ORACLE

Advisory: Hong Kong Monetary Authority's Supervisory Policy Manuals on Outsourcing and General Principles for Technology Risk Management

Description of Oracle Cloud Infrastructure Security Practices in the Context of the Hong Kong Monetary Authority's Guidelines

October 2023, 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 help you assess your use of Oracle Cloud Infrastructure (OCI) in the context of the guidance applicable to you under the Hong Kong Monetary Authority's (HKMA) Supervisory Policy Manual - Outsourcing (SA-2) and Supervisory Policy Manual - General Principles for Technology Risk Management (TM-G-1). This document 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, which is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines nor as representations or warranties. 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.

SA-2 and TM-G-1 are subject to periodic changes. The current versions are available at hkma.gov.hk/eng/regulatory-resources/regulatory-guides/supervisory-policy-manual/.

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.

Revision History

The following revisions have been made to this document.

DATE	REVISION
October 2023	Initial publication

Table of Contents

Introduction

The Hong Kong Monetary Authority (HKMA) is Hong Kong's central banking institution. It is a government authority founded in April 1993, when the Office of the Exchange Fund and the Office of the Commissioner of Banking merged. HKMA regulates and supervises Authorized Institutions (AIs), including banks and deposit-taking companies as well as retail payments systems and stored-value facilities.

HKMA issues guidelines to provide the Hong Kong financial services industry with practical guidance to facilitate compliance with regulatory requirements. The guidelines relevant to the use of outsourced services instruct AIs to perform risk assessments, perform due-diligence reviews of service providers, ensure that controls are in place to preserve information confidentiality, have sufficient monitoring and control oversight on the outsourcing arrangement, and establish contingency arrangements.

About Oracle Cloud Infrastructure

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

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

The Cloud Shared Management Model

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

Oracle provides best-in-class security technology and operational processes to secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle cloud services. By design, Oracle provides security functions for cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching. Customers are responsible for securely configuring and using their cloud resources. For more information, see the cloud service documentation.

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

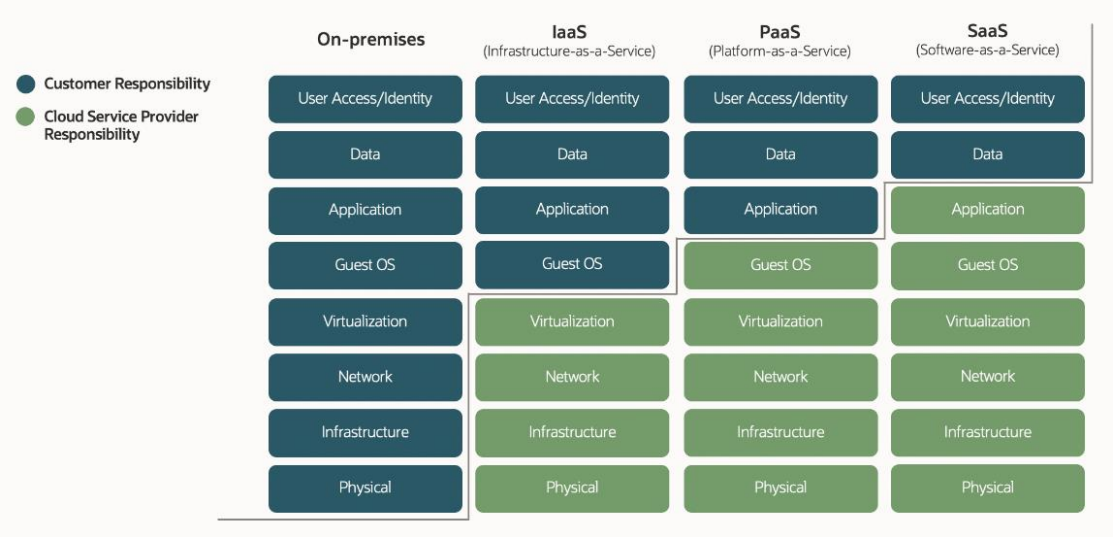

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

HKMA Compliance Summary

This document provides a summary of select portions of HKMA policy manuals SA-2 and TM-G-1, and provides information to help with the evaluation OCI in the context of these policy requirements.

AIs operating in Hong Kong are responsible for ensuring they meet their legal obligations under HKMA. Following is a summary of select sections of the HKMA policy manuals for which OCI practices and controls may assist AIs in meeting their requirements. It should be noted that this is not a complete evaluation of HKMA requirements, and any determination about compliance and the suitability of cloud services in the context of these requirements is the sole responsibility of the responsible entity.

Outsourcing (SA-2)

2.3.1: Ability of service providers

"Before selecting a service provider AIs should perform appropriate due diligence. In assessing a provider, apart from the cost factor and quality of services AIs should take into account the provider's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity, compatibility with the AI's corporate culture and future development strategies, familiarity with the banking industry and capacity to keep pace with innovation in the market."

Oracle provides several resources to assist its customers in conducting necessary due diligence, including but not limited to, the following resources:

EVALUATION CRITERIA	ORACLE RESOURCES
Financial soundness	Oracle Investor Relations - Financials
Reputation	Oracle Customer Successes
Managerial skills	OCI Documentation
Technical capabilities	OCI Consensus Assessment Initiative Questionnaire (CAIQ) Oracle Corporate Security Practices
Information about compliance frameworks	Oracle Cloud Compliance

2.3.2: Ability of service providers

"AIs should have controls in place (e.g. comparison with target service level) to monitor the performance of service providers on a continuous basis."

Customers are responsible for monitoring the performance of their service providers. Oracle uses various tools to monitor the availability and performance of OCI services and the operation of infrastructure and network components. Oracle monitors the hardware that supports the OCI services, and generates alerts for monitored network components, such as CPU, memory, storage, and database. Oracle Cloud Operations personnel monitor alerts associated with deviations from Oracle-defined thresholds and follow standard operating procedures to investigate and resolve any underlying issues.

OCI services are designed to be highly available and are backed by service commitments for availability, manageability, and performance. OCI Service Level Agreement (SLA) are described in detail in the Oracle PaaS and IaaS Public Cloud Services Pillar Document and the Oracle Cloud Hosting and Delivery Policies, available at oracle.com/contracts/cloud-services/.

OCI also offers multiple tools and services to support the monitoring of obligations to its customers:

- The OCI **Monitoring** service enables customers to actively and passively monitor their cloud resources by using metrics and alarms. For more information, see docs.oracle.com/iaas/Content/Monitoring/Concepts/monitoringoverview.htm.
- For current **OCI status** by region, see ocistatus.oraclecloud.com/.

2.4.1: Outsourcing agreement

"The type and level of services to be provided and the contractual liabilities and obligations of the service provider should be clearly set out in a service agreement between AIs and their service provider."

The terms governing the provision of OCI services and the relationship between the parties are set out in the Cloud Services Agreement, the Ordering Document, the Financial Services Addendum, and the Data Processing Agreement for Oracle Services, which are available at oracle.com/contracts/cloud-services/.

2.5.2: Customer data confidentiality

"AIs should have controls in place to ensure that the requirements of customer data confidentiality are observed and proper safeguards are established to protect the integrity and confidentiality of customer information. Typical safeguards include, among other things:

- ***undertakings by the service provider that the company and its staff will abide by confidentiality rules, including taking account of the data protection principles set out in PDPO;***
- ***AIs' contractual rights to take action against the service provider in the event of a breach of confidentiality;***
- ***segregation or compartmentalisation of AIs' customer data from those of the service provider and its other clients; and***
- ***access rights to AIs' data delegated to authorized employees of the service provider on a need basis."***

Customers are responsible for the confidentiality of the data that they place in OCI. However, OCI has implemented policies, processes, and technical security controls that are designed to protect data at rest and in transit, and to help ensure the confidentiality and integrity of data stored in OCI.

The Oracle Data Processing Agreement describes Oracle's obligations in the event of an information breach. Individual tenant service agreements may describe additional responsibilities during a security event. Oracle Cloud Service Contracts and Cloud Delivery Policy documents are available at oracle.com/corporate/contracts/cloud-services/.

2.7.2: Contingency planning

"Contingency arrangements in respect of daily operational and systems problems would normally be covered in the service provider's own contingency plan. AIs should ensure that they have an adequate understanding of their service provider's contingency plan and consider the implications for their own contingency planning in the event that an outsourced service is interrupted due to failure of the service provider's system"

Customers are responsible for implementing appropriate contingency planning and arrangements.

In addition to the information provided in section 2.7.1, OCI provides the following documentation and resources:

- Best practices for protecting your cloud topology against disasters: docs.oracle.com/en/solutions/design-dr/
- OCI Cloud Adoption Framework, Technology Implementation for Extreme Reliability: docs.oracle.com/iaas/Content/cloud-adoption-framework/extreme-reliability.htm
- OCI Cloud Adoption Framework, Technology Implementation for High Availability: docs.oracle.com/iaas/Content/cloud-adoption-framework/high-availability.htm
- OCI Cloud Adoption Framework, Technology Implementation for Disaster Recovery: docs.oracle.com/iaas/Content/cloud-adoption-framework/disaster-recovery.htm

2.7.1: Contingency planning

"Contingency plans should be maintained and regularly tested by AIs and their service providers to ensure business continuity, e.g. in the event of a breakdown in the systems of the service provider or telecommunication problems with the host country."

Customers are responsible for implementing business continuity plans in their environment.

Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) to plan for and respond to potential business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across LOBs and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO), which oversees LOB plans and preparedness, in alignment with the ISO 22301 international standard for business continuity management. For more information, see oracle.com/corporate/security-practices/corporate/resilience-management/.

Additionally, OCI maintains a Business Impact Analysis (BIA) and Service Resiliency Plan (SRP) for each service. The plans outline procedures, ownership, roles, and responsibilities to be followed in the event of a disaster and are reviewed annually. OCI exercises each service's SRP at least annually.

Lastly, the Oracle Cloud Hosting and Delivery Policies describe the Oracle Cloud Service Continuity Policy, Oracle Cloud Services High Availability Strategy, Oracle Cloud Services Backup Strategy, and Oracle Cloud Service Level Agreement. For more information, see oracle.com/contracts/cloud-services/.

2.8.1: Access to outsourced data

"AIs should ensure that appropriate up-to-date records are maintained in their premises and kept available for inspection by the HKMA in accordance with §§55 and 56 of the Banking Ordinance and that data retrieved from the service providers are accurate and available in Hong Kong on a timely basis."

Customers are responsible for maintaining up-to-date records and making them available to the HKMA.

Additionally, the Oracle Data Processing Agreement and Financial Services Addendum provide customers and their regulators with the right to access and audit Oracle's compliance with its obligations under the cloud services agreements.

2.8.2: Access to outsourced data

"Access to data by the HKMA's examiners and the AI's internal and external auditors should not be impeded by the outsourcing. AIs should ensure that the outsourcing agreement with the service provider contains a clause which allows for supervisory inspection or review of the operations and controls of the service provider as they relate to the outsourced activity."

Customers are responsible for their regulatory compliance with respect to their use of any Oracle cloud services.

Additionally, the Oracle Data Processing Agreement and Financial Services Addendum provide customers and their regulators with certain rights to access and audit Oracle's compliance with its contractual obligations.

2.9.1: Additional concerns in relation to overseas outsourcing

"In addition to the issues mentioned from subsections 2.1 to 2.8 above, there are further concerns that need to be addressed in relation to overseas outsourcing:

- ***implications of the overseas outsourcing for AIs' risk profile - AIs should understand the risks arising from overseas outsourcing, taking into account relevant aspects of an overseas country (e.g. legal system, regulatory regime, sophistication of technology, infrastructure);***
- ***right of access to customers' data by overseas authorities such as the police and tax authorities - AIs should generally obtain a legal opinion from an international or other reputable legal firm in the relevant jurisdiction on this matter. This will enable them to be informed of the extent and the authorities to which they are legally bound to provide information. Right of access by such parties may be unavoidable due to compulsion of law. AIs should therefore conduct a risk assessment to evaluate the extent and possibility of such access taking place. AIs should notify the HKMA if overseas authorities seek access to their customers' data. If such access seems unwarranted the HKMA reserves the right to require the AI to take steps to make alternative arrangements for the outsourced activity;***
- ***notification to customers - AIs should generally notify their customers of the country in which the service provider is located (and of any subsequent changes) and the right of access, if any, available to the overseas authorities;***
- ***right of access to customers' data for examination by the HKMA after outsourcing - AIs should not outsource to a jurisdiction which is inadequately regulated or which has secrecy laws that may hamper access to data by the HKMA or AIs' external auditors. They should ensure that the HKMA has right of access to data. Such right of access should be confirmed in writing by both AIs and their home or host authorities, as the case may be;***
- ***§33 of the PDPO in respect of transfer of personal data outside Hong Kong – although §33 has not yet come into operation, AIs are advised to take account of the provisions therein and the potential impact on their plans in respect of overseas outsourcing; and***
- ***governing law of the outsourcing agreement – the agreement should preferably be governed by Hong Kong law."***

OCI operates within various regions across the globe. Data center regions are composed of one or more physically isolated and fault-tolerant data centers (also called availability domains).

Customers are responsible for selecting a data center region during their initial Oracle account setup in which to locate their tenancy. This setup provides customers with clear insight and control over the geographic location of their data. Customers are responsible for selecting a data region that meets their business, regulatory, and end-customer requirements. The customer's data stays within this region unless the customer chooses to move data outside the region.

The most up-to-date OCI data center region information is available at oracle.com/cloud/public-cloud-regions/.

Technology Risk Management (TM-G-1)

3.1.3: Security management, Information classification and protection

"Protection of information confidentiality should be in place regardless of the media (including paper and electronic media) in which the information is maintained. AIs should ensure that all media are adequately protected, and establish secure processes for disposal and destruction of sensitive information in both paper and electronic media."

Customers are responsible for defining policies and establishing controls for securely managing and protecting their media.

Oracle's Media Sanitation and Disposal Policy defines requirements for the removal of information from electronic storage media (sanitization) and disposal of information that is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. Electronic storage media includes laptops, hard drives, storage devices, and removable media such as tape.

3.1.4: Security management, Information classification and protection

"If cryptographic technology is used to protect the confidentiality and integrity of AIs' information, AIs should adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys. Sound practices of key management generally include:

- ***provision of a secure control environment for generation, distribution, storage, entry, use and archiving of cryptographic keys to safeguard against modification and unauthorized disclosure. In particular, the use of tamper-resistant storage is recommended to prevent the disclosure of the cryptographic keys; and***
- ***adequate off-site back-up and contingency arrangements for cryptographic keys which are subject to the same security controls as the production cryptographic keys."***

Customers are responsible for implementing industry-accepted cryptographic solutions.

Oracle has corporate standards that define 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.

The OCI **Vault** key management service provides centralized management of the encryption of customer data with keys that customers control. It can be used for the following tasks:

- Create master encryption keys and data encryption keys
- Rotate keys to generate new cryptographic material
- Enable or disable keys for use in cryptographic operations
- Assign keys to resources
- Use keys for encryption and decryption to safeguard data

Additionally, OCI **Block Volume**, **Object Storage**, **File Storage**, and **Streaming** services integrate with Vault to support the encryption of data in those services. For more information, see docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.

3.2.1: Authentication and access control

"Access to the information and application systems should be restricted by an adequate authentication mechanism associated with access control rules. Access control rules determine what application functions, system resources and data a user can access. For each application system, all users should be identified by unique user-identification codes (e.g. user IDs) with appropriate method of authentication (e.g. passwords) to ensure accountability for their activities."

Customers are responsible for implementing access control rules with appropriate methods of authentication for their applications and cloud environment.

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. Authorization depends on successful authentication, because controlling access to specific resources depends on establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: need to know, segregation of duties, and least privilege.

OCI restricts access to systems to authorized personnel only. Logging and monitoring of privileged access to information security management systems is enforced in accordance with Oracle's Logging and Log Analysis Policy.

The OCI Identity and Access Management (IAM) service provides identity and access management features such as authentication, single sign-on (SSO), and identity lifecycle management for Oracle Cloud and non-Oracle applications. For more information, see docs.oracle.com/iaas/Content/Identity/getstarted/identity-domains.htm.

3.3.1: Security administration and monitoring

"A security administration function and a set of formal procedures should be established for administering the allocation of access rights to system resources and application systems, and monitoring the use of system resources to detect any unusual or unauthorized activities. In particular, the function should cover the following areas:

- ***granting, changing and removing user access rights subject to proper approval of the information owners. In particular, proper procedures should be in place to ensure that a user's relevant access rights are removed when he leaves the AI or when his job responsibilities no longer require such rights;***
- ***ensuring the performance of periodic user access re-certification (e.g. on an annual basis) that confirms whether user access rights remain appropriate and obsolete user accounts have been removed from the systems;***
- ***reviewing security logs and violation reports in a timely manner; and***
- ***performing incident analysis, reporting and investigation."***

Customers are responsible for the security administration and monitoring of access rights to system resources in their environment.

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. Authorization depends on successful authentication, because controlling access to specific resources depends on establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: need to know, segregation of duties, and least privilege.

Access to the infrastructure and services that support OCI requires multifactor authentication (MFA), a VPN connection, and an SSH connection with a user account and a password or private key. OCI users with access to the code deployment tool that supports OCI systems are reviewed quarterly. Authentication logs for servers that support services, hypervisors, and bastion hosts are forwarded to a Security Information and Event Monitoring

(SIEM) tool, which is configured to store logs for at least 90 days. Access to the log repository is restricted to approved personnel.

3.3.2: Security administration and monitoring

"Proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) should be in place to mitigate the risk of unauthorized activities being performed by the security administration function"

Customers are responsible for the security administration and monitoring of access rights to system resources in their environment.

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. Authorization depends on successful authentication, because controlling access to specific resources depends on establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles: need to know, segregation of duties, and least privilege.

3.3.3: Security administration and monitoring

"AIs should establish incident response and reporting procedures to handle information security-related incidents during or outside office hours. The incident response and reporting procedures should include timely reporting to the HKMA of any confirmed IT-related fraud cases or major security breaches."

Customers are responsible for implementing incident response and reporting procedures, including reporting to the HKMA.

For information about Oracle Security Incident Response, see oracle.com/corporate/security-practices/corporate/security-incident-response.html.

3.6.1: Physical and personnel security

"Physical security measures should be in place to protect computer facilities and equipment from damage or unauthorized access. Critical information processing facilities should be housed in secure areas such as data centres and network equipment rooms with appropriate security barriers and entry controls. Access to these areas should be restricted to authorized personnel only and the access rights should be reviewed and updated regularly. Buildings should give minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities."

OCI data centers 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. Data centers that house OCI services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place.

The Oracle Supplier Information and Physical Security Standards outline the ethical, business conduct, and physical security requirements for data center vendors. The document applies to vendors who provide data center and colocation services to Oracle for its internal use or for the provision of Oracle services to its customers. See oracle.com/us/assets/oracle-supplier-contractor-security-070672.pdf.

3.6.2: Physical and personnel security

"AIs should consider fully the environmental threats (e.g. proximity to dangerous factories) when selecting the locations of their data centres. Moreover, physical and environmental controls should be implemented to monitor environmental conditions which could affect adversely the operation of information processing facilities (e.g. fire, explosives, smoke, temperature, water and dust). Equipment and facilities should be protected from power failures and electrical supply interference by, for example, installing uninterruptible power supply (UPS) and a backup generator."

Customers are responsible for selecting the OCI data region in which to locate their tenancy. OCI data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build sites and provider locations undergo an extensive risk evaluation by Oracle that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), and geopolitical considerations among other criteria.

The OCI Data Center Services (DCS) Program Management, Audit, Security, and Safety (PASS) team performs an assessment of data center and point of presence (PoP) site control environments, including physical security controls and environmental safeguards, prior to the data center hosting production traffic (go-live) and then thereafter in accordance with the schedule defined in the Data Assessment Program. Identified issues are evaluated and tracked through resolution.

Each data center vendor operates a preventive maintenance program to reduce the risk of a failure of environmental safeguards. The program includes the servicing of air handling units, fire suppression and detection equipment, uninterruptable power supply (UPS), battery arrays, and generators on a predefined basis by competent professionals who are qualified to complete the maintenance. In addition to routine servicing, generators are turned on and run for a defined period at regular intervals to meet local environmental regulations.

Critical mechanical and electrical components that support Oracle data halls and suites at each facility are designed with N+1, N+2, and occasionally 2N redundancy. Each data center is served by multiple connections to the power grid and are connected to redundant power feeds. In addition, infrastructure within Oracle data halls is connected to an UPS and generator. Generators have a minimum 24-hour supply of fuel and can carry the entire data center load.

Emergency backup power is used in OCI data halls in the event of power loss. Backup power provides time for an orderly shutdown of systems or a transition to an alternate power source. Emergency power shutoff capabilities are available for OCI data halls. The devices are protected against accidental or unauthorized access but are easily accessible for authorized personnel. Emergency lighting automatically activates in OCI data halls if power is disrupted.

3.6.3: Physical and personnel security

"In controlling access by third-party personnel (e.g. service providers) to secure areas, proper approval of access should be required and their activities should be closely monitored. It is also important that proper screening procedures including verification and background checks, especially for sensitive technology-related jobs, are developed for recruitment of permanent and temporary technology staff, and contractors"

Data center facility access is restricted to approved personnel based on job function. Requests for permanent access to a data center, Oracle data hall, or PoP are approved prior to access being provisioned. When a user with permanent data center, Oracle data hall, or PoP access is terminated, their access to is revoked within 14 days of termination. Users with permanent access to OCI data halls at each facility are reviewed at least quarterly, and any issues identified during the review are investigated and remediated.

All OCI guests to a facility must have a preapproved access request. Requests are documented in the electronic ticketing system and must include the region, availability domain, name of the visitor or guest as it appears on a government-issued ID, the company the individual works for, contact information, duration of access, and

business justification for access. OCI management must approve all access requests prior to access being granted. Visitors are required to show a government-issued ID, and they must be escorted at all times by an OCI employee with permanent access to the facility. Visitors are provided with a visitor badge, which does not enable them to access any nonpublic areas of the facility.

Access to OCI data halls requires two-factor authentication. Each user must present a valid access card along with a biometric fingerprint, hand scan, or retina scan. An alert in the operations center is triggered if the door to an Oracle data hall is left open for a predefined period. The access control systems are contained in the control room or rooms.

4.2.6: Project life cycle

"AIs should ensure that on-going maintenance and adequate support of software packages are provided by the software vendors and are specified in formal contracts. For mission-critical software packages, AIs may consider including in the contracts an escrow agreement, which allows them to obtain access to the source code of the software packages under certain circumstances, such as when the software vendors cease their business."

The Oracle Cloud Hosting and Delivery Policies describe the Oracle Cloud change management procedures that are designed to minimize service interruption during the implementation of changes. Changes made through change management procedures include system and service maintenance activities, upgrades and updates, and customer-specific changes. See oracle.com/contracts/cloud-services/.

4.3.1: Change management

"Change management is the process of planning, scheduling, applying, distributing and tracking changes to application systems, system software (e.g. operating systems and utilities), hardware, network systems, and other IT facilities and equipment. An effective change management process helps to ensure the integrity and reliability of the production environment. AIs should develop a formal change management process that includes:

- ***classification and prioritisation of changes and determination of the impact of changes;***
- ***roles and responsibilities of each relevant party, including IT functions and end-user departments, with adequate segregation of duties. This is to ensure that no single person can effect changes to the production environment without the review and approval of other authorized personnel;***
- ***program version controls and audit trails;***
- ***scheduling, tracking, monitoring and implementation of changes to minimise business disruption;***
- ***a process for rolling-back changes to re-instate the original programs, system configuration or data in the event of production release problems; and***
- ***a post implementation verification of the changes made (e.g. by checking the versions of major amendments)."***

Customers are responsible for any changes made to their environment, including, but not limited to, virtual networks, operating systems, virtual machines, databases, storage, and applications.

Changes to the infrastructure configurations and services that support OCI follow the Cloud Compliance Standard for Change Management and are documented in an access-controlled ticketing system, tested, and peer-reviewed prior to implementation. The ticketing system is configured to prevent the peer reviewer from being the same person that developed the change.

5.2.2: Performance monitoring and capacity planning

"Capacity planning should be extended to cover back-up systems and related facilities in addition to the production environment."

Customers are responsible for capacity planning in their cloud environment.

OCI offers the following services that can help customers monitor their cloud resource capacity information:

- OCI **Operations Insights** provides holistic insight into database and host resource use and capacity. For more information, see docs.oracle.com/iaas/operations-insights/doc/operations-insights.html.
- OCI **Resource Monitoring** enables customers to monitor the health, capacity, and performance of their OCI resources. For more information, see docs.oracle.com/iaas/Content/General/Concepts/resourcemonitoring.htm.

OCI maintains processes to monitor infrastructure capacity and creates a capacity forecast at least quarterly for critical system components to ensure that OCI has sufficient capacity to meet customer demand.

5.3.1: IT facilities and equipment maintenance

"To ensure the continued availability of AIs' technology related services, AIs should maintain and service IT facilities and equipment (e.g. computer hardware, network devices, electrical power distribution, UPS and air conditioning units) in accordance with the industry practice, and suppliers' recommended service intervals and specifications. Proper record keeping (including suspected or actual faults, and preventive and corrective maintenance records) is necessary for effective facility and equipment maintenance. A hardware and facility inventory should be kept to control and track all hardware and software purchased and leased. These records can also be used for regular inventory taking."

Customers are responsible for ensuring the continued availability of technology in their environment.

Each data center that hosts OCI services operates a preventive maintenance program to reduce the risk of a failure of environmental safeguards. The program includes the servicing of air handling units, fire suppression and detection equipment, uninterruptable power supply (UPS), battery arrays, and generators on a predefined basis by competent professionals who are qualified to complete the maintenance. In addition to routine servicing, generators are turned on and run for a defined period at regular intervals to meet local environmental regulations.

A building management system (BMS) is in place at each OCI data center for mechanical, electrical, and plumbing management and monitoring. The BMS monitors the temperature across the data hall and on each individual computer room air conditioning (CRAC) unit, where applicable. The BMS also monitors the humidity level and water detectors. If the humidity or temperature is above or below the predefined levels, or water is detected, an alarm or notification is triggered. The BMS is also connected to generators for activation in the event of a power outage.

OCI data center colocation vendors must adhere to the security and maintenance requirements as defined in the Supplier Co-location Security Standard and Oracle Supplier Information and Physical Security Standards.

OCI data centers 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. Data centers that house OCI services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security and availability events that may arise.

7.1.1: Management of technology outsourcing

"While AIs are expected to take into account the general guidance specified in SA-2 "Outsourcing" when managing technology outsourcing, they should also have regard to the following controls:
[...]

- *in case of outsourcing of critical technology services (e.g. data centre operations), AIs are expected to commission a detailed assessment of the technology service provider's IT control environment. The assessment should ideally be conducted by a party independent of the service provider. The independent assessment report should set out clearly the objectives, scope and results of the assessment and should be provided to the HKMA for reference;*
- *the outsourcing agreement should specify clearly, among other things, the performance standards and other obligations of the technology service provider, and the issue of software and hardware ownership. As technology service providers may further sub-contract their services to other parties, AIs should consider including a notification or an approval requirement for significant sub-contracting of services and a provision that the original technology service provider is still responsible for its sub-contracted services;*
- *further to the regular monitoring activities set out in SA-2 "Outsourcing", AIs should conduct an annual assessment to confirm the adequacy of the IT control environment of the provider of critical technology services;*
- *AIs should try to avoid placing excessive reliance on a single outside service provider in providing critical technology services; and*
- *AIs should develop a contingency plan for critical outsourced technology services to protect them from unavailability of services due to unexpected problems of the technology service provider14. This may include an exit management plan and identification of additional or alternate technology service providers for such support and services."*

Customers are responsible for implementing the controls described in 7.1.1.

OCI operates under policies that are generally aligned with the ISO/IEC 27002 Code of Practice for information security controls. The internal controls of OCI are subject to periodic testing by independent third-party audit organizations. The resulting attestations provide independent assessment of the security, privacy, and compliance controls of the applicable Oracle cloud services and can assist with an institution's compliance and reporting. Such attestations include CSA STAR; SOC 1, 2, and 3; and ISO/IEC 27001, 27017, 27018, 27701, 20000-1, and 9001. For more information, see oracle.com/corporate/cloud-compliance/.

OCI attestation reports and certificates are periodically published and may be made available to customers in the Oracle Cloud Console or through their customer account representative. For more information, see docs.oracle.com/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm.

Conclusion

Oracle is committed to helping customers operate globally in a fast-changing business environment and address the challenges and risks of outsourcing. Before deploying OCI services, Oracle recommends that cloud customers formally analyze their cloud strategy to determine the suitability of using the applicable Oracle cloud services in light of their own legal and regulatory compliance obligations. For more information, see oracle.com/corporate/cloud-compliance/.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle