ORACLE

Advisory: Oracle Cloud Infrastructure and the Technology Risk Management Guidelines Issued by the Monetary Authority of Singapore in January 2021

Description of Oracle Cloud Infrastructure Security Practices in the Context of Section 8.5 of the 2021 Technology Risk Management Guidelines

January 2022, Version 2.0

Public

Disclaimer

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

This document is for informational purposes only and is intended solely to assist you assessing your use of Oracle cloud services in the context of the requirements applicable to you under the Monetary Authority of Singapore Technology Risk Management (TRM) Guidelines. This may also help you to assess Oracle as an outsourced service provider. You remain responsible for performing your own independent assessment of the information in this document, as the information in this document is not intended and may not be used as legal advice about the content, interpretation or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied 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 TRM Guidelines are subject to periodic changes or revisions by the Monetary Authority of Singapore. The current version of the Guidelines is at https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf.

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

Revision History

The following revisions have been made to this document since its initial publication.

DATE	REVISION
January 2022	• Added details about customer responsibility and about supplier colocation security standards • Revised title from “Advisory: Oracle Cloud Infrastructure Security Practices for Data Centre Resilience in the Context of the Technology Risk Management Guidelines”
April 2021	Initial publication

Table of Contents

Introduction

The Monetary Authority of Singapore (MAS), which was created with the passing of the MAS Act in 1970, is Singapore's central bank and integrated financial regulator. MAS has provided a list of guidelines applicable to financial institutions (FIs) operating in Singapore. The Technology Risk Management (TRM) Guidelines cover risk management, cyber security, and IT outsourcing. For more information, see www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf.

Document Purpose

This document provides relevant information about Oracle Cloud Infrastructure (OCI) that can assist you in determining the suitability of using OCI in relation to Section 8.5 of the TRM Guidelines.

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 possibilities. Oracle provides various 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 Infrastructure (OCI).

OCI is a set of complementary cloud services that enable customers to build and run a 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, infrastructure security patching, and so on. Customers are responsible for securely configuring and using their cloud resources. For more information, see docs.oracle.com/iaas/Content/Security/Concepts/security_overview.htm.

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

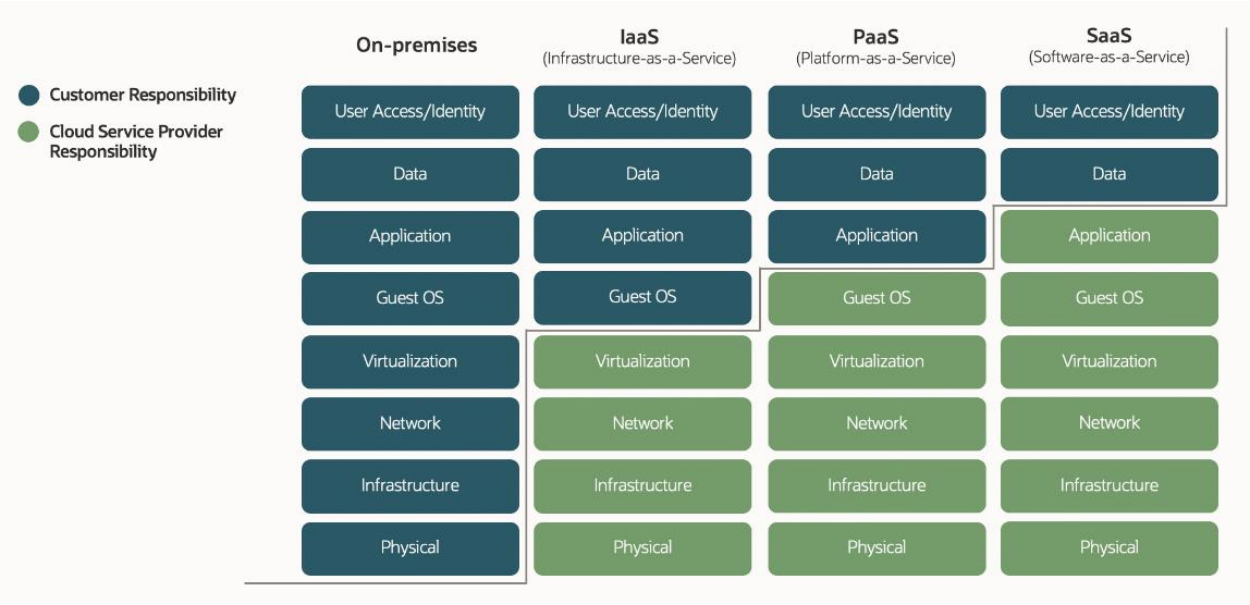

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Summary of Section 8.5 of the Technology Risk Management Guidelines

This section summarizes the "Data Centre Resilience" guidelines found in section 8.5 of the TRM Guidelines and describes OCI's operational and security services in the context of these guidelines.

TRM Section 8.5.1

"The FI should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centres (DCs) to identify potential vulnerabilities and weaknesses, and the protection that should be established to safeguard the DCs against physical and environmental threats. In addition, the TVRA should consider the political and economic climate of the country in which the DCs are located. The TVRA should be reviewed whenever there is a significant change in the threat landscape or when there is a material change in the DC's environment." (TRM, 2021)

Customers are solely responsible for determining the suitability of a cloud service in the context of safeguarding the data center from physical and environment threats. Therefore, you are responsible for ensuring that your use of the cloud service and business processes meet these requirements.

Oracle Global Physical Security uses a risk-based approach to implement physical and environmental security. The goal is to balance prevention, detection, protection, and response, while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. Oracle regularly performs risk assessments to confirm that appropriate mitigation controls are in place and maintained. For information about OCI's physical security policies and practices, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.

TRM Section 8.5.2

"The FI should ensure adequate redundancy for the power, network connectivity, and cooling, electrical and mechanical systems of the DC to eliminate any single point of failure." (TRM, 2021)

Customers are solely responsible for determining the suitability of a cloud service in the context of this requirement. Oracle requires appropriate and proportionate measures to protect its assets in colocation facilities against physical and environment threats. These requirements for colocation facilities include:

- Onsite generators must have fuel capacity that provides at least 48 hours of operational availability when at full load. The colocation supplier must also demonstrate the capability to source fuel from a diverse group of suppliers within 18 hours, by having, for example, contracts with multiple fuel suppliers.

- Regular testing on each generator must be performed and documented to ensure that they operate as expected if main power supplies are disrupted.
- Backup power must be available to support the alarm system, access control, video systems, and other supporting security infrastructure. Where batteries are used as the backup power source, a minimum of eight hours of power must be available.
- The colocation supplier must maintain a preventative maintenance program with documented procedures that address critical systems such as UPS, HVAC, generators, and fire suppression. Written procedures must be documented, reviewed, and published regularly.
- The facilities must have a central monitor and maintain temperature and humidity within Oracle data halls. Alarms are automatically generated for any events that exceed environmental thresholds.

For more information, see oracle.com/us/assets/supplier-security-standards-app2-1639575.pdf.

TRM Section 8.5.3

"As part of the DC's environmental controls, the FI should implement fire detection and suppression devices or systems, such as smoke or heat detectors, inert gas suppression systems, and wet or dry sprinkler systems." (TRM, 2021)

Customers are solely responsible for determining the suitability of a cloud service in the context of this requirement.

OCI requires measures from its colocation suppliers to protect its assets in colocation facilities against physical and environmental threats. These requirements for colocation facilities include:

- Fire suppression systems must be implemented throughout the facility. Maintenance must be kept up to date in accordance with local requirements. Reports are provided to Oracle or Oracle assessors on request.
- All fire suppression and detection devices must be supported by an independent energy source.

For more information, see oracle.com/us/assets/supplier-security-standards-app2-1639575.pdf.

TRM Section 8.5.4

"The FI's secondary or disaster recovery DC should be geographically separated from its primary or production DC so that both sites will not be impacted by a disruption to the underlying infrastructure (e.g. telecommunications and power) in a particular location." (TRM, 2021)

Customers are solely responsible for determining the suitability of a cloud service in the context of safeguarding the data center from physical and environment threats. Therefore, you are responsible for ensuring that your use of the cloud service and business processes meet these requirements.

When setting up your account, you choose a home region in which to initially locate your tenancy. Your data stays in that region unless you choose to move it outside the region. OCI offers powerful services that might operate across tenancies or regions. Through the OCI Console and API, you are informed when your actions might cause data to move to another tenancy or region.

For more information about regions, availability domains, and setting up your tenancy, see docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm and docs.cloud.oracle.com/iaas/Content/GSG/Concepts/settinguptenancy.htm.

OCI provides several services that you can use to plan for disaster recovery of your applications:

- **Object Storage:** Object Storage replication aids in disaster recovery efforts and can address 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:** The Compute service provides both bare metal and virtual machine instances that deliver performance, flexibility, and control. We recommend 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:** This service offering can help provide data protection and availability for Oracle Databases 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**: This advanced logical replication product offering supports multimaster replication, hub and spoke deployment, and data transformation. GoldenGate provides 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.

For more information about disaster recovery, see the following pages:

- docs.oracle.com/en/solutions/design-dr/learn-dr-building-blocks-oracle-cloud1.html
- docs.oracle.com/en/solutions/design-dr/plan-dr-databases1.html

TRM Section 8.5.5

"The DC's physical security and environmental controls should be monitored on a 24 by 7 basis. Appropriate escalation, response plans and procedures for physical and environmental incidents at DCs should be established and tested." (TRM, 2021)

Customers are solely responsible for determining the suitability of a cloud service in the context of safeguarding the data center from physical and environment threats.

OCI requires measures from its colocation suppliers to protect its assets in colocation facilities against physical and environmental threats. These requirements for colocation facilities include:

- Facilities must be monitored, staffed, and patrolled 24 hours a day, 7 days a week by dedicated and qualified onsite security personnel with the goal of preventing, detecting, and responding to incidents.
- All entry and exit points to the facility must be monitored 24 hours a day, 7 days a week, 365 days a year.
- Primary monitoring of video and alarms must be done by dedicated onsite security personnel located in a restricted or secure space within the facility perimeter.
- All alarms must be responded to immediately.
- Using a method of communication that is appropriate to the severity of the event, Oracle colocation suppliers must promptly report incidents such as security breaches, security incidents, and death or serious injuries to people or property, and operationally disruptive events within the facility or in the immediate vicinity.
- The onsite security team must physically respond within 15 minutes to emergency events, workplace disruptions, and system alarms in relation to services provided to Oracle.

For more information, see oracle.com/us/assets/supplier-security-standards-app2-1639575.pdf.

TRM Section 8.5.6

"The DC should have adequate physical access controls including: access granted to staff should be on a need-to have basis, and revoked promptly if access is no longer required; proper notification and approval for visitors to the DC. All visitors should be escorted by authorised staff at all times while in the DC; physical access points in the DC should be secured and monitored at all times; access to equipment racks should be restricted to authorized staff and monitored; access to keys and other physical access devices should be restricted to authorized staff, and replaced or changed promptly if they have been misplaced, lost or stolen; and segregation of delivery and common areas from security sensitive areas should be enforced." (TRM, 2021)

Customers are solely responsible for determining the suitability of a cloud service in the context of safeguarding the data center from physical and environment threats.

OCI requires measures from its colocation suppliers to protect its assets in colocation facilities against physical and environmental threats. These requirements for colocation facilities include:

- Colocation suppliers are responsible for ensuring that any personnel accessing Oracle spaces or assets are specifically authorized by Oracle. Oracle provides its colocation suppliers with a list of approved Oracle employees and vendors that are permitted to have access to the Oracle leased spaces. The colocation supplier must maintain access logs of all personnel entering Oracle spaces with full name, organization or company name, and date and time of entry and exit. Access lists for the Oracle leased spaces are reviewed with Oracle every six months, and access is removed for personnel who do not require it.
- Before access to facilities is granted to visitors, access must be confirmed by prearranged appointments, including approval for each visitor. Identities of all authorized visitors must be verified using government-issued identification. All visitors are escorted at all times.
- Facilities must be monitored, staffed, and patrolled 24 hours a day, 7 days a week by dedicated and qualified onsite security personnel with the goal of preventing, detecting, and responding to incidents.
- The facility must be equipped with an electronic, centrally managed access control system. The access control system records and stores entry and exit details for all facility personnel and visitors for at least 90 days.
- Physical keys, such as master keys that provide access to the Oracle leased spaces, storage, or office areas, must be appropriately managed, locked, and kept in a secure area. Manual or automated logging must provide accountability for all use of physical keys. Logs must be retained for one year. Oracle must be informed if keys are duplicated or replicated, or before they leave the facility.
- Supporting infrastructure located inside the facility, such as network infrastructure, demarcation points, communications, and any other infrastructure used to provide services to Oracle, must have physical security protections designed to ensure that access to those areas is limited to authorized personnel and is monitored.

For more information, see oracle.com/us/assets/supplier-security-standards-app2-1639575.pdf.

Conclusion

Oracle Cloud Infrastructure data centers are designed for security and availability of customer data. Oracle's physical security policies and practices are intended to reduce risks and help protect customer data against physical threats. Oracle's physical security standards and policies are company-specific, but they have been developed to align with various physical security industry initiatives. The goal is to balance prevention, detection, protection, and response, while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. For more information, see oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html.

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