework referenced in this document are subject to periodic changes or revisions by the applicable regulatory authority. The current versions of the India Regulatory Framework referenced in this document are available at the websites listed below. This document is based on information available at the time of creation, it is subject to change at the sole discretion of Oracle Corporation and may not always reflect changes in the regulations.

- Reserve Bank of India (RBI)
- Insurance Regulatory and Development Authority (IRDAI)
- Securities and Exchange Board of India (SEBI)

Table of Contents

Introduction

The Reserve Bank of India (RBI), India's central banking institution, the Insurance Regulatory and Development Authority of India (IRDAI), and the Securities and Exchange Board of India (SEBI), are among the main financial services industry regulators protecting the interests of investors in India and overseeing financial institutions, including banks, insurance organizations, and securities market.

Some of the most relevant guidelines, regulations and circulars pertaining to cyber security, outsourcing arrangements, and risk management in India's financial services sector, include:

- Guidelines on Managing Risk and Code of Conduct in Outsourcing of Financial Services by Banks (RBI)
- Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds (RBI).
- Outsourcing of Activities by Indian Insurers Regulation (IRDAI), providing insurers with a legal framework for assessing and managing risks associated with outsourcing arrangements
- Cyber Security Framework in Banks (2016) (RBI)
- Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) (2018) (RBI)
- 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)
- Circular on Outsourcing of Activities by Stock Exchanges and Clearing Corporations (Securities and Exchange Board of India, 2017)

Purpose

This document is intended to provide relevant information related to Oracle Cloud Application Services to assist you in determining the suitability of using Oracle Cloud Application Services in relation to RBI,IRDAI, and SEBI regulatory requirements and guidance and should be read in conjunction with Oracle Contract Checklist for India.

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

About Oracle Cloud

Oracle's mission is to help people see data in new ways, discover insights, and unlock endless possibilities. Oracle provides a number of cloud solutions tailored to customers' needs. These cloud offerings provide customers the benefits of the cloud including global, secure, and high-performance environments to run all their workloads. The cloud offerings discussed in this document include Oracle Cloud Applications (SaaS)[1].

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

The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On-premises customers are in full control of their technology infrastructure. For example, they have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers use components that are partially under the management of the cloud service providers. As a result, the management of security in the cloud is a shared responsibility between the cloud customers and the cloud service provider.

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

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

[1] Note that Oracle GBU SaaS, Netsuite and Advertising SaaS Services are not included in the scope of this document.

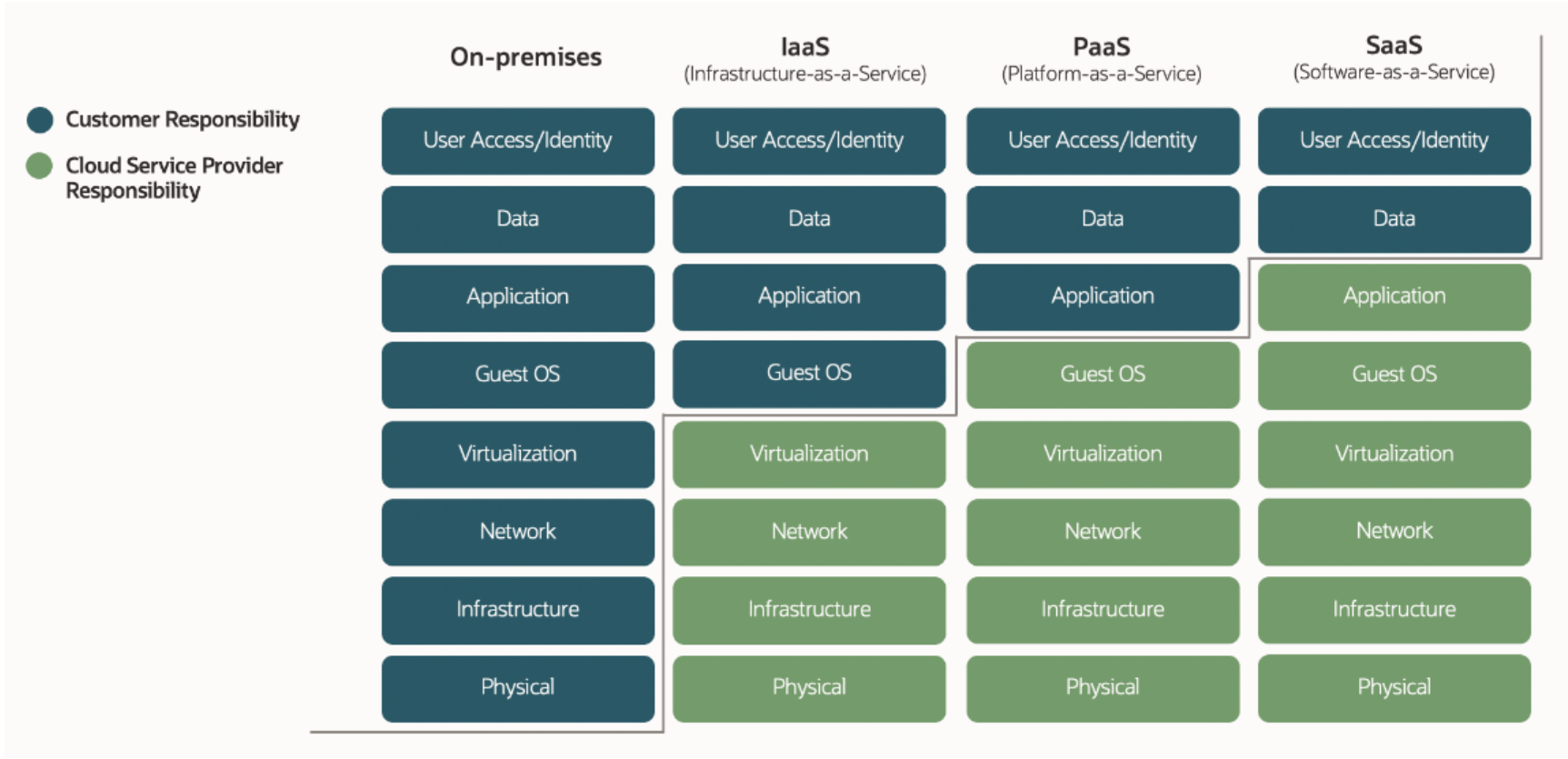

Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers

Overview of RBI, IRDAI, and SEBI Requirements

This section provides an overview of key regulatory considerations specified by RBI, IRDAI, and SEBI, that regulated financial services customers should consider.

Customers are responsible for determining the suitability of a cloud service in the context of these requirements for their needs. Customers are also responsible for ensuring that their use of the cloud service and business processes meet these requirements.

However, Oracle provides the following features and functions, which may help you in meeting these requirements.

There are two parts to this section:

Part 1 - Explains some key points to note about Oracle and Oracle Cloud Solutions in relation to RBI, IRDAI and SEBI requirements

Part 2 - Respond to key requirements of the India Regulatory Framework, describing SaaS Operational and Security practices and services.

PART 1 - Key Points You Should Know About Oracle and Oracle Cloud Solutions

Is Oracle a regulated entity under the supervision of RBI, IRDAI, and SEBI?

No. Oracle is not under the direct supervision of RBI, IRDAI or SEBI. However, Oracle is committed to helping regulated customers meet their regulatory objectives. Oracle may assist regulated customers by providing some of the information and resources that may be essential to the regulated customer's ability to satisfy their regulatory and compliance requirements.

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

Yes. In addition to its comprehensive cloud hosting and delivery, data protection, and security contract terms, Oracle offers the Financial Services Addendum (FSA) as an add-on to the Oracle Cloud Service Agreement. The FSA addresses various topics typically requested by regulated entities in the Financial Services sector, such as audit rights (for customers and their regulators), termination rights, exit provisions and transition services, and business continuity and sub-outsourcing obligations.

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

Oracle cloud services typically handle two types of customer data:

- Customer account information that is needed to operate the customer's cloud account. This information is primarily used for customer account management, including billing. Oracle is a controller with regard to the use of any personal information that it gathers from the customer for purposes of account management and handles such information in accordance with the terms of the Oracle General Privacy Policy.

- Customer content that customers choose to store within Oracle cloud services, which may include personal information gathered from the customer's individuals or data subjects, such as its users, end customers, or employees.

It is important to note that Oracle does not have a direct relationship with the customer's individuals or data subjects. The customer is the controller in these situations and is responsible for their data collection and data use practices. Oracle is the processor that acts on the instructions of the customer and handles personal information contained in customer content in accordance with the general processing terms of the Oracle Services Privacy Policy and the Oracle Data Processing Agreement. Oracle, as a data processor, among other things, provides customers appropriate technical and organizational measures that have been designed to protect customer personal data against risks associated with unauthorized processing, including advanced security controls and external audit certifications. Oracle also maintains an incident management and data breach notification framework.

Where is customers' data located?

Oracle operates within various regions across the globe. Data centre regions are composed of one of more physically isolated and fault-tolerant data centres (also called availability domains). Customers choose a data centre region during their initial Oracle account setup in an ordering document. This initially determines their data tenancy's location.

Does Oracle have access to customer's content?

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

Break Glass, available only for a number of Oracle Applications including Oracle HCM Cloud Service, Oracle CRM Cloud Service, and Oracle ERP Cloud Service, provides additional security by restricting administrative access to systems and services. As such, Oracle Support representatives can access a customer's cloud environment only after relevant approvals and authorization to troubleshoot any issues that may arise in the cloud environment has been obtained. For more information, see Oracle Break Glass,

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

Oracle provides secure and reliable product offerings and services and prioritizes protecting the integrity and security of products and services. Oracle cloud services are designed and operated following a defense-in-depth model. This model starts with a default-deny is a network-oriented configuration approach that denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source network address, and destination network address. As a result, tenants are isolated from one another and from Oracle.

Access controls are implemented to govern access to and use of resources. Examples of resources include a cloud service, physical server, file, application, , a table in a database, and a network device. These controls include following a least-privilege model is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.

How does Oracle manage availability risks?

Oracle deploys its cloud services on a resilient computing infrastructure designed to maintain service availability and continuity if an adverse event affects the services. Oracle cloud service data centres align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. These data centres housing Oracle cloud infrastructure services use redundant power sources and maintains generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.

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

How does Oracle handle security incidents?

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

Does Oracle provide audit rights to customers and their regulators?

Yes. Customers and their regulators have the right to access and audit Oracle's compliance with its obligations under their cloud services agreement as specified in the FSA. In addition, Oracle grants its customers and their regulators the same rights of access and audit of Oracle strategic subcontractors. Such audit rights and related terms are covered by the FSA.

What compliance documentation does Oracle provide?

Oracle provides information about frameworks for which an Oracle LoB has achieved a third-party attestation or certification for one or more of its services in the form of "attestations". These attestations can assist in your compliance and reporting, providing independent assessment of the security, privacy, and compliance

controls of the applicable Oracle cloud services. Such attestations include CSA Star, SOC, and ISO/IEC 27001, 27017, and 27018.it is important that you consider they are generally specific to a certain cloud service and may also be specific to a certain data centre or geographic region.

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

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

PART 2 SUMMARY OF INDIA REGULATORY FRAMEWORK This section include general summaries and excerpts from some of the most relevant India Regulatory Framework pertaining to cloud operations and security and describes SaaS operational and security practices and services.

REFERENCE	REGULATORY TOPIC	DESCRIPTION	ORACLE GUIDANCE	ORACLE RESOURCES
RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, Chapter 2, Section 30(a)	Penetration Testing	Penetration testing needs to be conducted at least on an annual basis.		Oracle Cloud Security Testing Policy.
RBI Guidelines on Information Security, Electronic Banking,	Contractual Agreement	Outsourcing arrangements shall be governed by written agreements/contracts that clearly describe all the material aspects of the		**Oracle Cloud Services Contracts:** oracle.com/corporate/contracts/cloudservices/contracts.html

				Oracle Contract Checklist for India: (https://www.oracle.com/uk/a/ocom/docs/india-checklist-9-14-22.pdf) **Data Processing Agreement (DPA):** DPA for Oracle services

			• Assistance with regulatory obligations, including the provision of necessary information requested by the customer's competent authority **The Data Processing Agreement (DPA) for Oracle Services covers key data privacy requirements for** **The Oracle Cloud Hosting and Delivery Policies covers:**	
SEBI Guidelines on Outsourcing of Activities by Intermediaries,	Data Security	Outsourcing contract has unambiguous confidentiality clauses to ensure protection of proprietary and customer	Customers are solely responsible for determining the suitability of a cloud service in the context of this requirement. Therefore, you are responsible for ensuring	**Cloud Services Hosting and Delivery Policies:**

Annexure I, Section 5.2(f) RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, Section 2 (15)(i) IRDAI Guidelines on Outsourcing of Activities by Indian Insurers, Regulation 12		data during the tenure of the contract and after the expiry of the contract.	that your organization's use of the cloud service and business processes meet these requirements. The Oracle Cloud Hosting and Delivery Policies include the Oracle Cloud Suspension and Termination Policy, which describes responsibilities when a contract is terminated. Additionally, the Oracle Financial Services Addendum (FSA) provides customers the ability to order transition services and transition assistance to help transfer or re-incorporate a concerned function back to the customer or to a third-party provider. For a period of 60 days after termination, Oracle makes available—by means of secure protocols and in a structured, machine-readable format—customers' content that resides in the production cloud services environment, or keeps the cloud service system accessible, for data retrieval. Oracle provides reasonable assistance to customers to retrieve their content from the production services environment and provides help to understand the structure and format of the export file. After the retrieval period expires, Oracle deletes the data from the Oracle cloud services environments unless otherwise required by applicable law (for more information, see Oracle CSA and DPA in the 'Resources' column.	oracle.com/corporate/contracts/cloudservices/hosting-delivery-policies.html **Oracle SaaS Help Center, Securing Applications:** docs.oracle.com/en/cloud/saas/applicationscommon/21c/facsa/index.html **Oracle Cloud Services Agreement (CSA):** CSA **Data Processing Agreement (DPA):** DPA for Oracle services
RBI Guidelines on Information	Business Continuity	Banks should at least on an annual basis, review the	This obligation does not apply to the Cloud services provider; however, Oracle provides a number of resources	**Oracle Risk Management Resiliency Business Continuity:**

Security, Electronic Banking, Technology Risk Management and Cyber Frauds, Section 2 (iv)		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.	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: • Oracle security practices • Compliance documentation Customers can access these materials via the Oracle Corporate Security Practices site. For each critical LOB, Oracle maintains a business continuity plan that includes a business impact analysis (BIA), risk assessments, and disaster recovery contingency plans. The plans align with Oracle's Risk Management and Resiliency Program policy, which requires the plans to outline procedures, ownership, roles, and responsibilities to be followed if a business disruption occurs. These plans are reviewed and tested annually. Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as used in the Oracle Risk Management Resiliency Program (RMRP). Upon request by a customer, Oracle provides a summary of the RMRP, material modifications to the RMRP within the last 12 months, and pertinent program governance areas, along with confirmation that an internal audit of these governance areas was performed within the last 12 months.	oracle.com/corporate/securitypractices/corporate/resilience-management/businesscontinuity.html **Compliance Documentation:** https://www.oracle.com/corporate/cloud-compliance/
RBI Guidelines on Managing Risks	Monitoring and Oversight	Provide for continuous monitoring and assessment	Customers are solely responsible for determining the suitability of a cloud service in the context of this	

and Code of Conduct in Outsourcing of Financial Services by banks, Section 5.5.1		by the bank of the service provider so that any necessary corrective measure to meet the Bank's legal and regulatory obligations.	requirement. Therefore, you are responsible for ensuring that your organization's use of the cloud service and business processes meet these requirements. However, Oracle Applications use a combination of tools, portals, and reports to provide customers insight and transparency in how their environment is performing and meeting various industry standards. **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.	
IRDAI Guidelines on Outsourcing of Activities by Indian Insurers, Regulation 13 RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks, Section 5.9.3	Inspection and Audit	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."	Customers or their regulator may audit Oracle's compliance with its obligations under the Data Processing Agreement up to once per year or more frequently as required by applicable law.	Data Processing Agreement for Oracle Services https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, Section 2 (iv)	Change Management and Notification	Formal process for tracking and monitoring program changes and projects.	Oracle has cloud services change management procedures that are designed to minimize service interruption during the implementation of changes. Changes made through change management procedures include system and service maintenance activities, upgrades and updates, and customer specific changes. For customer-specific changes and upgrades, where feasible, Oracle coordinates the maintenance periods with customers. Oracle reserved maintenance periods include the following ones: **Emergency maintenance** Oracle may be required to perform emergency maintenance to protect the security, performance, availability, or stability of Oracle cloud services. Emergency maintenance is required to address an exigent situation with a cloud service that cannot be addressed except on an emergency basis (for example, a hardware failure of the infrastructure underlying the service). Oracle works to minimize the use of emergency maintenance, and to the extent reasonable under the circumstances, provides 24 hours prior notice for any emergency maintenance requiring a service interruption. **Major maintenance changes** To help ensure continuous stability, availability, security, and performance of Oracle cloud services, Oracle limits major changes to its hardware infrastructure, operating software, applications software, and supporting application software under its control, typically to no more than twice per calendar year. Each such major change	**Cloud Services Hosting and Delivery Policies:** oracle.com/corporate/contracts/cloudservices/hosting-delivery-policies.html

			event is considered scheduled maintenance and may cause Oracle cloud services to be unavailable. Each such event is targeted to occur at the same time as the scheduled maintenance period. Oracle provides no less than 60 days prior notice of a major change event.	
RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, Section 2 (iv), Chapter 4, Page 81 Guideline 5.2(a) of the Intermediaries Guidelines IRDAI Guidelines on Outsourcing of Activities by Indian Insurers, Regulation 8	Service Levels and Performance Metrics	SLAs must clearly formalize the performance criteria to measure the quality and quantity of service levels	Oracle commits to deliver the services at the agreed level of availability and quality and offers multiple tools and services to support the monitoring obligations of its customers. Customers can access metrics on the Service Availability Level for Oracle cloud services that customers have purchased under their order through the Customer Notifications Portal. For those Oracle cloud services for which such metrics are not available in the Customer Notifications Portal, Oracle can provide metrics on the Service Availability Level upon receipt of a Service Request submitted by the customer requesting additional information regarding performance of the cloud services.	SaaS status: saasstatus.oracle.com/

Conclusion

Oracle is committed to helping customers operate globally in a fast-changing business environment and address the challenges of technology risks. Before deploying Oracle cloud services, Oracle strongly recommends that cloud customers formally analyse their cloud strategy to determine the suitability of using the applicable Oracle cloud services considering their own legal and regulatory compliance obligations. For more information, see oracle.com/corporate/cloud-compliance/.