Advisory: Contract Checklist for Oracle Cloud Infrastructure and the Monetary Authority of Singapore (MAS) Guidelines on Outsourcing

April 2022, Version 1.0

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 in assessing your use of Oracle Cloud Infrastructure (OCI) in the context of the requirements applicable to you under the MAS Outsourcing Guidelines. This may also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document. The information in this document is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied upon 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 MAS Outsourcing Guidelines are subject to periodic changes or revisions by the Monetary Authority of Singapore. The current version of the MAS Guidelines on Outsourcing is available at mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Outsourcing-Guidelines_Jul-2016-revised-on-5-Oct-2018.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 may not always reflect changes in the regulations.

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. These guidelines address risk management, cyber security, and IT outsourcing. For more information, see mas.gov.sg/regulation.

Document Purpose

We want to make it easier for financial institutions to identify the sections of the Oracle Cloud services contract that pertain to the requirements in the MAS Guidelines on Outsourcing. This document is also intended to provide relevant information related to Oracle to assist you in meeting your obligations and determining the suitability of using Oracle products in relation to the MAS outsourcing guidelines. Certain sections of this document provide a list of relevant guidelines along with a reference to the relevant sections of the Oracle Cloud services contract and a short explanation to help you conduct your review of the Oracle Cloud services.

The following customer-specific contract documents are referenced throughout this paper:

- **Oracle Cloud Services Contract**: An Oracle Cloud Services Agreement (CSA) or Oracle Master Agreement (OMA) with Schedule C (Cloud)
- **FSA**: The Oracle Financial Services Addendum to the Oracle Cloud Services Agreement (CSA)
- **Ordering Document**: Oracle Cloud services order
- **Services Specifications**: Service-specific components, including the Oracle Cloud Hosting and Delivery Policies with applicable Services Pillar Documents and the Oracle Data Processing Agreement

About Oracle Cloud Infrastructure

Oracle's mission is to help people see data in new ways, discover insights, and unlock endless possibilities. Oracle provides several cloud solutions tailored to customers' needs. These 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 solely reference Oracle Cloud Infrastructure (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 oracle.com/cloud/.

The Cloud Shared Management Mode

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

Oracle provides best-in-class security technology and operational processes to Oracle's secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle cloud environments. 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 at docs.oracle.com/iaas/Content/home.htm.

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

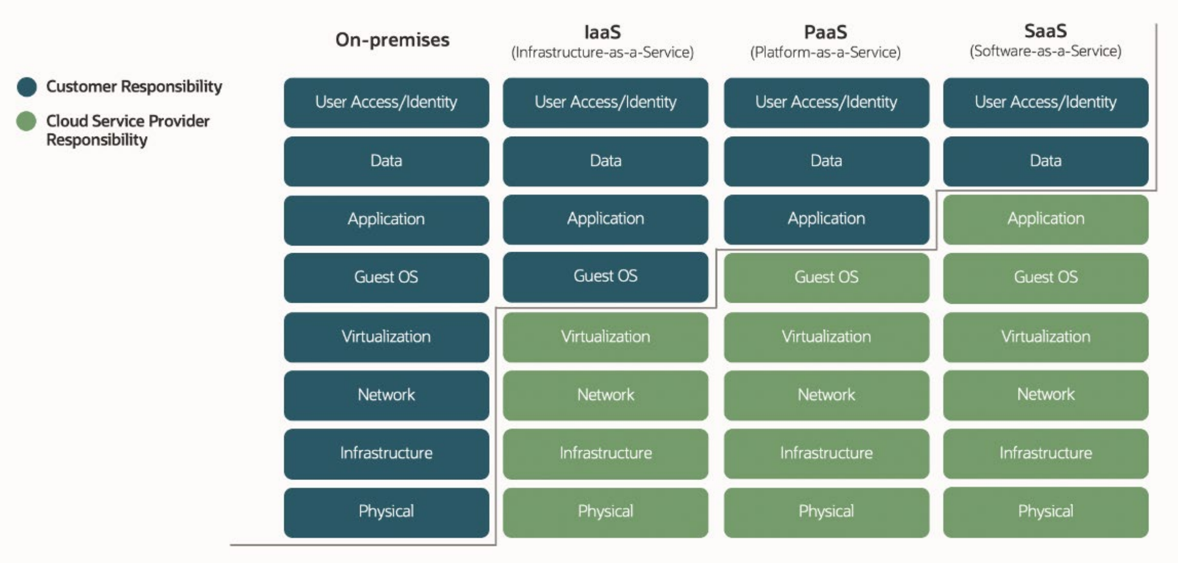
Customer Responsibility
Cloud Service Provider Responsibility
On-premises
IaaS (Infrastructure-as-a-Service)
PaaS (Platform-as-a-Service)
SaaS (Software-as-a-Service)
User Access/Identity
Data
Application
Guest OS
Virtualization
Network
Infrastructure
Physical

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

MAS Guidelines on Outsourcing

This section provides an overview of select regulatory considerations for Singapore financial institutions that engage with MAS on outsourcing, as specified by the MAS Guidelines on Outsourcing. Omitted portions have been identified as general guidance for financial institutions evaluating an outsourcing relationship, and not specific to the use of OCI services.

Customers are solely responsible for determining the suitability of cloud infrastructure in the context of the MAS requirements and these outsourcing guidelines. However, the following Oracle practices and resources may assist you in the evaluation of cloud services within the shared management model.

4. Engagement with MAS on Outsourcing

The following tables cover the guidelines provided in section 4 of the MAS Guidelines on Outsourcing.

4.1 Observance of the Guidelines

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
4.1.3	MAS may require an institution to modify, make alternative arrangements or reintegrate an outsourced service into the institution where one of the following circumstances arises:	FSA, Section 3	Under Section 3 of the FSA, customers have the right to terminate the cloud services in the following situations: Termination due to regulatory requirements • Continued use of the services would cause customers to violate applicable law and regulation upon the conclusion made by the regulator. • Termination requested based on express instruction issued by the regulator where the services are considered as an impediment to effective supervision over the customer. Termination due to insolvency • Oracle has become insolvent or resolved to go into liquidation. • A proposal is made for entering into any compromise or arrangement with any or all of Oracle's creditors. • A receiver is appointed over all or substantially all the assets of Oracle.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
4.1.3 (a)	An institution fails or is unable to demonstrate a satisfactory level of understanding of the nature and extent of risk arising from the outsourcing arrangement;	• Oracle Cloud Compliance: oracle.com/corporate/cloud-compliance • Risk Management Resiliency Program: oracle.com/a/ocom/docs/corporate/oracle-risk-management-resiliency-program-ds.pdf • Oracle Corporate Security Practices: oracle.com/corporate/security-practices	Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of "attestations." These attestations provide independent assessment of the security, privacy, and compliance controls of the applicable Oracle Cloud services and can assist with compliance and reporting. Such attestations include CSA STAR, SOC, and ISO/IEC 27001, 27017, and 27018. Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for critical business operations. Additionally, Oracle has formal policies to help deliver cloud products to its customers. See the Oracle Corporate Security Practices website for details.
4.1.3 (b)	An institution fails or is unable to implement adequate measures to address the risks arising from its outsourcing arrangements in a satisfactory and timely manner;	• Oracle Corporate Security Practices: oracle.com/corporate/security-practices • OCI CAIQ: oracle.com/a/ocom/docs/oci-corporate-caiq.pdf • Oracle Compliance Documents in Console: docs.oracle.com/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm	Oracle provides several resources to assist its customers in conducting necessary risk assessments and due diligence. Oracle provides customers with access to security questionnaires known as Consensus Assessment Initiative Questionnaires (CAIQs), audit reports, and other information regarding Oracle's operational and security practices.
4.1.3 (c)	Adverse developments arise from the outsourcing arrangement that could impact an institution;	• Oracle Corporate Security Practices: oracle.com/corporate/security-practices/corporate • Incident Response: oracle.com/corporate/security-practices/corporate/security-incident-response.html • OCI Status: ocistatus.oraclecloud.com • Oracle Cloud Console • My Oracle Support • DPA	Per the Oracle Corporate Security Practices, Oracle evaluates and responds to security incidents when Oracle suspects that Oracle-managed customer data has been improperly handled or accessed. The Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to such security incidents. Upon discovery of a security incident, Oracle 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 to improve security posture and defense in depth. If Oracle determines that a confirmed security incident involving personal information processed by Oracle has occurred, Oracle promptly notifies impacted customers in accordance with its contractual and regulatory responsibilities as defined in the Oracle Data Processing Agreement (DPA). Additionally, depending on the service infrastructure type and notification scenario (Outage, Maintenance, Informational, Action Required), Oracle provides several different communication channels used for customer notifications including through OCI Status, Oracle Cloud Console, and My Oracle Support.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
4.1.3 (d)	MAS' supervisory powers over the institution and ability to carry out MAS' supervisory functions in respect of the institution's services are hindered;	FSA, Section 2 DPA, Section 7	Oracle enables its customers' regulators, including MAS, to carry out its supervisory functions in respect of the financial institutions. Such rights are addressed in the Oracle FSA, as follows: • Section 2.1 further provides that a customer's regulator may audit Oracle as required by applicable law. • Section 2.4 explicitly acknowledges the information-gathering and investigatory powers of resolution authorities. Also refer to Section 2.5 of the FSA, which expressly states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law. Additionally, Section 7 (Audit Rights) of the Oracle Data Processing Agreement (DPA) stipulates Oracle will cooperate with regulator audits with Oracle's obligation under applicable laws.
4.1.3 (e)	The security and confidentiality of the institution's customer information is lowered due to changes in the control environment of the service provider;	Oracle Corporate Security Practices: oracle.com/corporate/security-practices	Oracle has a comprehensive change management process as a core requirement of its commitment to security, availability, and confidentiality. The change management process is reviewed annually, at a minimum, and outlines the processes and procedures to be followed for each change. The process incorporates segregation of duties and requires changes to be approved and tested prior to implementation. All change requests are documented in an electronic, access-controlled ticketing system. The workflow prevents the ticket from being moved into the scheduled or implementation phase without the required review and approval of child tickets being in the closed state. All changes must be peer reviewed prior to implementation. The reviewer is typically a member of the same team with knowledge of the in-scope system service who can technically review the change for accuracy and potential issues. Changes that have the potential to have a significant impact on customers are also required to have a documented approval from the manager of the team managing the service.

4.2 Notification of Adverse Developments

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
4.2.1	An institution should notify MAS as soon as possible of any adverse development arising from its outsourcing arrangements that could impact the institution. Such adverse developments include any event that could potentially lead to prolonged service failure or disruption in the outsourcing arrangement, or any breach of security and confidentiality of the institution's customer information.	• Resilience Management and Business Continuity: oracle.com/corporate/security-practices/corporate/resilience-management • DPA, Section 8.2 • CSA, Section 15.2 • Oracle Cloud Console • My Oracle Support	Oracle provides various resources, such as compliance reports and guidance documents, through the Oracle Cloud Console and My Oracle Support that may assist customers in their dialogue with competent authorities. In addition, as required by applicable law or regulation, Oracle provides customers and their regulators with necessary information (including summaries of reports and documents) regarding the activities outsourced to Oracle. Oracle has formal processes in place to inform customers of any personal data breaches impacting them. Oracle is contractually bound to notify customers of personal data breach incidents, their descriptions and nature, measures taken for mitigation, and the type of information affected. Oracle uses the Common Vulnerability Scoring System (CVSS) to report the relative severity of security vulnerabilities when it discloses security issues affecting Oracle products. Refer to Section 8.2 of the Oracle Data Processing Agreement (DPA) where it identifies that customers would be notified of a personal information breach without undue delay within 24 hours. Section 15.2 of the CSA discusses party notification requirements generally and how Oracle provides notices about the services via the customer portal.

5. Risk Management Practices

The following tables cover the guidelines provided in section 5 of the MAS Guidelines on Outsourcing.

5.4 Assessment of Service Providers

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.4.1	In considering, renegotiating or renewing an outsourcing arrangement, an institution should subject the service provider to appropriate due diligence processes to assess the risks associated with the outsourcing arrangements.	• Oracle Corporate Security Practices: oracle.com/corporate/security-practices • Risk Management Resiliency Program: oracle.com/corporate/security-practices/corporate/resilience-management	Oracle has implemented protective measures for identifying, analyzing, measuring, mitigating, responding to, and monitoring risk specific to its cloud services organizations. Risk assessments are performed annually across Oracle cloud services to identify threats and risks that could impact the security, confidentiality, or availability of the system. Risks are reviewed, assigned an owner, and remediated in line with the Oracle cloud services risk management assessment program. See also Section 4.1.3 (a) and (b) in a preceding table.
5.4.2	An institution should assess all relevant aspects of the service provider, including its capability to employ a high standard of care in the performance of the outsourcing arrangement as if the service is performed by the institution to meet its obligations as a regulated entity. The due diligence should also take into account the physical and IT security controls the service provider has in place, the business reputation and financial strength of the service provider, including the ethical and professional standards held by the service provider, and its ability to meet obligations under the outsourcing arrangement. Onsite visits to the service provider, and where possible, independent reviews and market feedback on the service provider, should also be obtained to supplement the institution's assessment.	• See Sections 4.1.3 (a) and (b) in a preceding table. • See Sections 5.4.3 (a) and (b) later in this table.	See Sections 4.1.3 (a) and (b) in a preceding table. See Sections 5.4.3 (a) and (b) later in this table.
5.4.3	The due diligence should involve an evaluation of all relevant information about the service provider. Information to be evaluated includes the service provider's:	N/A	N/A

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.4.3 (a)	experience and capability to implement and support the outsourcing arrangement over the contracted period;	• About Oracle Corporation: oracle.com/corporate • Oracle Corporate Facts: oracle.com/corporate/corporate-facts.html	Oracle provides products and services that address enterprise information technology (IT) environments. Our products and services include applications and infrastructure offerings that are delivered worldwide through various flexible and interoperable IT deployment models. Our customers include businesses of many sizes, government agencies, educational institutions, and resellers. Using Oracle technologies, our customers build, deploy, run, manage, and support their internal and external products, services, and business operations.
5.4.3 (b)	financial strength and resources;	Oracle Investor Relations: investor.oracle.com/home/default.aspx	As of FY2021, Oracle had $40 billion total GAAP revenue and 133,000 employees serving 430,000 customers in 175 countries. For more information about Oracle's financials, visit our Investor Relations website.
5.4.3 (c)	corporate governance, business reputation and culture, compliance, and pending or potential litigation;	• Oracle's Corporate Governance Guidelines: oracle.com/assets/cg-guidelines-176734.pdf • Oracle Employee Code of Ethics and Business Conduct: oracle.com/assets/cebc-176732.pdf	Oracle is committed to upholding the highest standards of business ethics and sound corporate governance practices.
5.4.3 (d)	security and internal controls, audit coverage, reporting and monitoring environment;	• Oracle Corporate Security Program: oracle.com/corporate/security-practices/corporate • Oracle Business Assessment & Audit: oracle.com/corporate/security-practices/corporate/governance/business-assessment-audit • Oracle Cloud Compliance: oracle.com/corporate/cloud-compliance • Oracle Cloud Observability and Management Platform: oracle.com/manageability	Oracle's Corporate Security Program is designed to protect the confidentiality, integrity, and availability of both Oracle and customer data, such as: • The mission-critical 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 Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27002:2013 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2013 standards, and guide all areas of security within Oracle. Oracle Cloud Infrastructure (OCI) services are certified per specific industry and government standards such as ISO/IEC 27001:2013, AICPA SSAE Number 18 (SOC), Payment Card Industry Data Security Standards (PCI DSS), and other standards. Additionally, Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of "attestations." These attestations can assist in your compliance and reporting, providing independent assessment of the security, privacy, and compliance controls of the applicable Oracle cloud services. In reviewing these third-party attestations, it is important that you consider that they are generally specific to a certain cloud service and may also be specific to a certain data center or geographic region.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
			Oracle monitors its environment 24x7x365 for potential security incidents. Alerts are sent to Oracle's IT security and cloud security operations teams for review and response to potential threats. Oracle customers are responsible for monitoring their tenancies for indicators of compromise and addressing their security events. OCI provides the Oracle Cloud Observability and Management Platform, which is a comprehensive set of management, diagnostic, and analytics services that help customers manage their OCI tenancy while reducing troubleshooting time, reducing likelihood of outages, and enabling IT to manage applications. The platform provides visibility across applications by using advanced analytics to automatically detect anomalies and enable quick remediation in near-real time. The platform includes services such as Logging, Monitoring, Notifications, Database Management, and Application Performance Monitoring.
5.4.3 (e)	risk management framework and capabilities, including technology risk management and business continuity management in respect of the outsourcing arrangement;	Risk Management Resiliency Program: oracle.com/corporate/security-practices/corporate/resilience-management	Oracle has implemented protective measures for identifying, analyzing, measuring, mitigating, responding to, and monitoring risk specific to its cloud services organizations. Risk assessments are performed annually across Oracle cloud services to identify threats and risks that could impact the security, confidentiality, or availability of the system. Risks are reviewed, assigned an owner, and remediated in line with the Oracle cloud services risk management assessment program.
5.4.3 (f)	disaster recovery arrangements and disaster recovery track record;	Risk Management Resiliency Disaster Recovery: oracle.com/corporate/security-practices/corporate/resilience-management/disaster-recovery.html	Oracle's Risk Management Resiliency Program (RMRP) objective is to establish a business-resiliency framework in order to help provide an efficient response to business-interruption events affecting Oracle's internal operations. Disaster recovery is a key subprogram of Oracle RMRP. Oracle's corporate Disaster Recovery (DR) plan focuses on the resiliency of computing infrastructure supporting Oracle's internal operations. Oracle's production data centers are geographically separated and have component and power redundancy, with backup generators in place for availability of data center resources in case of an impacting event. Oracle's DR plan leverages this separation of data centers in conjunction with other recovery strategies to both protect against disruption and enable recovery of services.
5.4.3 (g)	reliance on and success in dealing with sub-contractors;	• Oracle Supply Chain Security and Assurance: oracle.com/corporate/security-practices/corporate/supply-chain • My Oracle Support, Doc ID 111.2: support.oracle.com/portal • FSA, Section 6.1	Oracle may use subprocessors or strategic subcontractors for some of its cloud services. Oracle reviews all of its subcontractors that provide services to Oracle as part of its cloud services according to published criteria to determine the status of such subcontractors. Oracle publishes a list of its subprocessors and strategic subcontractors (collectively "subcontractors") to customers through My Oracle Support. Customers have a 30-day period to object to Oracle's use of such subcontractors. Under Section 6.1 of the FSA, Oracle's use of any subcontractors will not diminish Oracle's responsibility toward a customer under the Oracle Cloud services contract and Oracle will appropriately oversee a subcontractor's performance.
5.4.3 (h)	insurance coverage;	• Oracle Cloud Ordering Document	Oracle maintains various types and levels of insurance from highly rated insurance carriers covering its locations on a worldwide basis. Oracle generally takes out and maintains certain insurance coverages. Through insurance and/or operating cash, Oracle has the ability to pay the limits on liability set out in the Oracle Cloud services contracts. Oracle contracts may specify applicable insurance coverage and limits in the Ordering Document.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.4.3 (i)	external environment (such as the political, economic, social and legal environment of the jurisdiction in which the service provider operates);	• Oracle Cloud Regions: oracle.com/cloud/architecture-and-regions • OCI Regions and Availability Domains: docs.oracle.com/iaas/Content/General/Concepts/regions.htm	Oracle operates within various regions across the globe. Each region is composed of one of more physically isolated and fault-tolerant data centers (also named *availability domains*). When customers set up their Oracle account, they choose a data center region in which to initially locate their tenancy, and their content is hosted within that region unless the customer chooses to move their content outside of the region.
5.4.3 (j)	ability to comply with applicable laws and regulations and track record in relation to its compliance with applicable laws and regulations.	• Oracle Code of Ethics and Business Conduct: oracle.com/assets/cebc-176732.pdf • Oracle Corporate Governance Guidelines: oracle.com/assets/cg-guidelines-176734.pdf • Oracle Cloud Compliance: oracle.com/corporate/cloud-compliance	Oracle has established a Code of Ethics and Business Conduct applicable to our employees, partners, and suppliers to promote and maintain the highest ethical standards and compliance with the law. Oracle's Board of Directors has adopted Corporate Governance Guidelines and committee charters to help ensure it has the necessary authority and procedures in place to oversee the work of management and to exercise independence in evaluating Oracle's business operations. These guidelines allow the Board to align the interests of directors and management with those of Oracle's shareholders. In addition, Oracle provides general information and technical recommendations for the use of its cloud services in the form of "advisories." These advisories are provided to help you in your determination of the suitability of using specific Oracle cloud services and to assist you in implementing specific technical controls that may help you meet your compliance obligations.
5.4.4	The institution should ensure that the employees of the service provider undertaking any part of the outsourcing arrangement have been assessed to meet the institution's hiring policies for the role they are performing, consistent with the criteria applicable to its own employees.	• Oracle Background Check process: oracle.com/corporate/careers/background-check.html#apac • Oracle Human Resources Security: oracle.com/corporate/security-practices/corporate/human-resources-security.html	Oracle performs background checks on candidates for hire in accordance with local laws and regulations as well as local Oracle policy. Employees are required to complete the Ethics and Business Conduct, Information Protection Awareness, and the Anti-Corruption and Foreign Corrupt Practices Act online courses upon hire. Oracle employees are also required to complete annual security awareness training in accordance with the Information Security Policy, which outlines the process and procedures to report incidents.

5.5 Outsourcing Agreement

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.5.1	Contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in the outsourcing arrangement should be carefully and properly defined in written agreements.	• Oracle Cloud Hosting and Delivery Policies • DPA • Oracle PaaS and IaaS Public Cloud Services Pillar Document	Contractual terms governing the outsourcing relationship and obligations between you and Oracle are documented in the written Cloud services contract, referenced Service Specifications, and the Ordering Document as well as the following resources: • Oracle Cloud Hosting and Delivery Policies • Oracle Data Processing Agreement (DPA) • PaaS and IaaS Cloud Services Pillar Document
5.5.2	Every outsourcing agreement should at the very least, have provisions to address the following aspects of outsourcing:	N/A	N/A

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.5.2 (a)	scope of the outsourcing arrangement;	Oracle Cloud Ordering Document	The scope of services and other terms specific to the outsourcing arrangement are specified in the Oracle Cloud Ordering Document. See also Section 5.5.1 earlier in this table.
5.5.2 (b)	performance, operational, internal control and risk management standards;	• Oracle Cloud Hosting and Delivery Policies, Section 3.2.2 • PaaS and IaaS Cloud Services Pillar Document • CSA, Section 11.1 • Schedule C, Section 11.1	The operational elements of the outsourcing arrangement are detailed in the Oracle Cloud Hosting and Delivery Policies along with the PaaS and IaaS Cloud Services Pillar Document. In addition, Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability. Section 11.1 of the CSA and Section 11.1 of Schedule C, as applicable, explain that Oracle also continuously monitors the Cloud services. See also Section 5.5.1 earlier in this table.
5.5.2 (c)	confidentiality and security;	• Oracle Cloud Hosting and Delivery Policies, Section 1 • CSA, Sections 4, 4.3 and 5 • Schedule C, Sections 4 and 5 • FSA, Section 8 • DPA, Section 6 • Oracle PaaS and IaaS Public Cloud Services Pillar Document, Section 3	Section 1 of the Oracle Cloud Hosting and Delivery Policies contains the Oracle Cloud Security Policy, which describes Oracle's security practices. Oracle Cloud services are offered to multiple customers and are not bespoke offerings. As such, the hosting and delivery policies and Oracle's Security Practices govern Oracle's security obligations. Section 4.3 of the CSA and Section 4 of Schedule C, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the services). Section 5 of the CSA and Schedule C, as applicable. Section 8 of the FSA, Section 4 of the CSA, and Section 4 of Schedule C, as applicable. Section 6 of the Oracle Data Processing Agreement (DPA) states that Oracle has implemented and will maintain appropriate technical and organizational security measures for the processing of personal information. Section 3 of the Oracle PaaS and IaaS Public Cloud Services Pillar Document also addresses security measures, including physical safeguards.
5.5.2 (d)	business continuity management;	• FSA, Section 5 • Oracle Cloud Hosting and Delivery Policies, Section 2 • Oracle PaaS and IaaS Public Cloud Services Pillar Document, Section 4	Section 5 of the FSA indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Additionally, see the Oracle Cloud Service Continuity Policy in Section 2 of the Oracle Cloud Hosting and Delivery Policies. Section 4 of the Oracle PaaS and IaaS Public Cloud Services Pillar Document addresses cloud service continuity.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.5.2 (e)	monitoring and control;	• Ordering Document • Oracle Cloud Hosting and Delivery Policies, specifically section 3.2.2 • Oracle PaaS and IaaS Public Cloud Services Pillar Document • CSA, Section 11.1 • Schedule C, Section 11.1	Oracle's written Cloud services contract, referenced Service Specifications, and Ordering Document addresses monitoring and control of the Oracle cloud services in the following documents: • Oracle Cloud Hosting and Delivery Policies • PaaS and IaaS Cloud Services Pillar Document Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability. Section11.1 of the CSA and Section 11.1 of Schedule C, as applicable, explain that Oracle also continuously monitors the Cloud services.
5.5.2 (f)	audit and inspection;	• FSA, Section 1 • FSA, Section 2 • DPA • OCI Consensus Assessment Initiative Questionnaire (CAIQ): oracle.com/a/ocom/docs/oci-corporate-caiq.pdf	Refer to Section 1 (Customer Audit Rights) of the FSA: • Section 1.1 grants customers the same rights of access and audit for Oracle's Strategic Subcontractors. • Section 1.5 provides customers full access and unrestricted audits and supplements the Oracle Cloud services agreement and the Oracle Data Processing Agreement (DPA). • Section 1.9 allows pooled audits to the extent sufficient to allow customer to comply with its regulatory obligations Refer to Section 2 (Regulator Audit Rights) of the FSA: • Section 2.1 grants customer's regulators the same rights of access and audit for Oracle's Strategic Subcontractors. Oracle Cloud Services are operated under policies that are generally aligned with the ISO/IEC 27002 Code of Practice for information security controls. The internal controls are subject to periodic testing by independent third-party audit organizations. Such audits may be based on the Statement on Standards for Attestation Engagements (SSAE) 18, Reporting on Controls at a Service Organization (SSAE18), the International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization (ISAE3402), the International Standard on Assurance Engagements (ISAE) No. 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information (ISAE 3000), or other third-party auditing standards or procedures applicable to the specific Oracle Cloud Service. Audit reports about selected/a number of Oracle cloud environments are periodically published by Oracle's third-party auditors. Customer may request access to available audit reports for a particular Oracle Cloud service via Sales or Customer Cloud Portal.
5.5.2 (g)	Notification of adverse developments An institution should specify in its outsourcing agreement the type of events and the circumstances under which the service provider should report to the institution in order for an institution to take prompt risk mitigation measures and notify MAS of such developments under paragraph 4.2.1;	• FSA, Section 7 • DPA, Section 8 • CSA, Section 15 • Schedule C, Section 15	Section 7 of the FSA addresses notifications affecting service provisions. Section 8, "Incident Management and Breach Notification," of the Oracle Data Processing Agreement (DPA). Section 15 of the CSA and Section 15 of Schedule C discuss party notification requirements generally.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.5.2 (h)	Dispute resolution An institution should specify in its outsourcing agreement the resolution process, events of default, and the indemnities, remedies and recourse of the respective parties in the agreement. The institution should ensure that its contractual rights can be exercised in the event of a breach of the outsourcing agreement by the service provider;	- FSA, Section 10 - FSA, Section 3 - CSA, Section 6.3 - Schedule C, Section 6.3 - CSA, Section 8 - Schedule C, Section 8 - CSA, Section 14 - Schedule C, Section 14	Section 10 of the FSA addresses dispute resolution and respective obligations relating to service agreements. See also Section 3 of the FSA for information related to additional termination rights and insolvency. Section 6.3 of the CSA and Section 6.3 of Schedule C address remedies for breaches. Section 8 of the CSA and Section 8 of Schedule C discuss relevant indemnification terms. Section 14 of the CSA and Section 14 of Schedule C address jurisdiction for any disputes.
5.5.2 (i)	Default termination and early exit An institution should, have the right to terminate the outsourcing agreement in the event of default, or under circumstances where: (i) the service provider undergoes a change in ownership; (ii) the service provider becomes insolvent or goes into liquidation; (iii) the service provider goes into receivership or judicial management whether in Singapore or elsewhere; (iv) there has been a breach of security or confidentiality; or (v) there is a demonstrable deterioration in the ability of the service provider to perform the contracted service. The minimum period to execute a termination provision should be specified in the outsourcing agreement. Other provisions should also be put in place to ensure a smooth transition when the agreement is terminated or being amended. Such provisions may facilitate transferability of the outsourced services to a bridge-institution or a third party. Where the outsourcing agreement involves an intra-group entity, the agreement should be legally enforceable against the	- FSA, Section 3 - FSA, Section 4 - CSA, Sections 6.1 and 9.4 - Schedule C, Sections 6.1 and 9.3	Section 3 of the FSA addresses general termination rights. Customers have the right to terminate the cloud services in the following situations: Termination due to regulatory requirements - Continued use of the services would cause customers to violate applicable law and regulation upon the conclusion made by the regulator. - Termination requested based on express instruction issued by the regulator where the services are considered as an impediment to effective supervision over the customer. Termination due to insolvency - Oracle has become insolvent or resolved to go into liquidation. - A proposal is made for entering into any compromise or arrangement with any or all of Oracle's creditors. - A receiver is appointed over all or substantially all the assets of Oracle. Additionally, pursuant to Section 4 of the FSA, "Exit Provision," customers are able to order transition services and transition assistance to facilitate the transfer or the reincorporation of the concerned function back to the customer or to a third-party provider. Sections 6.1 and 9.4 of the CSA and Sections 6.1 and 9.3 of Schedule C, as applicable, further explain that customers have the right to terminate for any breach of a material contract term, including a breach of the service warranty. In the service warranty, Oracle warrants that it will perform the services using commercially reasonable care and skill in all material respects as described in the Service Specifications.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
	intra-group entity providing the outsourced service;		
5.5.2 (j)	Sub-contracting An institution should retain the ability to monitor and control its outsourcing arrangements when a service provider uses a sub-contractor. An outsourcing agreement should contain clauses setting out the rules and limitations on sub-contracting. An institution should include clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractor and for the sub-contractor's compliance with the provisions in its agreement with the service provider, including the prudent practices set out in these Guidelines. The institution should ensure that the sub-contracting of any part of material outsourcing arrangements is subject to the institution's prior approval;	- DPA, Section 4.1 - FSA, Section 6 - My Oracle Support, Doc ID 111.2: support.oracle.com - FSA, Section 6.1 - FSA, Section 6.2 - CSA, Section 17.2	Section 4.1 of the Oracle Data Processing Agreement (DPA) indicates that, to the extent Oracle engages third-party subprocessors or Oracle affiliates to process personal information, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Oracle Cloud services contract. This section also indicates that Oracle is responsible for the performance of the Oracle affiliates and third-party subprocessors' obligations in compliance with the terms of the Oracle Data Processing Agreement and applicable data protection law. Per Section 5 of the FSA, Oracle may use subprocessors or strategic subcontractors for some of its cloud services. Oracle reviews all of its subcontractors that provide services to Oracle as part of its cloud services according to a published criteria to determine the status of such subcontractors. Oracle publishes a list of its subprocessors and strategic subcontractors (collectively "subcontractors") to customers through My Oracle Support. Section 6.1 of the FSA further indicates that all subcontractors with access to customer content will be subject to the same level of data protection and security as Oracle under the terms of the Oracle Cloud services contract. In addition, under this section, Oracle agrees to enter into written agreements with subcontractors reflecting obligations that are consistent with Oracle's obligations under the relevant terms of the Oracle Cloud services contract. Any such subcontracting will not diminish Oracle's responsibility toward its customers under Oracle Cloud services contracts and Oracle will appropriately oversee a subcontractor's performance. Section 6.2 of the FSA include terms applicable to Oracle's use of subcontractors and strategic subcontractors, and similar to the Oracle Data Processing Agreement, includes a right for a customer to object to the intended involvement of a new strategic subcontractor. See also Section 17.2 of the CSA regarding third-party liability.
5.5.2 (k)	Applicable Laws Agreements should include choice-of-law provisions, agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction.	- CSA, Section 14 - Schedule C, Section 14 - FSA, Section 8	Section 14 of the CSA and Section 14 Schedule C set out the governing law and jurisdiction of the agreement. See also Section 8 of the FSA, "Compliance with Laws."
5.5.3	Each agreement should be tailored to address issues arising from country risks and potential obstacles in exercising oversight and management of the outsourcing arrangements made with a service provider outside Singapore.	See Section 4.1.3 (d) in a preceding table.	See Section 4.1.3 (d) in a preceding table.

5.6 Confidentiality and Security

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.6.1	As public confidence in institutions is a cornerstone in the stability and reputation of the financial industry, it is vital that an institution satisfies itself that the service provider's security policies, procedures and controls will enable the institution to protect the confidentiality and security of customer information.	• Oracle Corporate Security Practices: oracle.com/corporate/security-practices/corporate • Oracle Privacy Policy: oracle.com/legal/privacy • Oracle Information Protection Policy: oracle.com/corporate/security-practices/corporate/information-assets-classification.html • DPA, Section 6 • Schedule C, Sections 4 and 5 • CSA, Sections 4 and 5 • Oracle Cloud Hosting and Delivery Policies, particularly Sections 1.6, 3.1 and 3.2 • Oracle PaaS and IaaS Public Cloud Services Pillar Document	Oracle reviews internal controls identified to meet the requirements of the control framework, relevant standards, regulatory, legal, and statutory requirements at least annually. Section 1.6 of the Cloud Hosting and Delivery Policy describes Oracle personnel confidentiality training requirements. Additional contract terms regarding confidentially and security are as follows: Technical and organization security measures: • Section 6, "Security and Confidentiality," of the Oracle Data Processing Agreement (DPA) • The Oracle Cloud Hosting and Delivery Policies and the PaaS and IaaS Cloud Services Pillar Document as applicable. Confidentiality and Protection of "Your Content": • Section 4 of Schedule C and Section 4 of the CSA, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services). • Section 5 of Schedule C and Section 5 of the CSA, as applicable. • Section 8, "Incident Management and Breach Notification," of the Oracle Data Processing Agreement. Also see Sections 4.1.3 (a), (b), and (e), and Sections 5.4.3 (d) and (e) in preceding tables.
5.6.2	An institution should be proactive in identifying and specifying requirements for confidentiality and security in the outsourcing arrangement. An institution should take the following steps to protect the confidentiality and security of customer information:	N/A	N/A
5.6.2 (a)	State the responsibilities of contracting parties in the outsourcing agreement to ensure the adequacy and effectiveness of security policies and practices, including the circumstances under which each party has the right to change security requirements. The outsourcing agreement should also address:	• CSA, Section 1.2 • Schedule C, Section 1.2	Section 1.2 of the CSA and Section 1.2 of Schedule C specify that Oracle updates to the Services or Service Specifications will not materially reduce the level of performance, functionality, security, or availability of the services during the services period of your order. See also Section 5.5.2 (c) in the preceding table.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.6.2 (a)(i)	the issue of the party liable for losses in the event of a breach of security or confidentiality and the service provider's obligation to inform the institution; and	- CSA, Section 7 - Schedule C, Section 7	Section 7 of the CSA and Section 7 of Schedule C address liability for losses.
5.6.2 (a)(ii)	the issue of access to and disclosure of customer information by the service provider. Customer information should be used by the service provider and its staff strictly for the purpose of the contracted service;	- CSA, Section 4.3 - Schedule C, Section 4 - OCI Security Documentation: docs.oracle.com/iaas/Content/Security/Concepts/security_features.htm	As a IaaS service provider, Oracle does not generally have insight into customer content or the customer's decisions regarding its collection and use. Generally, Oracle customers are responsible for administering their own access rights with regard to their cloud services environment. Customers may use OCI services such as Identity and Access Management (IAM) and Vault, and compartments to manage access to cloud resources. Section 4.3 of the CSA and Section 4 of Schedule C, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Your Content" for as long as it resides in the Services). See also Section 5.5.2 (c) in the preceding table.
5.6.2 (b)	Disclose customer information to the service provider only on a need-to-know basis;	- CSA, Section 4 - Schedule C, Section 4	See Section 4 of the CSA and Section 4 of Schedule C regarding nondisclosure. **Note**: This is primarily a customer responsibility.
5.6.2 (c)	Ensure the service provider is able to protect the confidentiality of customer information, documents, records, and assets, particularly where multi-tenancy arrangements are present at the service provider; and	Data Security: Technical Controls: oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html	Oracle implements a wide variety of technical security controls designed to protect the confidentiality, integrity, and availability of corporate information assets. See also Section 5.5.2 (c) in the preceding table.
5.6.2 (d)	Review and monitor the security practices and control processes of the service provider on a regular basis, including commissioning audits or obtaining periodic expert reports on confidentiality, security adequacy and compliance in respect of the operations of the service provider, and requiring the service provider to disclose to the institution breaches of confidentiality in relation to customer information.	- Oracle Cloud Observability and Management Platform: oracle.com/manageability - Audit Service: docs.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm - OCI cost management tools: docs.oracle.com/iaas/Content/GSG/Concepts/costs.htm - Managing and Monitoring Oracle Cloud: docs.oracle.com/en/cloud/getstarted/subscriptions-cloud/mmocs/managing-and-monitoring-oracle-cloud.pdf - DPA	To help customers meet their monitoring and oversight obligations, Oracle provides the Oracle Cloud Observability and Management Platform, which is a comprehensive set of management, diagnostic, and analytics services that help customers manage their OCI tenancy while reducing troubleshooting time, reducing likelihood of outages, and enabling IT to manage applications. The platform provides visibility across applications by using advanced analytics to automatically detect anomalies and enable quick remediation in near-real time. The platform includes services such as Logging, Monitoring, Notifications, Database Management, and Application Performance Monitoring. Under the Oracle Data Processing Agreement (DPA), customers have the right to audit Oracle's compliance with its contractual obligations. Additionally, internal and external audits of OCI security practices and control processes are conducted by an independent third party on an annual basis. Customers can access audit reports and certifications directly from the Oracle Cloud Console. See also Sections 5.5.2 (f) and (g) in the preceding table.

5.7 Business Continuity Management

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.7.1	An institution should ensure that its business continuity is not compromised by outsourcing arrangements, in particular, of the operation of its critical systems as stipulated under the Technology Risk Management Notice. An institution should adopt the sound practices and standards contained in the Business Continuity Management ("BCM") Guidelines issued by MAS, in evaluating the impact of outsourcing on its risk profile and for effective BCM.	Oracle Risk Management Resiliency Business Continuity: oracle.com/corporate/security-practices/corporate/resilience-management/business-continuity.html	For each critical line of business, Oracle maintains a business continuity plan that includes a business impact analysis (BIA), risk assessments, and disaster recovery contingency plans. The plans align with Oracle's Risk Management and Resiliency Program policy, which requires the plans to outline procedures, ownership, roles, and responsibilities to be followed if a business disruption occurs. These plans are reviewed and tested annually.
5.7.2	In line with the BCM Guidelines, an institution should take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangement can be adequately mitigated such that the institution remains able to conduct its business with integrity and competence in the event of a service disruption or failure, or unexpected termination of the outsourcing arrangement or liquidation of the service provider. These should include taking the following steps:	N/A	N/A
5.7.2 (a)	Determine that the service provider has in place satisfactory business continuity plans ("BCP") that are commensurate with the nature, scope and complexity of the outsourcing arrangement. Outsourcing agreements should contain BCP requirements on the service provider, in particular, recovery time objectives ("RTO"), recovery point objectives ("RPO"), and resumption operating capacities;	• FSA, Section 5 • Oracle Cloud Hosting and Delivery Policies, Section 2 • Oracle PaaS and IaaS Public Cloud Services Pillar Document, particularly section 4	Section 5 of the FSA indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Upon at least 30 days' notice by you no more than once per calendar year, Oracle will make available to you via web conference or on Oracle premises, in a guided manner, a summary of the BCP Program and applicable test information, material modifications to the BCP Program within the last 12 months, and pertinent BCP governance areas, and confirmation that an internal review of these governance areas was performed within the last 12 months. Additionally, see the Oracle Cloud Service Continuity Policy in Section 2 of the Oracle Cloud Hosting and Delivery Policies. Section 4 of the Oracle PaaS and IaaS Public Cloud Services Pillar Document addresses cloud service continuity.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.7.2 (b)	Proactively seek assurance on the state of BCP preparedness of the service provider, or participate in joint testing, where possible. It should ensure the service provider regularly tests its BCP plans and that the tests validate the feasibility of the RTO, RPO and resumption operating capacities. Such tests would serve to familiarise the institution and the service provider with the recovery processes as well as improve the coordination between the parties involved. The institution should require the service provider to notify it of any test finding that may affect the service provider's performance. The institution should also require the service provider to notify it of any substantial changes in the service provider's BCP plans and of any adverse development that could substantially impact the service provided to the institution; and	- Resilience Management and Business Continuity: oracle.com/corporate/security-practices/corporate/resilience-management - Data Security: Physical and Environmental Controls: oracle.com/corporate/security-practices/corporate/physical-environmental.html	Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as used in the Oracle Risk Management Resiliency Program (RMRP). Upon request by a customer, Oracle provides a summary of the RMRP, material modifications to the RMRP within the last 12 months, and pertinent program governance areas, along with confirmation that testing of these governance areas was performed within the last 12 months. Oracle deploys its cloud services on a resilient computing infrastructure designed to maintain service availability and continuity if an adverse event affects the services. Availability domains align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Equipment uses redundant power sources and maintains generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Customers are notified of disruptive events and the implications to the customer's Oracle products or services, including the RTOs.
5.7.2 (c)	Ensure that there are plans and procedures in place to address adverse conditions or termination of the outsourcing arrangement such that the institution will be able to continue business operations and that all documents, records of transactions and information previously given to the service provider should be promptly removed from the possession of the service provider or deleted, destroyed or rendered unusable.	- FSA, Section 4.1 - DPA, Section 9.1 - FSA, Section 4.2 - FSA, Section 4.3	Under Section 4.1 of the FSA, without prejudice to the terms within the Service Specifications (including without limitation the Data Processing Agreement) relating to retrieval of your content, upon (a) the end of the Services Period applicable under your order or (b) your termination of the applicable cloud services in accordance with your services agreement and your order (both referred to as "Termination"), and provided you submit a service request in the Cloud Customer Support Portal designated for the cloud service (for example, My Oracle Support) no later than 30 days following termination, Oracle will provide reasonable assistance to you during the retrieval period to enable you to retrieve your content from the production services environment, including assistance with your understanding of the structure and format of the export file. Also refer to Section 9.1 of the Oracle Data Processing Agreement (DPA) regarding return and deletion of personal information upon termination of services. Under Section 4.2 and 4.3 of the FSA, in the event you require assistance with a transition (whether to another service provider or to your own organization), you may request additional professional services from Oracle ("Transition Assistance Services"), and Oracle will enter into good faith negotiations with you regarding such Transition Assistance Services. Any Transition Assistance Services to be performed by Oracle must be mutually agreed by the parties in a separate order.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.7.3	For assurance on the functionality and effectiveness of its BCP plan, an institution should design and carry out regular, complete and meaningful BCP testing that is commensurate with the nature, scope and complexity of the outsourcing arrangement. For tests to be complete and meaningful, the institution should involve the service provider in the validation of its BCP and assessment of the awareness and preparedness of its own staff. Similarly, the institution should take part in its service providers' BCP and disaster recovery exercises.	• Oracle Cloud Hosting and Delivery Policies • Oracle Risk Management Resiliency Business Continuity: oracle.com/cloud/backup-and-disaster-recovery • Risk Management Resiliency Program: oracle.com/a/ocom/docs/corporate/oracle-risk-management-resiliency-program-ds.pdf	Oracle will provide reasonable support to you as you develop and test 1) your termination plans so as to facilitate the migration of your content to you or a replacement service provider in the event of termination and 2) your own business continuity plans relating to a possible service disruption. Reasonable support may consist of assistance with understanding the structure and format of your data export file (in accordance with the Oracle Cloud Hosting and Delivery Policies), discussing additional Transition Services that may be available to you, or a review of Oracle's BCP Program. Business Critical Lines of Business (LoBs) conduct two tabletop exercises a year to challenge their BCPs and recovery strategies, for example, LoB-specific tabletop exercises and corporate coordinated tabletop exercise which is a global event across all LOBs. This is a requirement per the RMRP policy mandated by the Oracle Security Oversight Committee (OSOC). Also note that the Disaster Recovery organization may conduct its own cross-functional Disaster Recovery testing where they are challenging the RTOs and RPOs. Teams that would be part of this cross-functional testing team include Enterprise Engineering, OCI, and RE&Fs.
5.7.4	The institution should consider worst case scenarios in its business continuity plans. Some examples of these scenarios are unavailability of service provider due to unexpected termination of the outsourcing agreement, liquidation of the service provider and wide-area disruptions that result in collateral impact on both the institution and the service provider. Where the interdependency on an institution in the financial system is high, the institution should maintain a higher state of business continuity preparedness. The identification of viable alternatives for resuming operations without incurring prohibitive costs is also essential to mitigate interdependency risk.	• Oracle Cloud Hosting and Delivery Policies • Oracle Risk Management Resiliency Business Continuity: oracle.com/cloud/backup-and-disaster-recovery • Risk Management Resiliency Program: oracle.com/a/ocom/docs/corporate/oracle-risk-management-resiliency-program-ds.pdf	Oracle will provide reasonable support to you as you develop and test 1) your termination plans so as to facilitate the migration of your content to you or a replacement service provider in the event of termination and 2) your own business continuity plans relating to a possible service disruption. Reasonable support may consist of assistance with understanding the structure and format of your data export file (in accordance with the Oracle Cloud Hosting and Delivery Policies), discussing additional Transition Services that may be available to you, or a review of Oracle's BCP Program. Oracle's corporate Disaster Recovery (DR) plan focuses on the resiliency of computing infrastructure supporting Oracle's internal operations. Oracle's production data centers are geographically separated and have component and power redundancy, with backup generators in place for availability of data center resources in case of an impacting event. Oracle's DR plan leverages this separation of data centers in conjunction with other recovery strategies to both protect against disruption and enable recovery of services. Lessons learned from the annual exercises are implemented as deemed appropriate into standard operations and DR procedures as appropriate. Oracle identifies relevant business interruption scenarios, including essential people, resources, facilities, and technology. Plans are written to effectively manage and respond to these scenarios. Oracle provides the customer with the ability to use multiple OCI regions to support their BCP and DR requirements. Oracle Cloud Infrastructure maintains processes to monitor infrastructure capacity and creates capacity forecasts at least quarterly for critical system components. Corporate business continuity policy, standards, and practices are governed by the RMRP Program Management Office (PMO) and are generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance.

5.9 Audit and Inspection

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.9.1	An institution's outsourcing arrangements should not interfere with the ability of the institution to effectively manage its business activities or impede MAS in carrying out its supervisory functions and objectives.	FSA	Customers and their regulators have the unrestricted right to access and audit Oracle's compliance with its obligations under their cloud services agreement. Such audit rights and related terms are covered by the FSA. See also Sections 4.1.3 (d) and 5.5.2 (f) in preceding tables.
5.9.2	An institution should include, in all its outsourcing agreements for material outsourcing arrangements, clauses that:	N/A	N/A
5.9.2 (a)	allow the institution to conduct audits on the service provider and its subcontractors, whether by its internal or external auditors, or by agents appointed by the institution; and to obtain copies of any report and finding made on the service provider and its sub-contractors, whether produced by the service provider's or its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractor, in relation to the outsourcing arrangement;	FSA	Customers and their regulators have the unrestricted right to access and audit Oracle's compliance with its obligations under their cloud services agreement. In addition, Oracle grants the same rights of access and audit of its strategic subcontractors to its customers and their regulators. Such audit rights and related terms are covered by the FSA. See also Section 5.5.2 (f) in a preceding table.
5.9.2 (b)	Allow MAS, or any agent appointed by MAS, where necessary or expedient, to exercise the contractual rights of the institution to:	N/A	N/A
5.9.2 (b)(i)	access and inspect the service provider and its sub-contractors, and obtain records and documents, of transactions, and information of the institution given to, stored at or processed by the service provider and its sub-contractors; and	N/A	Independent auditors examine our Strategic Contractors and provide audit reports which can be shared with customers. These audit findings are tracked and remediated. Additionally, customers can report issues to Oracle through customer support portal. Oracle will work with customers and engage any teams necessary to resolve any issues or concerns. See also Section 5.5.2 (f) in a preceding table and Section 5.9.2 (a) in a preceding row in this table.
5.9.2 (b)(ii)	access any report and finding made on the service provider and its sub-contractors, whether produced by the service provider's and its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractors, in relation to the outsourcing arrangement.	N/A	Independent auditors examine our Strategic Contractors and provide audit reports which can be shared with customers. These audit findings are tracked and remediated. Additionally, customers can report issues to Oracle through customer support portal. Oracle will work with customers and engage any teams necessary to resolve any issues or concerns. See also Section 5.5.2 (f) in a preceding table and Section 5.9.2 (a) in a preceding row in this table.
5.9.3	Outsourcing agreements for material outsourcing arrangements should also include clauses that require the service provider to comply, as soon as possible, with any request from MAS or the institution, to the service provider or its sub-contractors, to submit any reports on the security and control environment of the service provider and its sub-contractors to MAS, in relation to the outsourcing arrangement.	FSA, Section 1.4	Under Section 1.4 of the FSA, Oracle acknowledges that you (if the request comes from your CEO or other C-level executive) may require an audit of Oracle and/or information relating to the ordered cloud service without prior notice due to an emergency or crisis situation. See also Section 5.5.2 (f) in a preceding table.

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.9.4	An institution should ensure that these expectations are met in its outsourcing arrangements with the service provider as well as any sub-contractor that the service provider may engage in the outsourcing arrangement, including any disaster recovery and backup service providers.	See Section 5.5.2 (f) in a preceding table.	See Section 5.5.2 (f) in a preceding table.
5.9.5	An institution should ensure that independent audits and/or expert assessments of all its outsourcing arrangements are conducted. In determining the frequency of audit and expert assessment, the institution should consider the nature and extent of risk and impact to the institution from the outsourcing arrangements. The scope of the audits and expert assessments should include an assessment of the service providers' and its sub-contractors' security and control environment, incident management process (for material breaches, service disruptions or other material issues) and the institution's observance of these Guidelines in relation to the outsourcing arrangement.	N/A	Internal and external audits of OCI security practices and control processes, including subcontractors, are conducted by an independent third party on an annual basis. Customers can access audit reports and certifications directly from the Oracle Cloud Console. See also Sections 4.1.3 (a) and 5.5.2 (f) in preceding tables.
5.9.6	The independent audit and/or expert assessment on the service provider and its subcontractors may be performed by the institution's internal or external auditors, the service provider's external auditors or by agents appointed by the institution. The appointed persons should possess the requisite knowledge and skills to perform the engagement, and be independent of the unit or function performing the outsourcing arrangement. Senior management should ensure that appropriate and timely remedial actions are taken to address the audit findings. Institutions and the service providers should have adequate processes in place to ensure that remedial actions are satisfactorily completed. Actions taken by the service provider to address the audit findings should be appropriately validated by the institution before closure. Where necessary, the relevant persons who possess the requisite knowledge and skills should be involved to validate the effectiveness of the security and control measures taken.	• FSA, Section 1.2 • Approved Auditors: support.oracle.com/epmos/main/downloadattachmentprocessor?parent=DOCUMENT&sourceId=2817391.2&attachid=2817391.1:CS_AUDITOR_LIST&clickstream=yes • Oracle Cloud Console	Per Section 1.2 of the FSA, if a third party is to conduct the audit, the third party will be mutually agreed to by you and Oracle (except if such third party is contained in Oracle's published list of approved auditors at the time of the audit request). Oracle will not unreasonably withhold its consent to a third-party auditor requested by you. The third party must execute a written confidentiality agreement acceptable to Oracle or otherwise be bound by a statutory or legal confidentiality obligation. If deviations are found in regular audits, we document, remediate, and track to closure. Audit reports are available to customers in the Console. Independent auditors examine our Strategic Contractors and provide audit reports which can be shared with financial institutions (FIs). These audit findings are tracked and remediated. Additionally, customers can report issues to Oracle through customer support portal. Oracle will work with FIs and engage any teams necessary to resolve any issues or concerns. See also Section 5.5.2 (f) in a preceding table.
5.9.8	Copies of audit reports should be submitted by the institution to MAS. An institution should also, upon request, provide MAS with other reports or information on the institution and service provider that is related to the outsourcing arrangement.	See Section 5.5.2 (f) in a preceding table and Section 5.9.6 in a preceding row in this table.	See Section 5.5.2 (f) in a preceding table and Section 5.9.6 in a preceding row in this table.

5.10 Outsourcing Outside Singapore

TOPIC REF.	COMPLIANCE REQUIREMENTS	ORACLE RESOURCES	DESCRIPTION OF ORACLE PRACTICES
5.10.1	In its risk management of such outsourcing arrangements, an institution should take into account, as part of its due diligence, and on a continuous basis: (a) government policies; (b) political, social, economic conditions; (c) legal and regulatory developments in the foreign country; and (d) the institution's ability to effectively monitor the service provider, and execute its business continuity management plans and exit strategy.	• Risk Management Resiliency Program: oracle.com/corporate/security-practices/corporate/resilience-management • OCI Consensus Assessment Questionnaire (CAIQ): oracle.com/a/ocom/docs/oci-corporate-caiq.pdf	OCI evaluates the data center control environment, including physical security controls and environmental safeguards, in accordance with the schedule defined in the Data Center Assessment Program. Identified issues are evaluated and tracked through resolution. OCI operates under policies that are aligned with the ISO/IEC 27002 Code of Practice for information security controls, at a minimum. OCI's internal controls are mapped to applicable regulations and standards and subject to internal control reviews and testing by independent third-party audit organizations. See also Section 5.4.3 (i) in a preceding table.
5.10.2	Material outsourcing arrangements with service providers located outside Singapore should be conducted in a manner so as not to hinder MAS' efforts to supervise the Singapore business activities of the institution in a timely manner, in particular: (a) An institution should, in principle, enter into outsourcing arrangements only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements. (b) An institution should not enter into outsourcing arrangements with service providers in jurisdictions where prompt access to information by MAS or agents appointed by MAS to act on its behalf, at the service provider, may be impeded by legal or administrative restrictions. An institution must at least commit to retrieve information readily from the service provider should MAS request for such information. The institution should confirm in writing to MAS, that the institution has provided, in its outsourcing agreements, for MAS to have the rights of inspecting the service provider, as well as the rights of access to the institution and service provider's information, reports and findings related to the outsourcing arrangement, as set out in paragraph 5.9. (c) An institution should notify MAS if any overseas authority were to seek access to its customer information or if a situation were to arise where the rights of access of the institution and MAS set out in paragraph 5.9, have been restricted or denied.	• FSA, Section 2.4 • FSA, Section 1.5 • FSA, Section 1.2 • FSA, Section 2, particularly section 2.7 • FSA, Section 1.9 • FSA, Section 6.1 • FSA, Section 1 and 2 • FSA, Section 4.1 • Oracle Cloud Hosting and Delivery Policy, Section 6.1 • DPA, Section 9 • Schedule C, Section 9.4 • CSA, Section 9.5 • FSA, Section 9	Oracle enables its customers' regulators, including MAS, to carry out its supervisory functions in respect of the financial institutions. Such rights are addressed in the Oracle FSA as follows: • Section 2.4 explicitly acknowledges the information gathering and investigatory powers of resolution authorities. • Section 1.5 provides customers full access and unrestricted audits and supplements the Oracle Cloud services agreement and the Oracle Data Processing Agreement. • Section 1.2 provides customers the right to use a third party to conduct the audit. • Section 2 provides audit rights for the customer's regulators. Section 2.7 in particular states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law. • Section 1.9 allows pooled audits to the extent sufficient to allow customer to comply with its regulatory obligations. • Section 6.1 states that any outsourcing will not diminish Oracle's responsibility under the agreement. • Sections 1 and 2 set out Oracle's obligations with regard to customer and customer regulators' audit rights. • Section 4.1 explains that Oracle will provide reasonable assistance to customers during the retrieval period to enable them to retrieve their content from the production services environment. See Section 6.1 of the Oracle Cloud Hosting and Delivery Policies, Section 9 of the Oracle Data Processing Agreement (DPA), Section 9.4 of Schedule C and Section 9.5 of the CSA, as applicable, where Oracle also agrees to make personal information and content available for retrieval by the customer. Additionally, see Section 9 of the FSA where Oracle agrees to continue to perform the services in the event of a Resolution Event.

Conclusion

Oracle enables customers to become more agile, collaborative, and insightful while striving to support them in meeting their own obligations under the MAS Outsourcing Guidelines. Oracle Cloud Infrastructure services and features can accelerate innovation for financial institutions operating in Singapore.

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