ORACLE

Advisory: Oracle Cloud Infrastructure and the Insurance Regulatory and Development Authority of India (IRDAI) (Outsourcing of Activities by Indian Insurers) Regulations, 2017

Partial Description of Oracle Cloud Infrastruture Security Practices in the Context of the 2017 Outsourcing of Activities by Indian Insurers Regulations

October 2022, version 2.0

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 help you assess your use of Oracle cloud services in the context of the requirements applicable to you under the Insurance Regulatory and Development Authority of India (IRDAI) (Outsourcing of Activities by Indian Insurers) Regulations, 2017. This document might 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, which 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 Outsourcing of Activities by Indian Insurers Regulations are subject to periodic changes or revisions by the Insurance Regulatory and Development Authority of India. The current version of the regulations is available at www.irdai.gov.in/.

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

Table of Contents

Introduction

The Insurance Regulatory and Development Authority of India (IRDAI) issued the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017 (IRDAI Regulations). These regulations discuss outsourcing and provide risk-management guidelines and requirements for the insurance industry across India. For more information, see IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017.

Document Purpose

This document is intended to provide relevant information related to Oracle Cloud Infrastructure (OCI) to help you determine the suitability of using OCI in relation to the IRDAI Regulations and should be read in conjunction with the Oracle Contract Checklist for Select India Financial Services Regulations, Guidance and Circulars.

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 in regard to their specific legal and regulatory requirements.

About Oracle Cloud Infrastructure

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

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

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 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, such as cloud operator access controls and infrastructure security patching. Customers are responsible for securely configuring and using their cloud resources. For more information, see the cloud service documentation available in the Oracle Help Center.

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

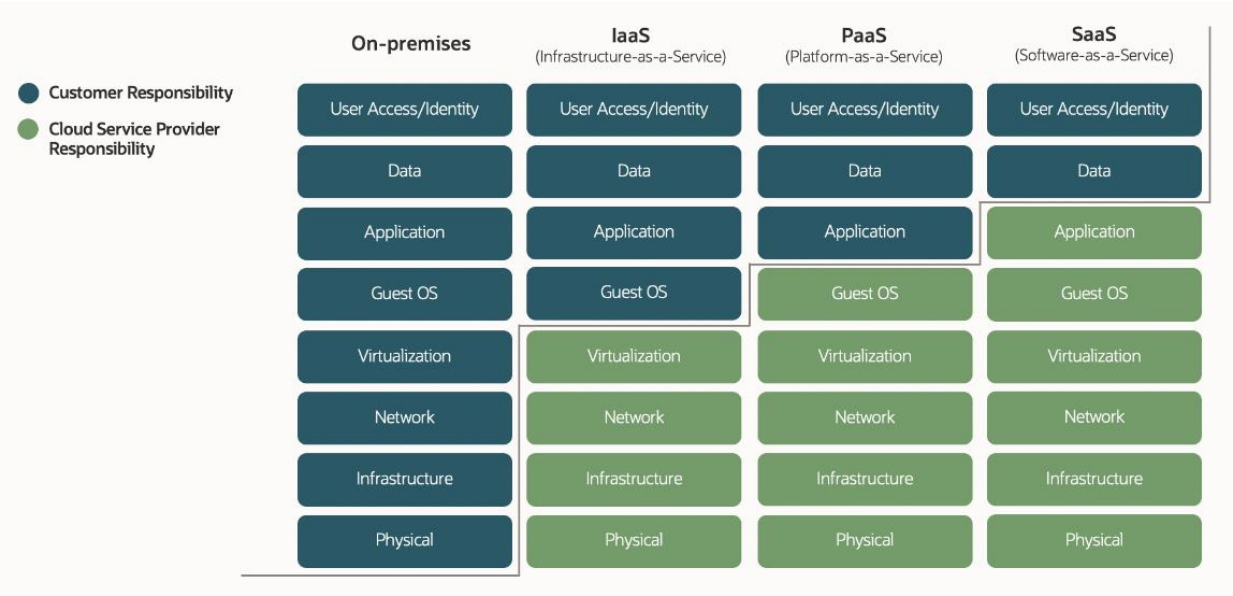

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

SUMMARY OF THE IRDAI REGULATIONS

This section includes general summaries and excerpts from some of the most relevant IRDAI Regulations pertaining to cloud operations and security, and describes OCI operational and security practices and services.

Regulation 10: Due Diligence of Outsourcing Service Providers

"...In considering or renewing an outsourcing arrangement, an insurer should subject the outsourcing service provider to appropriate due diligence which inter alia cover the following: [...] c) Existence of the outsourcing service provider as projected, its competence and experience to perform the activity proposed to be outsourced to it. d) Assessing the capability of the outsourcing Service Provider to employ standards envisaged, while performing outsourced activities. e) Its security and internal controls; f) Business continuity management; g) Where considered necessary, insurers shall obtain independent reviews and market feedback on the service provider to supplement its own findings; [...]"

Customers are solely responsible for determining the suitability of a cloud service in the context of this requirement. Therefore, you are responsible for ensuring that your organization's use of the cloud service and business processes meet these requirements.

Largely reflecting security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets.

For more information about Oracle's corporate security program, see oracle.com/assets/corporate-security-practices-4490843.pdf.

Regulation 11: Outsourcing Agreements

"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."

Customers are solely responsible for determining the suitability of a cloud service in the context of this requirement. Therefore, you are responsible for ensuring that your organization's use of the cloud service and business processes meet these requirements.

Oracle has standard terms and conditions that govern the use of cloud services. The rights and obligations of each party are defined in the following contractual documents, which are signed by the customer and Oracle before the provision of cloud services.

The Oracle Cloud Services Agreement (CSA) includes the following terms and conditions:

- Nondisclosure
- Governing law and jurisdiction
- Notice period and procedures

The Ordering Document covers the following terms and conditions:

- Description of cloud services
- Service-period time
- Fees
- Data center region (customers self-select their data center region in the OCI Console)

The Data Processing Agreement (DPA) defines obligations for each party that apply to the processing of personal information during the provision of services, such as the following ones:

- Allocation of responsibility between customers and Oracle for the processing of personal information
- Assistance with handling privacy inquiries and requests from individuals
- Subprocessor management and due diligence
- Audit rights
- Incident management and breach notification
- Return and deletion of personal information

The Oracle Cloud Hosting and Delivery Policies include the following policies:

- Oracle Cloud Security Policy
- Oracle Cloud Service Continuity Policy
- Oracle Cloud Service Level Agreement
- Oracle Cloud Suspension and Termination Policy

To help customers confirm that the necessary required contract terms are covered, Oracle provides a more detailed contract checklist for IRDAI outsourcing regulations.

Regulation 12: Confidentiality and Security

"The insurer shall satisfy itself that the outsourcing service provider's security policies, procedures and controls will enable the insurer to protect confidentiality and security of policyholders' information even after the contract terminates."

Customers are solely responsible for determining the suitability of a cloud service in the context of this requirement. Therefore, you are responsible for ensuring that your organization's use of the cloud service and business processes meet these requirements.

According to the Cloud Shared Management Model, customers are responsible for access to and protection of their data. OCI provides customers with the capability to restrict access to information stored or processed in their environment in accordance with their confidentiality commitments and 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.

Regulation 13: Inspection and Audit by the Insurer

"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. For more information, see oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf.

Regulation 16: Contingency Plans

"Insurers shall establish and maintain adequate contingency plans where the outsourced activity is material. These include disaster 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."

Customers have the option to deploy their instances and services in multiple, geographically separated regions for redundancy, high availability, and disaster recovery. Customers are responsible for designing and implementing a cloud architecture that meets their own requirements for availability, business continuity, and disaster recovery.

OCI provides several building blocks that customers can use to plan for the continuity of their applications:

- **Object Storage** replication aids in disaster recovery efforts and addresses data redundancy compliance requirements. Copies of objects can be made to other buckets in the same region or across regions. For more information, see docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm.
- **Compute** provides both bare metal and virtual machine compute instances that deliver performance, flexibility, and control. Oracle recommends deploying your compute instances across multiple availability domains or fault domains to protect your applications from outages. For more information, see docs.oracle.com/iaas/Content/Compute/home.htm.
- **Oracle Active Data Guard** helps provide data protection and availability for Oracle Database in a simple and economical manner. It maintains an exact physical replica of the production copy at a remote location that is open read-only while replication is active. For more information, see oracle.com/database/dataguard/.
- **Oracle GoldenGate** is an advanced logical replication product that supports multimaster replication, hub-and-spoke deployment, and data transformation. GoldenGate helps provide customers flexible options to address the complete range of replication requirements, including heterogeneous hardware platforms. For more information, see docs.oracle.com/iaas/goldengate/index.html.

In addition, Oracle provides several tools for customers to use to back up and recover infrastructure components based on their Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements. OCI conducts a Business Impact Analysis (BIA) and develops a Service Resiliency Plan (SRP) for each OCI service. OCI exercises each service's SRP at least annually. For more information, see oracle.com/cloud/backup-and-disaster-recovery/.

For more information that might help you meet the IRDAI Regulations requirements, see Disaster Recovery Capabilities of Oracle Cloud and Disaster Recovery for Databases.

Regulation 18: Regulatory Access

"Insurers shall, in all cases, obtain an undertaking from their outsourcing Service providers or include a provision within the outsourcing agreement, giving authorized representatives of the IRDAI the right to: […] b) access any internal audit reports or external audit findings of the outsourcing service Provider that concern the service being performed by the Insurer."

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. For more information, see oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf.

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 analyze their cloud strategy to determine the suitability of using the applicable Oracle cloud services in light of their own legal and regulatory compliance obligations. For more information, see oracle.com/corporate/cloud-compliance/.