ORACLE

Advisory: Oracle Cloud Infrastructure and the Reserve Bank of India 2011 Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds

Description of OCI Security Practices in the Context of the Reserve Bank of India (RBI) 2011 Guidelines

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 assist you assessing your use of Oracle cloud services in the context of the requirements applicable to you under the Reserve Bank of India Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds (2011). 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 Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds are subject to periodic changes or revisions by the Reserve Bank of India. The current version of the guidelines is available at rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf.

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 5

Document Purpose 5

About Oracle Cloud Infrastructure 5

The Cloud Shared Management Model 5

Summary of the RBI Guidelines 6

Chapter 2 (1) (1): Policies and Procedures 6

Chapter 2 (2): Risk Assessment 7

Chapter 2 (3): Inventory and Information/Data Classification 7

Chapter 2 (4): Defining Roles and Responsibilities 7

Chapter 2 (5) (i): Access Control 8

Chapter 2 (6) (i): Information Security and Information Asset Life Cycle 8

Chapter 2 (7) (i) and (iii): Personnel Security 9

Chapter 2 (8) (iii): Physical Security 9

Chapter 2 (9): User Training and Awareness 10

Chapter 2 (10) (i): Incident Management 10

Chapter 2 (11) (c): Application Control and Security 11

Chapter 2 (12) (i): Migration Controls 11

Chapter 2 (13) (i): Implementation of New Technologies 11

Chapter 2 (14) (v): Encryption 12

Chapter 2 (15) (i): Data Security 12

Chapter 2 (16) (ii) (b): Vulnerability Assessment 13

Chapter 2 (17) (i): Establishing On-Going Security Monitoring Processes 13

Chapter 2 (18) (iv): Security Measures Against Malware 13

Chapter 2 (19) (i): Patch Management 14

Chapter 2 (20) (i): Change Management 14

Chapter 2 (21) (i): Audit Trails 14

Chapter 2 (22) (ii): Information Security Reporting and Metrics 15

Chapter 2 (23) (ii): Information Security and Critical Service Providers/Vendors 15

Chapter 2 (24) (v): Network Security 15

Chapter 2 (25) (ii): Remote Access 16

Chapter 2 (26) (b): Distributed Denial of Service Attacks (DDoS/DoS) 16

Chapter 2 (27) (a): Implementation of ISO 27001 Information Security Management System 17

Chapter 2 (28) (ii): Wireless Security 17

Chapter 2 (29): Business Continuity Considerations 17

Chapter 2 (30) (a): Information Security Assurance 18

Chapter 3: IT Operations 18
Chapter 4 (2): IT Services Outsourcing 19
Chapter 5: Information System (IS) Audit 20
Chapter 6 (b): Cyber Fraud 20
Conclusion **20**

Introduction

The Reserve Bank of India (RBI) has issued Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds for financial institutions (RBI guidelines). These guidelines include requirements for governance of information security and information technology (IT) within banks. For more information, see rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf.

Document Purpose

This document is intended to provide relevant information related to Oracle Cloud Infrastructure (OCI) to assist you in determining the suitability of using OCI in relation to the RBI guidelines. Read it in conjunction with the Oracle Contract Checklist for Select India Financial Services Regulations, Guidance and Circulars.

This document includes general summaries and excerpts from chapter 2 through 6 of the RBI guidelines and describes Oracle Cloud operational and security practices and services in the context of these guidelines.

The information contained in this document doesn't 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 possibilities. Oracle provides several cloud solutions tailored to customers' needs. These solutions provide the benefits of the cloud, including global, secure, and high-performance environments in which to run all your workloads. The cloud offerings discussed in this document include OCI.

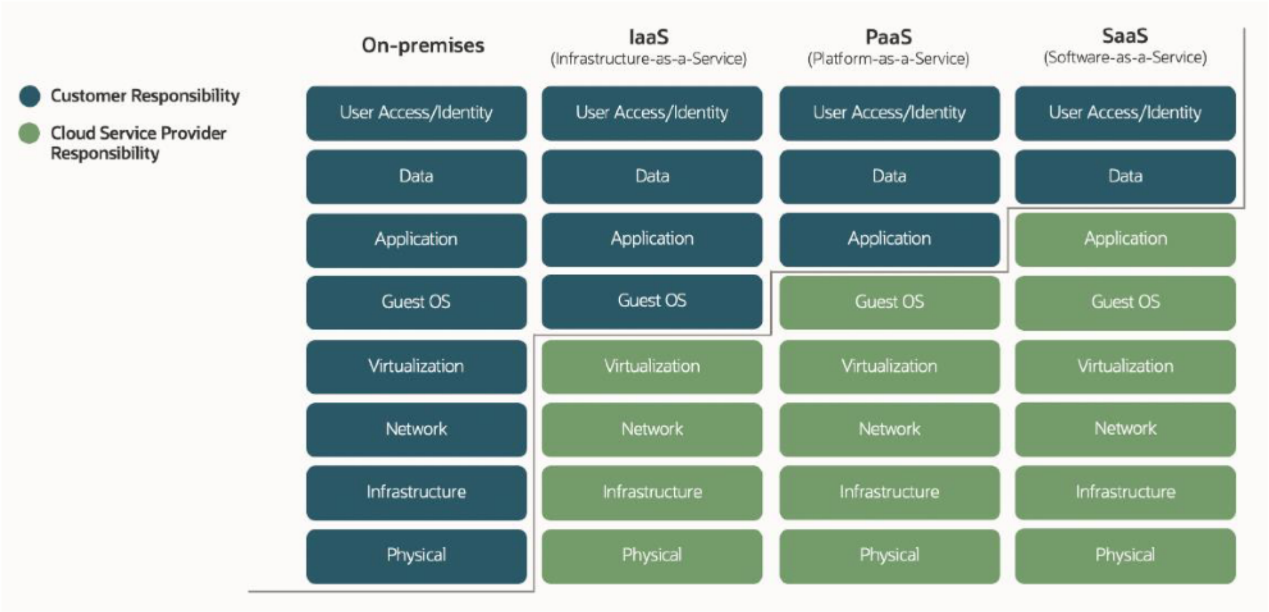
OCI is a set of complementary cloud services that enable you to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance compute capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from an on-premises network. OCI also 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 a high level.



🟦 Customer Responsibility

🟩 Cloud Service Provider Responsibility

On-premises	IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
🟦 User Access/Identity	🟦 User Access/Identity	🟦 User Access/Identity	🟦 User Access/Identity
🟦 Data	🟦 Data	🟦 Data	🟦 Data
🟦 Application	🟦 Application	🟦 Application	🟩 Application
🟦 Guest OS	🟦 Guest OS	🟩 Guest OS	🟩 Guest OS
🟦 Virtualization	🟩 Virtualization	🟩 Virtualization	🟩 Virtualization
🟦 Network	🟩 Network	🟩 Network	🟩 Network
🟦 Infrastructure	🟩 Infrastructure	🟩 Infrastructure	🟩 Infrastructure
🟦 Physical	🟩 Physical	🟩 Physical	🟩 Physical

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

Summary of the RBI Guidelines

This section addresses excerpts from chapters 2 through 6 of the RBI 2011 Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds. For the complete RBI guidelines, see rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf.

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

Chapter 2 (1) (1): Policies and Procedures

"Banks need to frame Board approved Information Security Policy and identify and implement appropriate information security management measures/practices keeping in view their business needs."

Customers are responsible for maintaining all required policies and procedures relevant to their own environment and operations.

OCI offers the following features and functions to help you meet these requirements:

- **Cloud Guard** helps you monitor, identify, achieve, and maintain a strong security posture on OCI. Use this cloud native service to examine OCI resources for security weaknesses related to configuration, and OCI operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist with, or take corrective actions, based on the configuration. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.
- **Data Safe** is a fully integrated cloud service focused on data security. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases. For more information, see docs.oracle.com/iaas/data-safe/index.html.

- **Oracle Autonomous Database** helps organizations transform IT database operations by automatically patching, updating, securing, and managing itself. Autonomous Database reduces the risk of human error and unexpected downtime, and accelerates the pace of innovation while using fewer resources. For more information, see docs.oracle.com/iaas/Content/Database/Concepts/adboverview.htm.

Chapter 2 (2): Risk Assessment

"The risk assessment must, for each asset within its scope, identify the threat/vulnerability combinations that have a likelihood of impacting the confidentiality, availability or integrity of that asset – from a business, compliance or contractual perspective."

Customers are responsible for implementing a risk assessment process within their OCI environment. Oracle provides the following information to assist customers in conducting necessary risk assessments:

- Oracle Cloud Compliance site
- Consensus Assessment Initiative Questionnaire (CAIQ) for OCI
- Cloud Services Hosting and Delivery Policies
- Oracle Corporate Security Practices

Additionally, OCI offers the following service to help you meet your risk assessment requirements:

- **Vulnerability Scanning Service** helps to improve your security posture in Oracle Cloud by routinely checking hosts for potential vulnerabilities. This service gives developers and administrators detailed scan reports and analysis reports that include applicability, risks, and trends for remediation of vulnerabilities. For more information, see docs.oracle.com/iaas/scanning/using/overview.htm.

Chapter 2 (3): Inventory and Information/Data Classification

"Effective control requires a detailed inventory of information assets."

Customers are responsible for implementing effective controls of their information assets and data classification in their environment.

OCI offers the following features to help you meet these requirements:

- **Data Catalog** helps you find, understand, govern, and track Oracle Cloud data assets. For more information, see docs.oracle.com/iaas/data-catalog/home.htm.
- **Tagging** helps you organize and manage the resources in your tenancy by adding metadata tags. For more information, see docs.oracle.com/iaas/Content/Tagging/Concepts/taggingoverview.htm.

Chapter 2 (4): Defining Roles and Responsibilities

"All defined and documented responsibilities and accountabilities must be established and communicated to all relevant personnel and management."

Customers are responsible for defining and documenting roles and responsibilities related to their assets and the data in their environment.

OCI has developed an organizational structure to meet its needs in support of its control obligations. Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel who support system design, development, implementation, security, operation, maintenance, and monitoring. For more information, see oracle.com/a/ocom/docs/oci-soc-3-report.pdf.

Chapter 2 (5) (i): Access Control

"An effective process for access to information assets is one of the critical requirements of information security. [...] Hence, access to information assets needs to be authorised by a bank only where a valid business need exists and only for the specific time period that the access is required."

Customers are responsible for implementing effective controls of their information assets.

OCI offers the following services and features to help you meet these requirements:

- **Identity and Access Management (IAM)** lets you control who has access to cloud resources. You can control what type of access a group of users has and to which specific resources. You can write policies to control access to all the services in OCI. IAM support multifactor authentication and identity federation with Security Assertion Markup Language (SAML)-based identity providers, which you can configure for extra security. You can also define password complexity and lockout requirements. Customers should protect their cloud access credentials and set up individual user accounts. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.
- **Vault** is a managed service that lets you centrally manage the encryption keys that protect data and the secret credentials that you use to securely access resources. Vaults securely store master encryption keys and secrets that might otherwise be stored in configuration files or in code. Specifically, depending on the protection mode, keys are stored either on the server or on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification. For more information, see docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.

Chapter 2 (6) (i): Information Security and Information Asset Life Cycle

"Information security needs to be considered at all stages of an information asset's life-cycle like planning, design, acquisition and implementation, maintenance and disposal. Banks need to apply systematic project management oriented techniques to manage material changes during these stages and to ensure that information security requirements have been adequately addressed."

To ensure the reliability of their information assets for decision-making and risk assessment, customers are responsible for implementing and maintaining information security governance policies that preserve and protect the integrity, confidentiality, and authenticity of information assets by employing and adjusting appropriate security controls throughout the information assets' life cycle.

OCI offers the following features to help you meet these requirements:

- **Data Safe** is a fully integrated cloud service focused on data security. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases. For more information, see docs.oracle.com/iaas/data-safe/index.html.
- **Identity and Access Management (IAM)** lets you control who has access to cloud resources. You can control what type of access a group of users has and to which specific resources. You can write policies to control access to all the services in OCI. IAM support multifactor authentication and identity federation with SAML-based identity providers, which you can configure for extra security. You can also define password complexity and lockout requirements. Customers should protect their cloud access credentials and set up individual user accounts. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.

Chapter 2 (7) (i) and (iii): Personnel Security

"Application owners grant legitimate users access to systems that are necessary to perform their duties and security personnel enforce the access rights in accordance with institution standards. […] Banks should have a process to verify job application information on all new employees. Additional background and credit checks may be warranted based on the sensitivity of a particular job or access level."

Customers are responsible for developing security policies and procedures that define information security responsibilities for their own personnel.

OCI offers the following service to help you meet these requirements:

- **Identity and Access Management (IAM)** lets you control who has access to cloud resources. You can control what type of access a group of users has and to which specific resources. You can write policies to control access to all the services in OCI. IAM support multifactor authentication and identity federation with SAML-based identity providers, which you can configure for extra security. You can also define password complexity and lockout requirements. Customers should protect their cloud access credentials and set up individual user accounts. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.

OCI also supports federation with Oracle Identity Cloud Service, Microsoft Active Directory (through Active Directory Federation Services), Microsoft Azure Active Directory, Okta, and other identity providers that supports the SAML 2.0 protocol. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/federation.htm.

Chapter 2 (8) (iii): Physical Security

"A bank needs to deploy the following environmental controls:

- ***Secure location of critical assets providing protection from natural and man-mad threats***
- ***Restrict access to sensitive areas like data centres, which also includes detailed procedures for handling access by staff, third party providers and visitors***

  […]

- ***Monitoring mechanisms for the detection of compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access log reviews etc"***

Customers are responsible for restricting access to their own facilities and other locations where they operate their business.

OCI data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow an N2 redundancy methodology for critical equipment operation. Data centers that house OCI services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security and availability events that might arise. For more information, see oracle.com/cloud/architecture-and-regions/.

OCI has implemented controls designed to prevent unauthorized persons from gaining access to computing facilities, such as the use of security personnel, secured buildings, and designated data center premises. Oracle provides secured computing facilities for both office locations and production cloud infrastructure.

Common controls between office locations and Oracle-controlled colocations or data centers currently include, for example, the following controls:

- Physical access requires authorization and is monitored.
- All employees and visitors must visibly wear official identification while onsite.
- Visitors must sign a visitor's register and be escorted or observed while onsite.
- Physical access to data halls is approved before access is granted.

For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.

Chapter 2 (9): User Training and Awareness

"[…] there is a vital need for an initial and ongoing training and information security awareness programme. The programme may be periodically updated keeping in view changes in information security, threats/vulnerabilities and/or the bank's information security framework."

Customers are responsible for implementing a formal security awareness program to ensure that their personnel are aware of security policies and procedures in their own environment.

Oracle promotes security awareness and educates its employees through regular newsletters and various security awareness campaigns. Each OCI employee must complete information-protection awareness training when hired and annually thereafter. The course instructs employees about their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that might apply to employees' jobs at Oracle and are required by company policy. For more information, see oracle.com/corporate/security-practices/corporate/.

Chapter 2 (10) (i): Incident Management

"Incident management is defined as the process of developing and maintaining the capability to manage incidents within a bank so that exposure is contained and recovery achieved within a specified time objective. Incidents can include the misuse of computing assets, information disclosure or events that threaten the continuance of business processes."

Customers are responsible for implementing an incident response plan for their own environment and testing it annually.

OCI offers the following services and features to help you meet this requirement:

- **Monitoring** helps you actively and passively monitor your cloud resources by using metrics and alarms. For more information, see docs.oracle.com/en-us/iaas/Content/Monitoring/home.htm.
- **Audit** helps you track activity in your environment. For more information, see docs.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm.

Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to security incidents. This policy authorizes the Oracle Global Information Security organization to provide overall direction for incident prevention, identification, investigation, and resolution in Oracle's Lines of Business (LoBs). When an incident is discovered, OCI defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures, which improves security posture and defense-in-depth. Formal procedures and systems are used within the LoBs to collect information and maintain a chain of custody for evidence during incident investigation.

For more information, see oracle.com/corporate/security-practices/corporate/security-incident-response.html.

Chapter 2 (11) (c): Application Control and Security

"The following are the important Application control and risk mitigation measures that need to be implemented by banks:

1. Each application should have an owner which will typically be the concerned business function that uses the application […]

5. All application systems need to have audit trails along with policy/procedure of log monitoring for such systems including the clear allocation of responsibility in this regard."

Customers are solely responsible for the control and security of the applications that they develop and run on OCI.

OCI offers the following service to help you meet this requirement:

- **Audit** helps you track activity in your environment. Audit automatically records calls to all supported OCI API endpoints as log events. Log events recorded by Audit include API calls made by the Oracle Cloud Console, CLI, SDKs, custom clients, or other OCI services. Information in the logs includes the time that the API activity occurred, the source and the target of the activity, along with the type of action and response. For more information, see docs.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm.

Chapter 2 (12) (i): Migration Controls

"There needs to be a documented Migration Policy indicating the requirement of road-map / migration plan / methodology for data migration (which includes verification of completeness, consistency and integrity of the migration activity and pre and post migration activities along with responsibilities and timelines for completion of same)."

Customers are solely responsible for all their data migration processes and controls.

Oracle provides the following features and functions to help you meet this requirement:

- **Database Migration** provides a high performance, self-service experience for migrating databases to OCI. This service operates as a multitenant service in a Database Migration service tenancy and communicates with your resources by using private endpoints, which it manages. For more information, see docs.oracle.com/iaas/database-migration/doc/overview-oracle-cloud-infrastructure-database-migration.html.
- **Classic Migration Service** migrates applications, such as Oracle Java Cloud Service, SOA Cloud Service, and Integration Classic applications, from OCI Classic and Oracle Cloud@Customer to OCI. For more information, see docs.oracle.com/iaas/application-migration/home.htm.
- **Oracle Cloud Lift Services** provide guidance from cloud engineers on planning, architecting, prototyping, and managing cloud migrations. Clients can move critical workloads in weeks, or even days, instead of months by using these included services for customer tenancies. For more information, see oracle.com/cloud/cloud-lift/.

Chapter 2 (13) (i): Implementation of New Technologies

"Banks need to carry out due diligence with regard to new technologies since they can potentially introduce additional risk exposures."

Customers are responsible for risk evaluations and decisions regarding new technologies relevant to their own environment. Oracle provides the following information to assist its customers in conducting its assessment:

- Oracle Cloud Compliance site

- Consensus Assessment Initiative Questionnaire (CAIQ) for OCI
- Cloud Services Hosting and Delivery Policies
- Oracle Corporate Security Practices

Additionally, OCI offers the following service to help you meet this requirement:

- **Cloud Advisor** finds potential inefficiencies in your tenancy and offers guided solutions that explain how to address them. The recommendations help you maximize cost savings and improve the tenancy security. For more information, see docs.oracle.com/iaas/Content/CloudAdvisor/home.htm.

Chapter 2 (14) (v): Encryption

"Banks should only select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international cryptographer community or approved by authoritative professional bodies, reputable security vendors or government agencies."

Customers are responsible for implementing the appropriate encryption processes and controls in their environment.

OCI offers the following service to help you meet these requirements:

- **Vault** is a managed service that lets you centrally manage the encryption keys that protect data and the secret credentials that you use to securely access resources. Vaults securely store master encryption keys and secrets that might otherwise be stored in configuration files or in code. Specifically, depending on the protection mode, keys are stored either on the server or on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification. For more information, see docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.

The Block Volumes, Object Storage, and File Storage services enable at-rest data encryption by default, by using Advanced Encryption Standard (AES) algorithm with 256-bit encryption. In-transit control plane data is encrypted by using Transport Layer Security (TLS) 1.2 or later.

Chapter 2 (15) (i): Data Security

"Banks need to define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives."

As cloud provider, Oracle generally has no insight into the data that customers store or process in OCI. Customers are solely responsible for implementing procedures that ensure the integrity and security of their data stored in OCI. However, Oracle's security practices are designed to help protect the confidentiality, integrity, and availability of both customer and Oracle data. For more information about Oracle data security practices, see oracle.com/corporate/security-practices/corporate/data-protection/.

OCI offers the following features and functions to help you meet this requirement:

- **Audit** helps you track activity in your environment. For more information, see docs.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm.
- **Data Safe** is a fully integrated cloud service focused on data security. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases. For more information, see docs.oracle.com/iaas/data-safe/index.html.

Chapter 2 (16) (ii) (b): Vulnerability Assessment

"Banks should ensure that vulnerability scanning is performed in an authenticated mode (i.e., configuring the scanner with administrator credentials) at least quarterly, either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested, to overcome limitations of unauthenticated vulnerability scanning."

Customers are responsible for security, vulnerability, and penetration testing of applications that they develop or deploy within their environment. For information about the Oracle Cloud Security Testing Policy, see docs.oracle.com/iaas/Content/Security/Concepts/security_testing-policy.htm.

OCI offers the following service to help you meet this requirement:

- **Vulnerability Scanning Service** helps to improve your security posture in Oracle Cloud by routinely checking hosts for potential vulnerabilities. This service gives developers and administrators detailed scan reports and analysis reports that include applicability, risks, and trends for remediation of vulnerabilities. For more information, see docs.oracle.com/en-us/iaas/scanning/using/overview.htm.

Oracle regularly performs penetration and vulnerability testing and security assessments against Oracle cloud infrastructure, platforms, and applications. These tests are intended to validate and improve the overall security of Oracle cloud services.

Chapter 2 (17) (i): Establishing On-Going Security Monitoring Processes

"A bank needs to have robust monitoring processes in place to identify events and unusual activity patterns that could impact on the security of IT assets."

Customers are responsible for intrusion detection and prevention systems in their own environment.

OCI offers the following services to help you meet this requirement:

- **Monitoring** helps you actively and passively monitor your cloud resources by using the metrics and alarms. For more information, see docs.oracle.com/iaas/Content/Monitoring/home.htm.
- **Cloud Guard** examines OCI resources for security weaknesses related to configuration, and operators and users for risky activities. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.
- **Health Checks** provides high-frequency external monitoring to help you determine the availability and performance of any public-facing service, including hosted websites, API endpoints, or externally facing load balancers. For more information, see docs.oracle.com/iaas/Content/HealthChecks/home.htm.

Oracle uses a variety of software tools to monitor the availability and performance of Oracle cloud services and the operation of infrastructure and network components under Oracle's control. Oracle monitors the hardware that supports the Oracle cloud service environments, and generates alerts for monitored network components such as CPU, memory, storage, and database. Oracle Cloud Operations staff monitors alerts associated with deviations to Oracle-defined thresholds and follows standard operating procedures to investigate and resolve underlying issues. For more information, see oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf.

Chapter 2 (18) (iv): Security Measures Against Malware

"Banks should employ anti-malware software and signature auto update features to automatically update signature files and scan engines whenever the vendor publishes updates."

Customers are responsible for the deployment, configuration, use, and maintenance of an antivirus solution within their own environment.

Additionally, OCI deploys the following security measures:

- A host intrusion-detection system that monitors and detects security events
- A network intrusion-detection system on the edge to monitor production traffic and detect security events
- Antivirus to detect malware
- File integrity monitoring to monitor unauthorized modification of critical system files, configuration files, or content files

Chapter 2 (19) (i): Patch Management

"A Patch Management process needs to be in place to address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising."

To ensure secure cloud infrastructure services and operations, OCI conducts infrastructure security patching. However, customers are responsible for configuring, managing, patching, and maintaining the operating systems, databases, applications, and other components within their environment in line with their requirements and policies.

Chapter 2 (20) (i): Change Management

"A change management process should be established, which covers all types of change. For example, upgrades and modifications to application and software, modifications to business information, emergency 'fixes', and changes to the computers/networks that support the application."

Customers are responsible for maintaining a change management process that addresses these requirements in their own environment.

Changes to the OCI production environment must go through a defined change-management process. OCI follows formal change management procedures to review, test, and approve changes before applying them in the production environment under its control. Changes made through change-management procedures include system and service maintenance activities, upgrades and updates, and customer-specific changes. OCI change-management procedures are designed to minimize service interruption during the implementation of changes.

Oracle reserves specific maintenance periods for changes that might require OCI to be unavailable during the maintenance period. Oracle works to ensure that change-management procedures are conducted during these scheduled maintenance windows, while taking into consideration low traffic periods and geographical requirements. Oracle provides prior notice of modifications to the standard maintenance-period schedule. For customer-specific changes and upgrades, where feasible, Oracle coordinates maintenance periods with customers.

For more information about the Oracle Cloud Change Management Policy, see the Oracle Cloud Hosting and Delivery Policies.

Chapter 2 (21) (i): Audit Trails

"Banks needs to ensure that audit trails exist for IT assets satisfying the banks business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution."

Customers are responsible for implementing secure audit trails within their own environment.

OCI offers the following services to help you meet this requirement:

- **Audit** helps you track activity in your environment. Audit provides records of API operations performed against supported services as a list of log events. The service logs events at both the tenancy and compartment level. For more information, see docs.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm.

- **Data Safe** is a fully integrated cloud service focused on data security. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases. For more information, see docs.oracle.com/iaas/data-safe/doc/audit-trails.html.

Additionally, API calls, including actions from the customer administration console, are logged and retained for 90 days and cannot be deleted by customers. Customers may request an export of their logs by contacting Oracle.

Chapter 2 (22) (ii): Information Security Reporting and Metrics

"There should be arrangements for monitoring the information security condition of the organisation, which are documented, agreed with top management and performed regularly."

Customers are responsible for implementing appropriate security monitoring and reporting to meet their information security requirements.

OCI offers the following services to help you meet this requirement:

- **Monitoring** helps you actively and passively monitor your cloud resources by using the metrics and alarms. For more information, see docs.oracle.com/iaas/Content/Monitoring/home.htm.
- **Cloud Guard** examines OCI resources for security weaknesses related to configuration, and OCI operators and users for risky activities. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.
- **Security Zones** policies can be applied to various OCI resources to ensure that they stay secure, prevent security misconfigurations, and comply with your security policies. For more information, see docs.oracle.com/iaas/security-zone/using/security-zones.htm.

Chapter 2 (23) (ii): Information Security and Critical Service Providers/Vendors

"Management should evaluate the role that the third party performs in relation to the IT environment, related controls and control objectives."

Customers are responsible for evaluating all third-party business partners and service providers.

Additionally, Oracle provides several resources to assist its customers in conducting necessary risk assessments:

- Oracle Cloud Compliance site
- Consensus Assessment Initiative Questionnaire (CAIQ) for OCI
- Cloud Services Hosting and Delivery Policies
- Oracle Corporate Security Practices

Chapter 2 (24) (v): Network Security

"With a clear understanding of network connectivity, banks can avoid introducing security vulnerabilities by minimizing access to less-trusted domains and employing encryption and other controls for less secure connections."

Customers are responsible for securely configuring network elements such as virtual cloud networks, load balancer DNS, access control lists, and gateways.

OCI offers the following service to help you meet this requirement:

- **Isolated Network Virtualization** helps prevent attacks on customer tenancies. A foundational element of OCI's security-first architecture, isolated network virtualization helps stop malware with a custom-designed SmartNIC to isolate and virtualize the network. For more information, see oracle.com/sg/security/cloud-security/isolated-network-virtualization/.

Chapter 2 (25) (ii): Remote Access

"The management should establish policies restricting remote access and be aware of all remote-access devices attached to their systems."

Customers are responsible for restricting access to their virtual cloud networks to authorized users and remain responsible for managing data within their environment.

OCI offers the following service to help you meet this requirement:

- **Identity and Access Management (IAM)** lets you control who has access to cloud resources. You can control what type of access a group of users has and to which specific resources. You can write policies to control access to all the services in OCI. IAM support multifactor authentication and identity federation with SAML-based identity providers, which you can configure for extra security. You can also define password complexity and lockout requirements. Customers should protect their cloud access credentials and set up individual user accounts. For details, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.

Chapter 2 (26) (b): Distributed Denial of Service Attacks (DDoS/DoS)

"As part of the defence strategy, banks should install and configure network security devices discussed earlier in the chapter for reasonable preventive/detective capability."

Customers are responsible for using intrusion detection and prevention systems in their own environment and the incorporation of appropriate infrastructure event data.

OCI offers the following services and features to help you meet this requirement:

- **Distributed Denial of Service (DDoS)** protection is an always-on detection and mitigation platform for common DDoS volumetric attacks. The service protects against common layer 3 and 4 attacks like SYN floods, UDP floods, ICMP floods, and NTP amplification attacks. DDoS protection of system traffic passing through gateway routers is included with all OCI accounts, and no configuration or monitoring is required. However, customers are responsible for designing DDoS protection mechanisms to meet their requirements.
- **Isolated Network Virtualization** helps prevent attacks on customer tenancies. For more information, see oracle.com/sg/security/cloud-security/isolated-network-virtualization/.
- **Cloud Guard** helps you monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud. Use this cloud native service to examine OCI resources for security weaknesses related to configuration, and OCI operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist with, or take corrective actions, based on your configuration. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.

Chapter 2 (27) (a): Implementation of ISO 27001 Information Security Management System

"Commercial banks should implement Information Security Management System (ISMS) best practices for their critical functions/processes."

Customers are responsible for maintaining all required governance standards and policies relevant to their own ISMS, and for risk management and decisions within that framework.

OCI maintains an ISMS program and undergoes regular independent third-party audits to maintain International Organization for Standardization (ISO) 27000 series certifications. For more information about OCI compliance programs, see oracle.com/corporate/cloud-compliance/.

Chapter 2 (28) (ii): Wireless Security

"[…] wireless networks rely on extensive use of encryption to authenticate users and devices and to shield communications. If a bank uses a wireless network, it should carefully evaluate the risk and implement appropriate additional controls."

Customers are solely responsible for evaluating risk and implementing wireless network security controls in their environment.

OCI offers the following service to help you meet this requirement:

- **Identity and Access Management (IAM)** lets you control who has access to cloud resources. You can control what type of access a group of users has and to which specific resources. You can write policies to control access to all the services in OCI. IAM support multifactor authentication and identity federation with SAML-based identity providers, which you can configure for extra security. You can also define password complexity and lockout requirements. Customers should protect their cloud access credentials and set up individual user accounts. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.

Oracle's Network Security Policy establishes formal requirements for the provision and use of wireless networks and connectivity to access the Oracle corporate network, including network segmentation requirements. Oracle IT manages wireless networks and monitors for unauthorized wireless networks. Network devices must be registered in an Oracle-approved information systems inventory per Oracle Information Systems Inventory Policy. This policy requires the accurate inventory and documented ownership of all information systems processing information assets throughout their life cycle. For more information, see oracle.com/corporate/security-practices/corporate/network-communications-security.html.

Chapter 2 (29): Business Continuity Considerations

"Risk assessments should consider the changing risks that appear in business continuity scenarios and the different security posture that may be established."

Customers are responsible for designing, developing, and implementing a cloud architecture that meets their own requirements for availability, business continuity, and disaster recovery.

Oracle provides geographically resilient data regions and services needed to build and run applications in a highly secure, hosted environment with high performance and availability. For more information, see docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/extreme-reliability.htm.

Oracle Cloud Hosting and Delivery Policies describe the Oracle Cloud Service Continuity Policy, Oracle Cloud Services High Availability Strategy, Oracle Cloud Services Backup Strategy, and Oracle Cloud Service Level Agreement. Service-specific pillar documents provide additional information about specific cloud services. For more information, see oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html.

Chapter 2 (30) (a): Information Security Assurance

"Penetration testing needs to be conducted at least on an annual basis."

Customers are responsible for penetration testing, audits, and assessments to identify any security vulnerabilities within their own environment. For more information about the Oracle Cloud Security Testing Policies, see docs.oracle.com/iaas/Content/Security/Concepts/security_testing-policy.htm.

Oracle offers the following services to help you meet this requirement:

- **Vulnerability Scanning Service** helps to improve your security posture in Oracle Cloud by routinely checking hosts for potential vulnerabilities. This service gives developers and administrators detailed scan reports and analysis reports that include applicability, risks, and trends for remediation of vulnerabilities. For more information, see docs.oracle.com/iaas/scanning/using/overview.htm.
- **Cloud Guard** helps you monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud. Use this cloud native service to examine OCI resources for security weaknesses related to configuration, and OCI operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist with, or take corrective actions, based on your configuration. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.

Oracle regularly performs penetration and vulnerability testing and security assessments against Oracle cloud infrastructure, platforms, and applications. These tests are intended to validate and improve the overall security of Oracle Cloud services.

Chapter 3: IT Operations

"IT Operations should ensure effectiveness and efficiency in delivery and support of these services to ensure value for customers."

Customers are solely responsible for determining the suitability of a cloud service in the context of their IT Operations.

Functions covered as a part of IT Operations are as follows:

- IT Operations Management: ***"IT Operations management is a function which is primarily responsible for the day-to-day management and maintenance of an organisation's IT infrastructure, ensuring service delivery to the agreed level as defined by Service Level Agreement (SLA)."***

  Oracle Cloud Service Level Agreement is described in the Oracle Cloud Hosting and Delivery Policy at oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf.

- Application Management: ***"It involves handling and management of application as it goes through the entire life-cycle. The life-cycle encompasses both application development and application management activities."***
- Infrastructure Management: ***"It is the function primarily responsible for providing technical expertise and overall management of the IT infrastructure. Its primary objective is to assist plan, implement and maintenance of a stable technical infrastructure in order to support an organisation's business processes."***

Oracle cloud service data centers are designed to help protect the security and availability of customer data. These data centers align with ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow an N2 redundancy methodology for critical equipment operation. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.

- IT Operations Framework Risk Management: ***"[Banks] should conduct a periodic risk assessment which should identify: Internal and external risks, and [risks] associated with individual platforms, systems, or processes, as well as automated processing units."***

  Oracle offers several documents to assist its customers in conducting necessary risk assessment of OCI services:

  - Consensus Assessment Initiative Questionnaire (CAIQ) for OCI
  - Oracle Corporate Security Practices
  - Oracle Cloud Compliance site

Chapter 4 (2): IT Services Outsourcing

"Risks inherent to process outsourcing, including Strategic risk, Reputation risk, Operational risk, Compliance risk, Legal risk, Counter party risk, Country risk, Contractual risk, Access risk, Concentration and systemic risk, and Exit strategy risk."

Customers are solely responsible for evaluating the risks of any outsourcing arrangement and periodically reviewing the effectiveness of their policies and procedures.

OCI delivers an enterprise-grade public cloud. Oracle architected it specifically to run enterprise applications and databases. It also includes tools and utilities for constructing new cloud native and mobile apps, all on a unified platform and networking fabric. OCI delivers the performance, versatility, and governance required by enterprise IT while offering a level of performance that often exceeds what is commonly found in on-premises, high-performance computing environments. OCI also combines the elasticity and utility of the public cloud with the control, security, performance, and predictability of on-premises computing environments. Customers receive consistent, dependable service levels for all types of applications and computing environments, including complex, technical computing workloads such as simulating crash tests, modeling insurance risks, and testing new manufacturing materials. For more information, see oracle.com/us/solutions/cloud/cloudessentials-oci-5100435.pdf.

Oracle makes the following information available about its various cloud offerings that can help regulated entities in making this determination:

- Consensus Assessment Initiative Questionnaire (CAIQ) for OCI
- Oracle Corporate Security Practices
- Oracle Cloud Compliance site

The required rights and obligations of each party are defined in the following contractual documents, which the customer and Oracle sign before the provision of cloud services:

- Oracle Cloud Service Agreement
- Oracle Financial Services Addendum
- Data Processing Agreement for Oracle Services

Chapter 5: Information System (IS) Audit

"[...] Bank's management and RBI, need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the risks are managed."

OCI operates under policies that are generally aligned with the ISO/IEC 27002 Code of Practice for information security controls. The internal controls of OCI are subject to periodic testing by independent third-party audit organizations. Such audits may be based on the following standards:

- Statement on Standards for Attestation Engagements 18 (SSAE 18), Reporting on Controls at a Service Organization
- International Standard on Assurance Engagements No. 3402 (ISAE 3402), Assurance Reports on Controls at a Service Organization
- ISAE 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information
- Other third-party auditing standards or procedures applicable to OCI

The Data Processing Agreement (DPA) for Oracle Services describes the rights and obligations of each party, including the audit rights of customers and their regulators.

Chapter 6 (b): Cyber Fraud

"Banks are required to constitute a special committee for monitoring and follow up of cases of frauds involving amounts of 1 crore and above exclusively, while the Audit Committee of the Board (ACB) may continue to monitor all the cases of frauds in general."

Customers are responsible for using fraud prevention and detection systems in their own environment. Fraud prevention practices, fraud detection, fraud investigation, and reporting of frauds to the RBI are generally internal process responsibilities of banks.

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/.

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