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 the 2021 Technology Risk Management Guidelines

June 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 help you assess your use of Oracle cloud services in the context of the requirements applicable to you under the Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines. This document might 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, 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 TRM Guidelines are subject to periodic changes or revisions by the Monetary Authority of Singapore. The current version of the TRM Guidelines is available at 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 Corporation and might not always reflect changes in the regulations.

Revision History

The following revisions have been made to this document.

DATE	REVISION
June 2022	• Combined two existing papers under one title: *Advisory: Oracle Cloud Infrastructure Practices in the Context of the Technology Risk Management Guidelines* and *Advisory: Oracle Cloud Infrastructure and the Technology Risk Management Guidelines Issued by the Monetary Authority of Singapore in January 2021* • Updated to call out specific sections of the TRM Guidelines and provide more detailed information about how certain OCI services might help customers meet requirements
January 2022	Made the following updates to *Advisory: Oracle Cloud Infrastructure and the Technology Risk Management Guidelines Issued by the Monetary Authority of Singapore in January 2021*: • 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*
June 2021	Initial publication of *Advisory: Oracle Cloud Infrastructure Practices in the Context of the Technology Risk Management Guidelines*
April 2021	Initial publication of *Advisory: Oracle Cloud Infrastructure and the Technology Risk Management Guidelines Issued by the Monetary Authority of Singapore in January 2021*

Table of Contents

Introduction

The Monetary Authority of Singapore (MAS), 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 operating in Singapore with regard to risk management, cyber security, and IT outsourcing. For more information, see 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 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 MAS Technology Risk Management (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 OCI

Oracle's mission is to help people see data in new ways, discover insights, and unlock endless possibilities. Oracle provides numerous 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 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 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 docs.oracle.com/iaas/Content/home.htm.

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

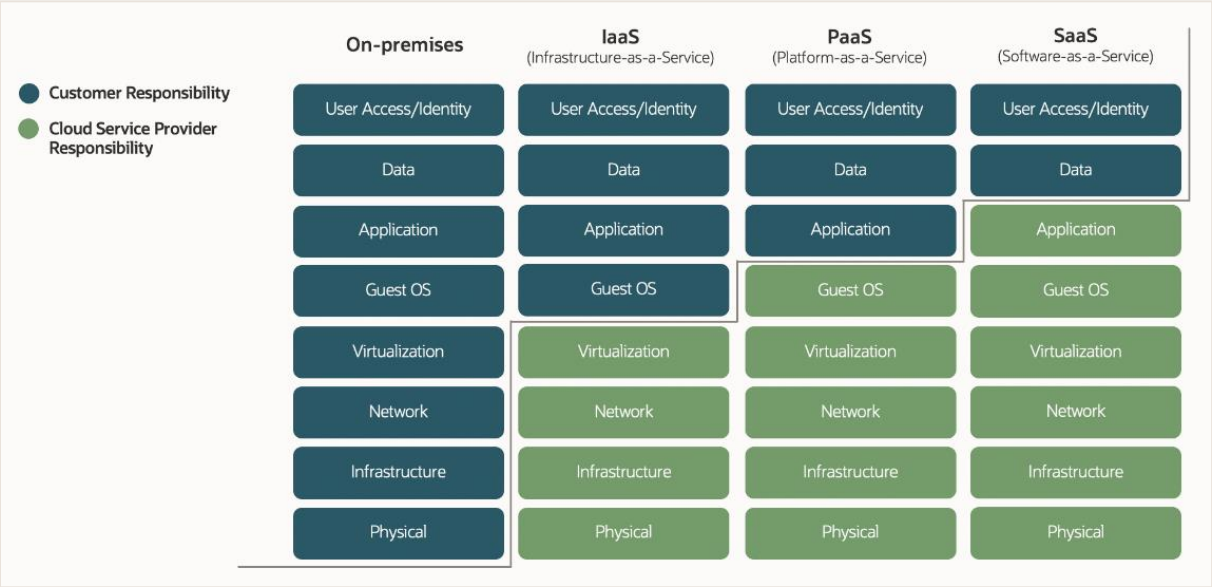

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Summary of the Technology Risk Management Guidelines

This section summarizes select sections of the TRM Guidelines, describes OCI's operational and security practices and services in the context of the guidelines, and offers recommendations for how customers can use OCI to address these requirements. Sections 1, 2, 5 and 6 of the TRM Guidelines are intentionally omitted because they are general references or refer solely to a customer responsibility.

Note: In the guidelines, the abbreviation *FI* stands for *financial institution*.

TRM Section 3.1: Role of the Board of Directors and Senior Management

"It is vital that the FI's board of directors and senior management ensure effective internal controls and risk management practices are implemented to achieve security, reliability, and resilience of its IT operating environment."

"Both the board of directors and senior management should have members with the knowledge to understand and manage technology risks, which include risks posed by cyber threats."

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 provides the following training and associated certifications to educate and train customers' directors and management to build, deploy, and maintain a cloud topology that's fault tolerant and that can be recovered quickly in the event of any outage:

- Oracle Cloud Infrastructure Certified Architect Associate
- Oracle Cloud Infrastructure Certified Architect Professional
- Oracle Cloud Infrastructure Certified Cloud Operations Associate

For more information about Oracle's certification programs to aid in the continuing education for Board of Directors and Senior Management, see oracle.com/education/.

TRM Section 3.2.1: Policies, Standards and Procedures

"The FI should establish policies, standards and procedures and, where appropriate, incorporate industry standards and best practices to manage technology risks and safeguard information assets in the FI. The policies, standards and procedures should also be regularly reviewed and updated, taking into consideration the evolving technology and cyber threat landscape."

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.

OCI provides the **Vulnerability Scanning** service, which might help you meet these requirements. Vulnerability Scanning helps improve the security posture in an OCI environment when configured to routinely check hosts for potential vulnerabilities. For more information, see docs.oracle.com/iaas/scanning/home.htm.

Oracle has implemented security policies to address security for both Oracle's internal operations and the services that Oracle provides to its customers. Oracle security policies apply to all Oracle personnel and contractors. These policies are generally aligned with International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 27002:2013 and ISO/IEC 27001:2013 standards and guide all areas of security within Oracle. For more information, see oracle.com/corporate/security-practices/corporate/.

TRM Section 3.3.2: Management of Information Assets

"The FI should maintain an inventory of all its information assets. The inventory should be reviewed periodically and updated whenever there are changes."

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.

OCI provides the following services and features that might help you meet these requirements:

- **Data Catalog** is a metadata management service that helps organizations discover data and support data governance. For more information, see docs.oracle.com/iaas/data-catalog/home.htm.
- **Resource Manager** is an OCI service that lets you automate the process of provisioning your OCI resources. For more information, see docs.oracle.com/iaas/Content/ResourceManager/home.htm.
- **Tagging** lets you add metadata to resources, which enables you to define keys and values and associate them with resources. You can use the tags to organize and list resources based on business needs. For more information, see docs.oracle.com/iaas/Content/Tagging/home.htm.

Oracle has requirements to maintain an accurate system inventory to enable effective general information systems management and operational security for the systems that it manages. For more information, see oracle.com/corporate/security-practices/corporate/information-assets-classification.html.

TRM Section 3.4: Management of Third Party Services

"The FI should assess and manage its exposure to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the third party before entering into a contractual agreement or partnership."

"On an ongoing basis, the FI should ensure the third party employs a high standard of care and diligence in protecting data confidentiality and integrity as well as ensuring system resilience."

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's Corporate Security Program is designed to protect the confidentiality, integrity, and availability of both Oracle and customer data, such as:

- The systems that customers rely on for cloud, technical support, and other services
- Oracle source code and other sensitive data, against theft and malicious alteration
- Personal and other sensitive information that Oracle collects in the course of its business, including customer, partner, supplier, and employee data residing in Oracle's internal IT systems

Oracle's security policies cover the management of security for both Oracle's internal operations and the services that Oracle provides to its customers, and apply to all Oracle personnel and contractors. These policies are aligned with the ISO/IEC 27002:2013 and ISO/IEC 27001:2013 standards and guide all areas of security within Oracle. For more information, see oracle.com/corporate/security-practices/corporate/.

TRM Section 3.5: Competency and Background Review

"The FI should ensure personnel, including contractors and service providers, have the requisite level of competence and skills to perform the IT functions and manage technology risks."

"A background check on personnel, who has access to the FI's data and IT systems, should be performed to minimise this risk [of insider threats]."

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 strongly emphasizes personnel security. The company has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities. These initiatives include personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions of Oracle policies.

In the US, Oracle uses an external screening agency to perform preemployment background investigations for newly hired US personnel. Personnel screening in other countries varies according to local laws, employment regulations, and local Oracle policy. To learn more about Oracle's global background check practices, see oracle.com/corporate/careers/background-check.html.

TRM Section 3.6: Security Awareness and Training

"A comprehensive IT security awareness training programme should be established to maintain a high level of awareness among all staff in the FI."

"The training programme should be conducted at least annually for all staff, contractors and service providers who have access to the FI's information assets."

"The training program should be reviewed periodically to ensure its contents remain current and relevant. The review should take into consideration changes in the FI's IT security policies, prevalent and emerging risks, and the evolving cyber threat landscape."

Customers are solely responsible for implementing, reviewing, and maintaining an IT security awareness training program.

OCI employees are required to complete Security Awareness Training when hired and annually thereafter. The course instructs employees on their obligations under Oracle privacy and security policies for the management of OCI systems. This course also covers data-privacy principles and data-handling practices. For more information, see oracle.com/corporate/security-practices/corporate/human-resources-security.html.

TRM Section 4.1: Risk Management Framework

"The FI should establish a risk management framework to manage technology risks. Appropriate governance structures and processes should be established, with well-defined roles, responsibilities, and clear reporting lines across the various organisational functions."

"The risk framework should also encompass the following components: risk identification . . . risk assessment . . . risk treatment . . . [and] risk monitoring, review and reporting. . . ."

"The FI should review the adequacy and effectiveness of its risk management framework regularly."

Customers are solely responsible for establishing a risk management framework that appropriately manages technology risks in their environment.

TRM Section 4.2.1: Risk Identification

"The FI should identify the threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third party service providers. Examples of security threats that could have a severe impact on the FI and its stakeholders include internal sabotage, malware and data theft."

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.

OCI offers the following services and features that might help you deal with technical risks in the IT environment:

- **Anomaly Detection** provides with a rich set of tools that you can use to identify unwanted events or observations in business data in real time so that you can act to avoid business disruptions. For more information, see docs.oracle.com/iaas/anomaly/using/home.htm.
- **Vulnerability Scanning** scans compute instances and virtual machines (VMs) to detect vulnerabilities within Oracle environments. For more information, see docs.oracle.com/iaas/scanning/home.htm.

Oracle conducts security tests of OCI services at least annually. Identified exploitable threats and vulnerabilities are investigated and tracked to resolution.

TRM Section 4.3: Risk Assessment

"The FI should perform an analysis of the potential impact and consequences of the threats and vulnerabilities on the overall business and operations. The FI should take into consideration financial, operational, legal, reputational and regulatory factors in assessing technology risks."

"To facilitate the prioritisation of technology risks, a set of criteria measuring and determining the likelihood and impact of the risk scenarios should be established."

Customers are solely responsible for performing a risk assessment and analyzing potential impact and consequences in their environment.

Oracle provides several resources to help customers perform their risk assessments and due diligence. Oracle provides customers with access to the security questionnaires, audit reports, and other information regarding Oracle's operational and security practices:

- Oracle Cloud Compliance site: oracle.com/corporate/cloud-compliance/
- Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Infrastructure: oracle.com/a/ocom/docs/oci-corporate-caiq.pdf
- Oracle Corporate Security Practices site: oracle.com/corporate/security-practices/

TRM Section 4.4.1: Risk Treatment

"The FI should develop and implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance. The IT control and risk mitigation approach should be subject to regular review and update, taking into account the changing threat landscape and variations in the FI's risk profile."

Customers are solely responsible for the implementation of risk mitigation and control measures, and establishing a risk tolerance level for their environment.

TRM Section 4.5: Risk Monitoring, Review and Reporting

"The FI should institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks."

"Significant risks should be monitored closely and reported to the board of directors and senior management. The frequency of monitoring and reporting should be commensurate with the level of risk."

"To facilitate risk reporting to management, technology risk metrics should be developed to highlight information assets that have the highest risk exposure. In determining the technology risk metrics, the FI should take into account risk events and audit observations, as well as applicable regulatory requirements."

Customers are solely responsible for assessing, monitoring, and reporting risks in their environment.

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

- **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.
- **Monitoring** enables customers to actively and passively monitor their cloud resources using metrics and alarms that notify them when metrics meet alarm-specific triggers. For more information, see docs.oracle.com/iaas/Content/Monitoring/home.htm.

TRM Section 7.1.1: IT Service Management Framework

"A robust IT service management framework . . . should comprise the governance structure, processes and procedures for IT service management activities including configuration management, technology refresh management, patch management, change management, software release management, incident management and problem management."

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.

TRM Section 7.2: Configuration Management

"The FI should implement a configuration management process to maintain accurate information of its hardware and software to have visibility and effective control of its IT systems."

"The FI should review and verify the configuration information of its hardware and software on a regular basis to ensure it is accurate and up-to-date."

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 employs standardized system hardening practices across OCI devices. For more information, see oracle.com/a/ocom/docs/oci-corporate-caiq.pdf.

TRM Section 7.3.1: Technology Refresh Management

"The FI should avoid using outdated and unsupported hardware or software, which could increase its exposure to security and stability risks. The FI should closely monitor the hardware's or software's end-of-support (EOS) dates as service providers would typically cease the provision of patches, including those relating to security vulnerabilities that are found after the EOS date."

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's Lifetime Support Policy puts customers in control of their upgrade strategy. Our flexible support policy stages make it easier for customers to plan and budget for Oracle's exclusive product upgrades. When it's time to upgrade, customers have rights to major product releases. For more information, see oracle.com/us/support/library/lifetime-support-technology-069183.pdf.

TRM Section 7.4: Patch Management

"A patch management process should be established to ensure applicable functional and non-functional patches (e.g. fixes for security vulnerabilities and software bugs) are implemented within a timeframe that is commensurate with the criticality of the patches and the FI's IT systems."

"Patches should be tested before . . . [being released]."

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.

OCI offers **Autonomous Database** on shared Exadata infrastructure, which might help you meet this requirement. With Autonomous Database on shared Exadata infrastructure, Oracle manages automatic maintenance updates and database patching. For more information, see docs.oracle.com/iaas/autonomous-database-shared/index.html.

TRM Section 7.5.1: Change Management

"The FI should establish a change management process to ensure changes to information assets are assessed, tested, reviewed and approved before implementation."

Customers are solely responsible for establishing a change management process to meet section 7.5 guidance.

You can use the following management features and services to help partially meet change management 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. For more information, see docs.oracle.com/iaas/Content/Identity/home1.htm.
- **Compartments** let you organize and isolate resources to make it easier to manage and secure access to them. For more information, see docs.oracle.com/iaas/Content/Identity/Tasks/managingcompartments.htm.

TRM Section 7.6.1: Software Release Management

"Segregation of duties in the software release process should be practiced to ensure no single individual has the ability to develop, compile and move software codes from one environment to another."

Customers are solely responsible for implementing policies and controls to meet section 7.6 guidance.

OCI offers the **Identity and Access Management (IAM)** service, which might help you partially meet this Software Release Management guidance, where segregation of duties can be implemented and audited. IAM lets

you control who has access to your cloud resources. You can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/iaas/Content/Identity/home1.htm.

OCI follows established software development and release management processes included within the Oracle Software Security Assurance (OSSA) process to ensure quality standards are being met. For more information, see oracle.com/support/assurance/index.html.

TRM Section 7.7: Incident Management

"The FI should establish an incident management framework with the objective of restoring an affected IT service or system to a secure and stable state, as quickly as possible, so as to minimise impact to the FI's business and customers."

"The incident management framework should minimally cover: the process and procedure for handling IT incidents, including cyber related incidents; maintenance and protection of supporting evidence for the investigation and diagnosis of incidents; and the roles and responsibilities of staff and external parties involved in recording, analysis, escalation, decision-making, resolution and monitoring of incidents."

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.

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

- **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 the configuration. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.
- **Data Safe** is a fully integrated cloud service focused on the security of data. 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.
- **Events** enables you to create automation based on the changes of resources throughout a tenancy. For more information, see docs.oracle.com/iaas/Content/Events/home.htm.

If Oracle determines that a confirmed security event involving personal information processed by Oracle has occurred, Oracle promptly notifies impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services at oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing.

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

TRM Section 8.1: System Availability

"IT systems should be designed and implemented to achieve the level of system availability that is commensurate with its business needs."

"Procedures should be established to respond to situations when pre-defined thresholds for system resources and system performance have been breached."

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.

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

- **Monitoring** is used to query metrics and manage alarms. Metrics and alarms help monitor the health, capacity, and performance of your cloud resources. For more information, see docs.oracle.com/iaas/Content/Monitoring/home.htm.
- **Oracle Active Data Guard** provides 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** is an advanced logical replication product that supports multimaster replication, hub and spoke deployment, and data transformation. GoldenGate provides 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.

Oracle deploys the OCI services on resilient computing infrastructure designed to maintain service availability and continuity if a performance impact or other service interruption affecting the availability of services occurs. Also, Oracle provides several different communication channels for customer notifications, which include the OCI Status website (ocistatus.oraclecloud.com), the Oracle Cloud Console, and the My Oracle Support site.

Oracle Cloud Service Level Agreements are described in the following documents:

- Oracle Cloud Hosting and Delivery Policies: oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
- Oracle PaaS and IaaS Public Cloud Services Pillar Document: oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf

TRM Section 8.2: System Recoverability

"The FI should establish systems' recovery time objectives (RTO) and recovery point objectives (RPO) that are aligned to its business resumption and system recovery priorities."

"The FI's disaster recovery plan should include procedures to recover systems from various disaster scenarios, as well as the roles and responsibilities of relevant personnel in the recovery process. The disaster recovery plan should be reviewed at least annually and updated when there are material changes to business operations, information assets or environmental factors."

Customers are given 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 you can use to plan for the disaster recovery of applications:

- **File Storage** supports snapshots for data protection of file systems. Creating a snapshot of an instance lets you capture the current state of the nonpersistent boot disk used by an instance. You can use the snapshot to restore a VM. For more information, see docs.oracle.com/iaas/Content/File/Tasks/managingsnapshots.htm.
- **Oracle Active Data Guard** provides 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** is an advanced logical replication product that supports multimaster replication, hub and spoke deployment, and data transformation. GoldenGate provides 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.

Oracle offers features for customers to use to back up and recover PaaS and IaaS components based on their RTO and RPO requirements. For more information, see docs.oracle.com/en/solutions/oci-best-practices/back-your-data1.html.

For more information to meet requirements, see Disaster Recovery Capabilities of Oracle Cloud and Disaster Recovery for Databases.

OCI is organized by data regions, which are built within a certain geography. Each region has one, two, or three availability domains, and each availability domain is divided into multiple fault domains. Whether the customer instances reside in a region with one availability domain or multiple availability domains, numerous layers of redundancy are available for data and service resiliency and backups through fault domains and cross-region replication. For more information about OCI regions and availability domains, see docs.oracle.com/iaas/Content/General/Concepts/regions.htm.

TRM Section 8.3: Testing of Disaster Recovery Plan

"The FI should perform regular testing of its disaster recovery plan to validate the effectiveness of the plan and ensure its systems are able to meet the defined recovery objectives."

"The testing of disaster recovery plan should comprise: various plausible disruption scenarios, including full and partial incapacitation of the primary or production site and major system failures; and recovery dependencies between information assets, including those managed by third parties."

Customers are responsible for designing, developing, and implementing procedures for recovering their applications in accordance with their own recovery plans. Customers are also responsible for periodically testing such plans to help meet the availability commitments and requirements of their customers.

TRM Section 8.4: System Backup and Recovery

"The FI should establish a system and data backup strategy, and develop a plan to perform regular backups so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted."

"To ensure data availability is aligned with the FI's business requirements, the FI should institute a policy to manage the backup data life cycle, which includes the establishment of the frequency of data backup and data retention period, management of data storage mechanisms, and secure destruction of backup data."

Customers are solely responsible for developing a data backup strategy and implementing a backup plan.

As a cloud provider, OCI generally has no insight into the data stored or processed on OCI. However, OCI offers several building blocks that you can use to support system backup and recovery plans:

- **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/home.htm.
- **Oracle Active Data Guard** provides 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/.

OCI provides recommendations for creating resilient architectures and backing up customer data, applications, and operating environments to meet RPO and RTO requirements at docs.oracle.com/en/solutions/oci-best-practices/back-your-data1.html.

TRM Section 8.5: Data Centre Resilience

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."

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 organization's 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.

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."

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 the following ones:

- 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.

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."

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 the following ones:

- 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.

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."

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 organization's use of the cloud service and business processes meet these requirements.

When setting up an account, you choose a home region in which to initially locate the tenancy. 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 a 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** 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/home.htm.
- **Compute** 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/en-us/iaas/Content/Compute/home.htm.
- **Oracle Active Data Guard** provides 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** is an advanced logical replication product that supports multimaster replication, hub and spoke deployment, and data transformation. GoldenGate provides 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

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."

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 the following ones:

- 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.

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."

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 the following ones:

- 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.

TRM Section 9: Access Control

Section 9.1.2: User Access Management: ***"The FI should establish a user access management process to provision, change and revoke access rights to information assets. Access rights should be authorised and approved by appropriate parties, such as the information asset owner."***

Section 9.2.1: Privileged Access Management: ***"Users granted privileged system access have the ability to inflict severe damage on the stability and security of the FI's IT environment. Access to privileged accounts should only be granted on a need-to-use basis; activities of these accounts should be logged and reviewed as part of the FI's ongoing monitoring."***

Section 9.3.2: Remote Access Management: ***"The FI should ensure remote access to the FI's information assets is only allowed from devices that have been secured according to the FI's security standards."***

Customers are responsible for all aspects of access management to their facilities, applications, devices, information, and data stored or processed in their environment.

OCI offers the following features and services that might help you meet these access control requirements:

- **Identity and Access Management (IAM)** lets customers control who has access to their cloud resources. IAM supports multifactor authentication and identity federation with SAML-based identity providers, which you can configure for more security. You can also define password complexity and lockout requirements for the service environment. For more information, see docs.oracle.com/iaas/Content/Identity/home1.htm.
- **Vault** key management provides centralized management of the encryption of customer data with keys that you control. For more information, see docs.oracle.com/iaas/Content/KeyManagement/home.htm.

Oracle creates a tenancy for each customer, which is an isolated partition within OCI where customers can create, organize, and administer their cloud resources. Customer isolation lets you deploy application and data assets in an environment that commits full isolation from other tenants and Oracle's staff.

Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. Users with access to the customer environment are reviewed at least quarterly, and all access is logged and audited in the event of employee termination, death, or resignation. Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.

For more information, see oracle.com/corporate/security-practices/corporate/access-control.html.

TRM Section 10: Cryptography

Section 10.1.2: Cryptographic Algorithm and Protocol: ***"The FI should adopt cryptographic algorithms from well-established international standards. The FI should also select an appropriate algorithm and encryptions key length that meet its security objectives and requirements."***

Section 10.2: Cryptographic Key Management: ***"Cryptographic key management policy, standards and procedures covering key generation, distribution, installation, renewal, revocation, recovery and expiry should be established. The FI should ensure cryptographic keys are securely generated and protected from unauthorised disclosure."***

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.

OCI offers the **Vault** service, which might 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 (HSMs) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification.

The key encryption algorithms that the Vault service supports includes the Advanced Encryption Standard (AES), the Rivest-Shamir-Adleman (RSA) algorithm, and the elliptic curve digital signature algorithm (ECDSA). You can create and use AES symmetric keys and RSA asymmetric keys for encryption and decryption. You can also use RSA or ECDSA asymmetric keys for signing digital messages. For more information, see docs.oracle.com/iaas/Content/KeyManagement/home.htm.

Oracle has corporate standards that define the approved cryptographic algorithms and protocols. Oracle products and services are required to use only up-to-date versions of approved security-related implementations, as guided by industry practice. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms.

TRM Section 11.1: Data Security

"The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, or transmission of its confidential data taking into consideration . . . data in motion . . . data at rest . . . [and] data in use. . . ."

"The FI should ensure systems managed by the FI's service providers are accorded the same level of protection and subject to the same security standards."

Customers are responsible for implementing data loss prevention policies and implementing controls to ensure that data is protected from unauthorized access.

As a cloud provider, OCI generally has no insight into the data stored or processed on OCI. However, OCI provides the following services and features that might help you meet this requirement:

- **Identity and Access Management (IAM)** lets you control who has access to your cloud resources. You can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/iaas/Content/Identity/home1.htm.
- **Audit** helps you track activity in the IT environment. For more information, see docs.oracle.com/iaas/Content/Audit/home.htm.
- **Health Checks** helps you monitor the health of endpoints. For more information, see docs.oracle.com/iaas/Content/HealthChecks/home.htm.

- **Monitoring** is used to query metrics and manage alarms. Metrics and alarms help monitor the health, capacity, and performance of cloud resources. For more information, see docs.oracle.com/iaas/Content/Monitoring/home.htm.
- **Vault** helps you centrally manage the encryption keys that protect data and the secret credentials that you use to access resources. For more information, see docs.oracle.com/iaas/Content/KeyManagement/home.htm.

TRM Section 11.2: Network Security

"The FI should install network security devices such as firewalls to secure the network between the FI and the Internet, as well as connections with third parties."

"To minimise the risk of cyber threats, such as lateral movement and insider threat, the FI should deploy effective security mechanisms to protect information assets."

Customers are responsible for securely configuring network elements such as virtual networking, load balancing, domain name system (DNS), and gateways.

OCI provides the following services and features that might help you meet this requirement:

- **Load Balancing** provides automated traffic distribution from one entry point to multiple servers reachable from a virtual cloud network (VCN). The service offers a load balancer with a public or private IP address, and provisioned bandwidth. For more information, see docs.oracle.com/iaas/Content/Balance/home.htm.
- **API Gateway** enables you to create governed HTTP/S interfaces for other OCI services, including Functions, Container Engine for Kubernetes, and Container Registry. API Gateway also provides policy enforcement such as authentication and rate-limiting to HTTP/S endpoints. For more information, see docs.oracle.com/iaas/Content/APIGateway/home.htm.
- **Isolated Network Virtualization** helps to prevent attacks on customer tenancies with isolated network virtualization. A foundational element of OCI's security-first architecture, isolated network virtualization helps to prevent malware attacks with a custom-designed SmartNIC to isolate and virtualize the network. For more information, see oracle.com/sg/security/cloud-security/isolated-network-virtualization/.
- **DNS** lets you create and manage your DNS zones. You can create zones, add records to zones, and allow OCI's edge network to handle your domain's DNS queries. For more information, see docs.oracle.com/iaas/Content/DNS/Tasks/managingdnszones.htm.

By default, customer communications with OCI services are done using strong TLS ciphers and configuration to secure customer data in transit and avoid man-in-the-middle attacks. As a further defense in depth, customer commands to the services are digitally signed using public keys, to prevent any tampering. The services also deploy proven, industry-leading tools and mechanisms to help mitigate distributed denial of service (DDoS) attacks and maintain high availability. For more information, see docs.oracle.com/iaas/Content/Security/Concepts/security_overview.htm.

TRM Section 11.3.1: System Security

"The security standards for the FI's hardware and software (e.g., operating systems, databases, network devices and endpoint devices) should outline the configurations that will minimise their exposure to cyber threats. The standards should be reviewed periodically for relevance and effectiveness."

Customers are responsible for securely configuring and managing compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform (database configuration) services. This customer responsibility includes implementing hypervisor security and configuring permissions and network access controls to allow hosts to communicate correctly and enable devices to attach or mount the correct storage.

OCI provides the following services and features that might help you meet this requirement:

- **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 to monitor 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/using/index.htm.
- **Data Safe** is a fully integrated cloud service focused on the security of data. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases. Features include security assessment, user assessment, data discovery, data masking, and activity auditing . For more information, see docs.oracle.com/iaas/data-safe/index.html.

Oracle has a long history of enterprise-class secure hardware development. Our Hardware Security team is responsible for designing and testing the security of the hardware used to deliver OCI services. This team works with our supply chain and tests hardware components to validate them against rigorous OCI hardware security standards. This team also works closely with our product development functions to ensure that hardware can be returned to a pristine, safe state after customers release it.

TRM Section 11.4.1: Virtualisation Security

"The FI should ensure security standards are established for all components of a virtualisation solution."

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

Oracle designed the OCI architecture for security of the platform through isolated network virtualization, highly secure firmware installation, a controlled physical network, and network segmentation. Isolated network virtualization prevents attacks on customer tenancies with a custom-designed SmartNIC that isolates and virtualizes the network. For more information, see oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf.

OCI offers shielded compute instances to harden firmware security on bare metal hosts and VMs to defend against malicious boot-level software. For more information, see docs.oracle.com/iaas/Content/Compute/References/shielded-instances.htm.

TRM Section 12: Cyber Security Operations

Section 12.1.1: Cyber Threat Intelligence and Information Sharing: ***"To maintain good cyber situational awareness, the FI should establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to the FI's business and IT environment. Cyber-related information would include cyber events, cyber threat intelligence and information on system vulnerabilities."***

Section12.2.1: Event Monitoring and Detection: ***"The FI should establish a security operations center or acquire managed security services."***

Section 12.3.1: Cyber Incident Response and Management: ***"The FI should establish a cyber incident response and management plan to swiftly isolate and neutralise a cyber threat and to securely resume affected services. The plan should describe communication, coordination and response procedures to address plausible cyber threat scenarios."***

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.

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

- **Monitoring** is used to query metrics and manage alarms. Metrics and alarms help monitor the health, capacity, and performance of cloud resources. For more information, see docs.oracle.com/iaas/Content/Monitoring/home.htm.
- **Cloud Guard** helps you monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud. Use this cloud native service to examine your OCI resources for security weaknesses related to configuration, and your 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.
- **Logging Analytics** lets you index, enrich, aggregate, explore, search, analyze, correlate, visualize, and monitor all log data from applications and system infrastructure. For more information, see docs.oracle.com/iaas/logging-analytics/index.html.
- **Events** lets you create automation based on the state changes of resources throughout a tenancy. For more information, see docs.oracle.com/iaas/Content/Events/home.htm.

Oracle has processes to evaluate and respond to any security event. Oracle's 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 (LoBs). GIS defines roles and responsibilities for the incident response teams embedded within the Lines of Business (LoBs). All LoBs must comply with GIS incident response guidance about detecting events and timely corrective action. For more information, see oracle.com/corporate/security-practices/corporate/security-incident-response.html.

TRM Section 13: Cyber Security Assessment

Section 13.1.1: Vulnerability Assessment: ***"The FI should establish a process to conduct regular vulnerability assessment (VA) on their IT systems to identify security vulnerabilities and ensure risk arising from these gaps are addressed in a timely manner. The frequency of VA should be commensurate with the criticality of the IT system and the security risk to which it is exposed."***

Section 13.2.1: Penetration Testing: ***"The FI should carry out penetration testing (PT) to obtain an in-depth evaluation of its cyber security defences. A combination of blackbox and greybox testing should be conducted for online financial services."***

Section 13.6.1: Remediation Management: ***"A comprehensive remediation process should be established to track and resolve issues identified from the cyber security assessments or exercises. The process should minimally include the following: severity assessment and classification of an issue; timeframe to remediate issues of different severity; and risk assessment and mitigation strategies to manage deviations from the framework."***

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 organization's use of the cloud service and business processes meet these requirements.

OCI provides the following services and features that might help you meet these requirements:

- **Isolated Network Virtualization** prevents attacks on customer tenancies with isolated network virtualization. A foundational element of OCI's security-first architecture, isolated network virtualization disrupts 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/.
- **Vulnerability Scanning** helps improve your organization's security posture by routinely checking compute instances and container images for potential vulnerabilities. For more information, see docs.oracle.com/iaas/scanning/home.htm.

Conclusion

Oracle Cloud Infrastructure 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, we strongly recommend 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.