ORACLE

Advisory: Oracle Cloud Infrastructure and Bank Negara Malaysia Risk Management in Technology

Description of Oracle Cloud Infrastructure Security Practices in the Context of the Bank Negara Malaysia RMiT Requirements

July 2023, Version 1.1

Public

Disclaimer

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

This document is for informational purposes only and is intended solely to assist you assessing your use of Oracle Cloud Infrastructure (OCI) in the context of the requirements applicable to you under the Bank Negara Malaysia Risk Management in Technology (RMiT) requirements. 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. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied on in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

The Bank Negara Malaysia RMiT requirements are subject to periodic changes or revisions by Bank Negara Malaysia. The current version of the requirements is available at www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+(RMiT).pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078.

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
July 2023	Minor updates
May 2023	Initial publication

Table of Contents

Introduction

Bank Negara Malaysia is the central bank for Malaysia and is mandated to promote monetary and financial stability conducive to the sustainable growth of the Malaysian economy. Bank Negara Malaysia has played a significant role in developing the financial system infrastructure and advancing the financial inclusion agenda.

Risk Management in Technology (RMiT) sets out the bank's requirements regarding financial institutions' management of technology risk, and provides guidance for risk management practices and controls that are commensurate with the increased technology risk exposure of the institution.

Document Purpose

This document is intended to provide relevant information about Oracle Cloud Infrastructure (OCI) that may assist you in determining the suitability of using OCI in relation to the Bank Negara Malaysia RMiT requirements.

The information contained in this document does not constitute legal advice. Customers are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by Oracle in regard to their specific legal and regulatory requirements.

About Oracle Cloud Infrastructure

Oracle's mission is to help 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 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.

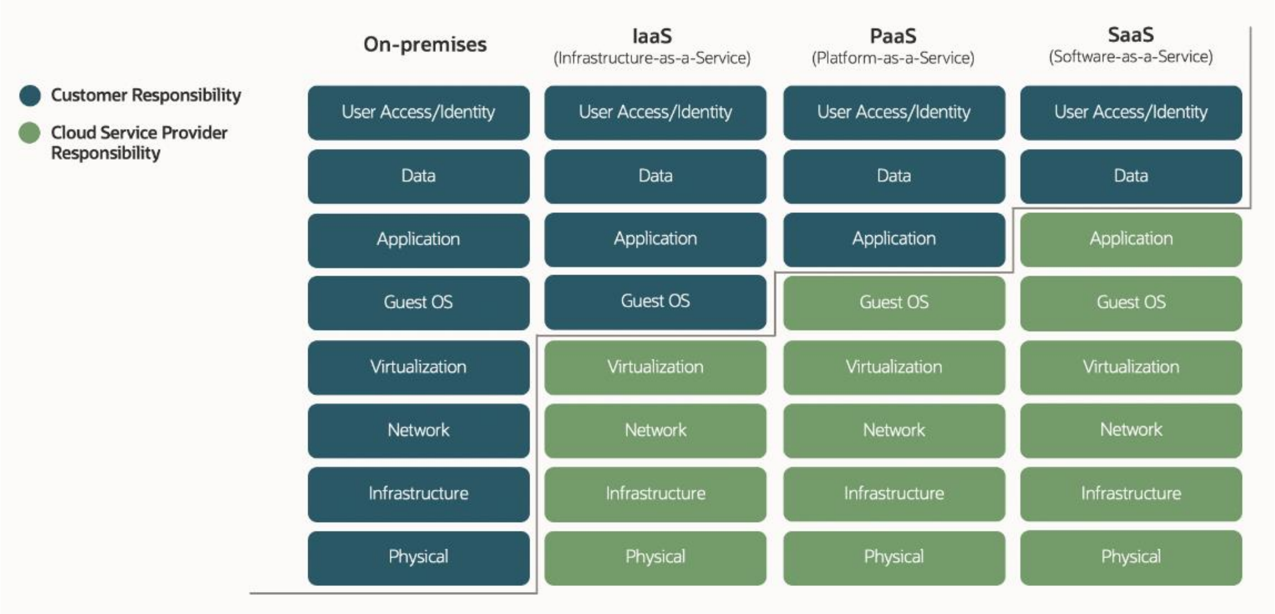
Customer Responsibility
Cloud Service Provider Responsibility
On-premises
IaaS (Infrastructure-as-a-Service)
PaaS (Platform-as-a-Service)
SaaS (Software-as-a-Service)
User Access/Identity
Data
Application
Guest OS
Virtualization
Network
Infrastructure
Physical

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

Bank Negara Malaysia RMiT Requirement Mapping to OCI

This section provides a summary of select Bank Negara Malaysia RMiT policy requirements that may be applicable to Malaysian financial institutions in their use of OCI services. Each applicable RMiT requirement has been mapped to the corresponding OCI control or capability, which may help financial institutions in their evaluation of OCI or in meeting their own requirements within the cloud shared management model. RMiT compliance, and any determination about the suitability of cloud services in the context of these requirements, is the sole responsibility of the customer. The complete set of Bank Negara Malaysia RMiT requirements are available at www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+(RMiT).pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078.

Chapter 10: Technology Operations Management

Technology Project Management

10.1 *A financial institution must establish appropriate governance requirements commensurate with the risk and complexity of technology projects undertaken. This shall include project oversight roles and responsibilities, authority and reporting structures, and risk assessments throughout the project life cycle.*

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

10.2 *The risk assessments shall identify and address the key risks arising from the implementation of technology projects. These include the risks that could threaten successful project implementation and the risks that a project failure will lead to a broader impact on the financial institution's operational capabilities.*

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

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

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

System Development and Acquisition

10.4 *A financial institution should establish an enterprise architecture framework (EAF) that provides a holistic view of technology throughout the financial institution. The EAF is an overall technical design and high-level plan that describes the financial institution's technology infrastructure, systems' inter- connectivity and security controls. The EAF facilitates the conceptual design and maintenance of the network infrastructure, related technology controls and policies, and serves as a foundation on which financial institutions plan and structure system development and acquisition strategies to meet business goals.*

Customers are solely responsible for establishing an enterprise architecture framework for their environment.

Oracle offers resources such as the OCI Cloud Adoption Framework and OCI Architecture Center that may assist customers in developing a suitable cloud architecture.

Cryptography

10.16 *A financial institution must establish a robust and resilient cryptography policy to promote the adoption of strong cryptographic controls for protection of important data and information. This policy, at a minimum, shall address requirements for:*

(a) the adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation;

(b) the adoption of robust and secure processes in managing cryptographic key lifecycles which include generation, distribution, renewal, usage, storage, recovery, revocation and destruction;

(c) the periodic review, at least every three years, of existing cryptographic standards and algorithms in critical systems, external linked or transactional customer-facing applications to prevent exploitation of weakened algorithms or protocols; and

(d) the development and testing of compromise-recovery plans in the event of a cryptographic key compromise. This must set out the escalation process, procedures for keys regeneration, interim measures, changes to business-as-usual protocols and containment strategies or options to minimise the impact of a compromise.

Customers are solely responsible for establishing their cryptography policies.

OCI offers the Vault key management service, which may help customers meet these requirements. Vault is a managed service that customers can use to centrally manage the encryption keys that protect data and the secret credentials that they use to securely access resources. Vaults securely store master encryption keys and secrets that might otherwise be stored in configuration files or in code. Specifically, depending on the protection mode, keys are stored either on the server or on highly available and durable hardware security modules (HSMs) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification.

The key encryption algorithms that the Vault service supports includes the Advanced Encryption Standard (AES), the Rivest-Shamir-Adleman (RSA) algorithm, and the elliptic curve digital signature algorithm (ECDSA).

Customers can create and use AES symmetric keys and RSA asymmetric keys for encryption and decryption. They can also use RSA or ECDSA asymmetric keys for signing digital messages. For more information, see docs.oracle.com/iaas/Content/KeyManagement/home.htm.

Oracle has corporate standards that define approved cryptographic algorithms and protocols. Oracle's products and services, along with security-related updates, are designed with industry best practice in mind. Oracle modifies these standards as the industry and technology evolve, to enforce, for example, the timely deprecation of weaker encryption algorithms.

10.18 *A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non-repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.*

Customers are responsible for implementing cryptographic solutions to meet their objectives.

The following OCI services enable at-rest data encryption by default, by using the AES algorithm with 256-bit encryption. In-transit control plane data is encrypted by using Transport Layer Security (TLS) 1.2 or later. Customers can use these services and features to help them meet the encryption requirements.

- **Object Storage** enables customers to store unstructured data of many content types. This regional service stores data redundantly across multiple storage servers and multiple availability domains. It actively monitors and provides data redundancy. If a redundancy loss is detected, Object Storage automatically creates more data copies. For more information, see docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm.
- **Block Volume** enables customers to use a block volume as a regular hard drive when it's attached and connected to a Compute instance. Volumes are automatically replicated to help protect against data loss. For more information, see docs.oracle.com/iaas/Content/Block/Concepts/overview.htm.
- **File Storage** enables customers to manage shared file systems and mount targets, and create file system snapshots. File storage uses synchronous replication and high-availability failover for resilient data protection. For more information, see docs.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm.
- **Vault** enables customers to centrally manage encryption keys. For more information, see docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.

Additionally, the Oracle Information Protection Policy defines requirements for protecting data through encryption, and the OCI Standard for Encryption establishes appropriate encryption methods to protect the confidentiality, integrity, and availability of customer-owned data.

10.19 *A financial institution must ensure cryptographic controls are based on the effective implementation of suitable cryptographic protocols. The protocols shall include secret and public cryptographic key protocols, both of which shall reflect a high degree of protection to the applicable secret or private cryptographic keys. The selection of such protocols must be based on recognised international standards and tested accordingly. Commensurate with the level of risk, secret cryptographic key and private-cryptographic key storage and encryption/decryption computation must be undertaken in a protected environment, supported by a hardware security module (HSM) or trusted execution environment (TEE).*

Customers are responsible for implementing effective cryptographic controls and protocols to meet their objectives.

The following OCI services enable at-rest data encryption by default, by using the AES algorithm with 256-bit encryption. In-transit control plane data is encrypted by using TLS 1.2 or later. Customers can use these services and features to help them meet the encryption requirements.

- **Object Storage** enables customers to store unstructured data of many content types. This regional service stores data redundantly across multiple storage servers and multiple availability domains. It actively monitors and provides data redundancy. If a redundancy loss is detected, Object Storage automatically creates more data copies. For more information, see docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm.
- **Block Volume** enables customers to use a block volume as a regular hard drive when it's attached and connected to a Compute instance. Volumes are automatically replicated to help protect against data loss. For more information, see docs.oracle.com/iaas/Content/Block/Concepts/overview.htm.
- **File Storage** enables customers to manage shared file systems and mount targets, and create file system snapshots. File storage uses synchronous replication and high-availability failover for resilient data protection. For more information, see docs.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm.
- **Vault** enables customers to centrally manage and control use of keys and secrets across a wide range of OCI services and applications. OCI Vault is a secure, resilient managed service that lets customers focus on their data encryption needs without worrying about time-consuming administrative tasks such as hardware provisioning, software patching, and high availability.

  Key management uses HSMs that meet FIPS 140-2 Security Level 3 security certification. Customers can create master encryption keys protected either by HSM or software. With the HSM-protected keys, all the cryptographic operations and storage of keys are inside the HSM. With the software-protected keys, encryption keys are stored and processed in software but are secured at rest with a root key from HSM.

  For more information, see docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.

Additionally, the Oracle Information Protection Policy defines requirements for protecting data through encryption, and the OCI Standard for Encryption establishes appropriate encryption methods to protect the confidentiality, integrity, and availability of customer-owned data.

Data Centre Resilience

Data Centre Infrastructure

10.21 *A financial institution must specify the resilience and availability objectives of its data centres which are aligned with its business needs. The network infrastructure must be designed to be resilient, secure and scalable. Potential data centre failures or disruptions must not significantly degrade the delivery of its financial services or impede its internal operations.*

Customers are responsible for determining the resilience and availability objectives that align with their business needs.

OCI is organized by regions, which are built within a certain geography. Each region has one, two, or three availability domains, and each availability domain is divided into multiple fault domains. This resilient service architecture provides multiple layers of redundancy at the node, service, and hardware component levels.

Data centers hosting Oracle cloud services are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate sites and provider locations undergo an extensive risk evaluation that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), standards compliance, and geopolitical considerations among other criteria.

Oracle cloud service 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 housing Oracle Cloud Infrastructure 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. Personnel are trained in incident response and escalation procedures to address security and availability events that may arise.

10.22 *A financial institution must ensure production data centres are concurrently maintainable. This includes ensuring that production data centres have redundant capacity components and distribution paths serving the computer equipment.*

Oracle contracts with third-party data center colocation vendors to provide dedicated data halls and suites for the use of OCI. The Oracle Supplier Information and Physical Security Standard and the Supplier Co-Location Security Standard apply to vendors who provide data center colocation services. These standards include, but are not limited to, the following requirements:

- Onsite generators must have fuel capacity that provides at least 48 hours of operational availability when at full load. Supplier must also demonstrate the capability to source fuel from a diverse group of suppliers within 18 hours, by providing evidence of, for example, contracts with multiple fuel suppliers.
- Regular testing on each generator must be performed and documented to ensure that they operate as expected in the event of disruption to the main power supplies.
- Backup power must be available to support the alarm system, access control, video systems, and other supporting security infrastructure. Where batteries are used as the backup power source, a minimum of eight hours of power must be available.
- Supplier must maintain a preventative maintenance program with documented procedures that address critical systems such as UPS, HVAC, generators, and fire suppression. Written procedures must be documented, reviewed, and published regularly.
- The facility must have a central monitor and maintain temperature and humidity within Oracle data halls. Alarms are automatically generated for any events which exceed environmental thresholds.

For more information, see oracle.com/corporate/security-practices/corporate/supply-chain/suppliers.html.

10.23 *In addition to the requirement in paragraph 10.22, large financial institutions are also required to ensure recovery data centres are concurrently maintainable.*

Customers are responsible for implementing a disaster recovery solution that meets their business objectives.

Deploying workloads across multiple Oracle Cloud data regions can help protect against disaster scenarios that impact data center or data region failure. Depending on a customer's disaster recovery goals, they can back up or replicate their data to another data region or set up a fully active-to-active standby in another data region. For more information, see docs.oracle.com/iaas/Content/cloud-adoption-framework/disaster-recovery.htm.

All Oracle Cloud data regions are subject to the Oracle Supplier Information and Physical Security Standard and the Supplier Co-Location Security Standard as described in paragraph 10.22.

10.24 *A financial institution shall host critical systems in a dedicated space intended for production data centre usage. The dedicated space must be physically secured from unauthorised access and is not located in a disaster-prone area. A financial institution must also ensure there is no single point of failure (SPOF) in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure. A financial institution must also ensure adequate maintenance, and holistic and continuous monitoring of these critical components with timely alerts on faults and indicators of potential issues.*

Customers are solely responsible for determining the criticality of the applications and workloads running on OCI.

Oracle contracts with third-party data center colocation vendors to provide dedicated data halls and suites for the use of OCI. The Oracle Supplier Information and Physical Security Standard and the Supplier Co-Location Security Standard apply to vendors who provide data center colocation services. These standards include, but are not limited to, the following physical security requirements:

- Onsite generators must have fuel capacity that provides at least 48 hours of operational availability when at full load. Supplier must also demonstrate the capability to source fuel from a diverse group of suppliers within 18 hours, by providing evidence of, for example, contracts with multiple fuel suppliers.
- Regular testing on each generator must be performed and documented to ensure that they operate as expected in the event of disruption to the main power supplies.
- Backup power must be available to support the alarm system, access control, video systems, and other supporting security infrastructure. Where batteries are used as the backup power source, a minimum of eight hours of power must be available.
- Supplier must maintain a preventative maintenance program with documented procedures that address critical systems such as UPS, HVAC, generators, and fire suppression. Written procedures must be documented, reviewed, and published regularly.
- The facility must have a central monitor and maintain temperature and humidity within Oracle data halls. Alarms are automatically generated for any events which exceed environmental thresholds.

For more information, see oracle.com/corporate/security-practices/corporate/supply-chain/suppliers.html.

OCI requires measures from its colocation suppliers to protect its assets in colocation facilities. Following are some of the requirements for colocation facilities:

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

For more information, see oracle.com/corporate/security-practices/corporate/supply-chain/suppliers.html.

10.25 *A financial institution is required to appoint a technically competent external service provider to carry out a production data centre resilience and risk assessment (DCRA) and set proportionate controls aligned with the financial institution's risk appetite. The assessment must consider all major risks and determine the current level of resilience of the production data centre. A financial institution must ensure the assessment is conducted at least once every three years or whenever there is a material change in the data centre infrastructure, whichever is earlier. The assessment shall, at a minimum, include a consideration of whether the requirements in paragraphs 10.22 to 10.24 have been adhered to. For data centres managed by third party service providers, a financial institution may rely on independent third-party assurance reports provided such reliance is consistent with the financial institution's risk appetite and tolerance, and the independent assurance has considered similar risks and meets the expectations in this paragraph for conducting the DCRA. The designated board-level committee must deliberate the outcome of the assessment.*

Customers are solely responsible for conducting a risk assessment and establishing controls aligned with their risk appetite and business objectives.

OCI regularly undergoes independent third-party audits to examine the implementation of policies, procedures and controls. The SOC 1, SOC 2, SOC 3, PCI DSS, ISO 27001, ISO 27017, 27018, and other OCI assessment reports and certifications are made available to the customer on-demand in the Oracle Cloud Console. For information about OCI's current compliance programs, see Oracle Cloud Compliance at oracle.com/corporate/cloud-compliance.

Data Centre Operations

10.26 *A financial institution must ensure its capacity needs are well-planned and managed with due regard to business growth plans. This includes ensuring adequate system storage, central processing unit (CPU) power, memory, and network bandwidth. A financial institution shall involve both the technology stakeholders and the relevant business stakeholders within the financial institution in its development and implementation of capacity management plans.*

Customers are responsible for planning and monitoring their data processing capacity to help meet their business objectives and growth plans.

However, OCI maintains processes to monitor infrastructure capacity and creates capacity forecasts at least quarterly for critical system components.

OCI offers the following services and features that may assist customers in meeting their capacity planning requirements:

- **Capacity Reservation** enables customers to reserve capacity for future usage and ensure that capacity is available to create compute instances whenever needed. For more information, see docs.oracle.com/iaas/Content/Compute/Tasks/reserve-capacity.htm.
- **Dedicated Capacity** enables customers to run VM instances on dedicated servers that are a single tenant and not shared with other customers. When creating a dedicated virtual machine host, customers select a shape, which determines how much capacity is available and what type of instance can be launched on the host. For more information, see docs.oracle.com/iaas/Content/Compute/Concepts/dedicatedvmhosts.htm.
- **Operations Insights** provides customers with 360-degree insight into the resource utilization and capacity of databases and hosts. Customers can use it to analyze CPU and storage resources, forecast issues, and proactively identify SQL performance issues across a database fleet. For more information, see docs.oracle.com/iaas/operations-insights/index.html.

10.27 *A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.*

Customers are solely responsible for establishing monitoring procedures in their environment.

OCI offers a suite of Observability and Management services, including the following one, that customers can use to track performance and capacity of their cloud resources:

- **Monitoring** enables customers to monitor the health, capacity, and performance of their OCI resources by using metrics and alarms. For more information, see docs.oracle.com/iaas/Content/Monitoring/Concepts/monitoringoverview.htm

10.28 *A financial institution must segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity. In the case where vendors' or programmers' access to the production environment is necessary, these activities must be properly authorised and monitored.*

In such cases where the financial institution is running their applications and workloads on OCI, Oracle contracts with third-party data center colocation vendors to provide dedicated data halls and suites for the use of OCI. The data halls within each data center are for the exclusive use of OCI. The term *data hall* refers to any physically separated and secured computer room housing OCI equipment, including equipment used to host customer data. *Separation* refers to physical barriers, such as solid walls or metal security caged areas.

OCI restricts facility access to approved personnel based on job function. Requests for permanent access to a data center are approved prior to access being provisioned. Users with permanent access to data halls at each facility are reviewed at least quarterly. 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 an electronic ticketing system and must include the region, availability domain, name of the guest as it appears on a government-issued ID, company the individual works for, contact information, duration of access, and business justification for access.

Refer to the data center operations physical security controls described in paragraph 10.24.

10.29 *A financial institution must establish adequate control procedures for its data centre operations, including the deployment of relevant automated tools for batch processing management to ensure timely and accurate batch processes. These control procedures shall also include procedures for implementing changes in the production system, error handling as well as management of other exceptional conditions.*

Oracle contracts with third-party data center colocation vendors to provide dedicated data halls and suites for the use of OCI. The Oracle Supplier Information and Physical Security Standard and the Supplier Co-Location Security Standard apply to vendors who provide data center colocation services and define the control procedures for change management.

Changes to infrastructure configurations and services that support the system follow the OCI Standard for Change Management and are documented in an access-controlled ticketing system, tested, and peer-reviewed prior to implementation.

10.30 *A financial institution is required to undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that existing controls are adequate in protecting sensitive data at all times. A financial institution must also maintain a sufficient number of backup copies of critical data, the updated version of the operating system software, production programs, system utilities, all master and transaction files and event logs for recovery purposes. Backup media must be stored in an environmentally secure and access-controlled backup site.*

Customers are solely responsible for implementing a backup strategy that meets their business objectives and policies.

Oracle offers solutions to help customers develop backup and disaster recovery plans to meet their business continuity objectives. For more information, visit oracle.com/cloud/backup-and-disaster-recovery/.

Network Resilience

10.33 *A financial institution must design a reliable, scalable and secure enterprise network that is able to support its business activities, including future growth plans.*

Customers are responsible for designing a reliable and secure enterprise network to support their business activities.

Customers need to set up at least one virtual cloud network (VCN) when they launch an instance. For additional information about OCI networking services, see docs.oracle.com/iaas/Content/Network/Concepts/overview.htm.

10.34 *A financial institution must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats.*

Customers are responsible for designing a reliable and secure enterprise network to support their business activities.

OCI offers the following services that customers can use to detect and respond to potential threats in their cloud service environment:

- **Threat Intelligence** aggregates threat-intelligence data across many different sources and curates this data to provide actionable guidance for threat detection and prevention in Cloud Guard and other OCI services. For more information, see docs.oracle.com/iaas/Content/threat-intel/using/overview.htm.
- **Cloud Guard** compares data from Threat Intelligence to Audit logs and telemetry to detect suspicious activity and report it as a problem. For more information, see docs.oracle.com/iaas/Content/Security/Concepts/security_features.htm#Cloud_Guard.
- **Vulnerability Scanning** helps improve security posture by routinely checking compute instances and container images for potential vulnerabilities. The service generates reports with metrics and details about these vulnerabilities and assigns each a risk level. For more information, see docs.oracle.com/iaas/Content/Security/Concepts/security_features.htm#security_features_topic_Scanning.

Additionally, Oracle employs intrusion-detection systems within the Oracle intranet to provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle utilizes a network-based monitoring approach to detect attacks on open firewall ports within Oracle's intranet. Events are analyzed using signature detection, which is a pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as soon as new releases become available for commercial distribution. Alerts are forwarded to Oracle's IT security for review and response to potential threats.

Oracle maintains teams of specialized security professionals for the purpose of assessing the security strength of the company’s infrastructure, products, and services. These teams perform various levels of security testing. This includes operational security scanning and penetration testing.

For more information about Oracle security testing practices, see oracle.com/corporate/security-practices/assurance/development/ethical-hacking.html#team.

10.35 *A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.*

Customers are solely responsible for establishing appropriate network monitoring.

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

OCI offers a suite of Observability and Management services, including the following one, that customers can use to track performance and capacity of their cloud resources:

- **Monitoring** enables customers to monitor the health, capacity, and performance of their OCI resources by using metrics and alarms. For more information, see docs.oracle.com/iaas/Content/Monitoring/Concepts/monitoringoverview.htm.

10.36 *A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.*

Oracle's Corporate Security programs are designed to protect Oracle and customer information assets.

Oracle has implemented and maintains strong network controls for the protection and control of both Oracle and customer data during its transmission. Oracle's network security policy establishes requirements for network management, network access, and network device management, including authentication and authorization requirements for both physical devices and software-based systems.

For administration of network security and network-management devices, Oracle requires IT personnel to use secure protocols with authentication, authorization, and strong encryption. Network devices must be located in an environment protected with physical access controls and other physical security measure standards defined by Global Physical Security (GPS).

Communications to and from the Oracle corporate network must pass through network security devices at the border of Oracle's internal corporate network. Remote connections to the Oracle corporate network must exclusively use virtual private networks (VPNs) that have been approved via the Corporate Security Solution Assurance Process (CSSAP). Corporate systems available outside the corporate network are protected by alternative security controls such as multifactor authentication (MFA).

The OCI Global Network Operations Center (GNOC) is the front line for physical network issues. The GNOC is responsible for performing triage, incident mitigation, data collection, technical analysis, and redirection, as needed.

Customers are responsible for designing, implementing, operating, and maintaining their virtual cloud network (VCN) in accordance with their policies and procedures for firewall rules, network segmentation, access control lists, load balancing, routing, and encryption of data in transit relevant to their own environment. Access to customer VCNs is controlled by a combination of security lists and routing tables configured by the customer. For more information about OCI Networking components, see docs.oracle.com/iaas/Content/Network/Concepts/overview.htm.

10.38 *A financial institution must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years.*

Customers are responsible for implementing sufficient and relevant network device logs in their environment.

OCI offers a suite of Observability and Management services, such as the following ones, that customers can use to monitor their cloud resources:

- **Monitoring:** Enables customers to monitor the health, capacity, and performance of their OCI resources by using metrics and alarms. For more information, see docs.oracle.com/iaas/Content/Monitoring/Concepts/monitoringoverview.htm.
- **Logging**: Provides logs from OCI resources, including critical diagnostic information that describes how resources are performing and being accessed. For more information, see docs.oracle.com/iaas/Content/Logging/Concepts/loggingoverview.htm.

10.39 *A financial institution must implement appropriate safeguards to minimise the risk of a system compromise in one entity affecting other entities within the group. Safeguards implemented may include establishing logical network segmentation for the financial institution from other entities within the group.*

Customers are responsible for implementing appropriate safeguards to minimize risk within their own environment.

Oracle has designed OCI's physical network for customer and service isolation. It's segmented into enclaves with unique communication profiles. Access into and out of these enclaves is controlled, monitored, and policy driven.

Additionally, OCI deploys the following security measures:

- A host-intrusion-detection system that monitors and detects security events
- A network-intrusion-detection system on the edge to monitor production traffic and detect security, and events
- Antivirus software to detect malware

Third Party Service Provider Management

10.42 *A financial institution must conduct proper due diligence on the third-party service provider's competency, system infrastructure and financial viability as relevant prior to engaging its services. In addition, an assessment shall be made of the third-party service provider's capabilities in managing the following specific risks—*

(a) data leakage such as unauthorised disclosure of customer and counterparty information;(b) service disruption including capacity performance;
(c) processing errors;
(d) physical security breaches;
(e) cyber threats;
(f) over-reliance on key personnel;
(g) mishandling of confidential information pertaining to the financial institution or its customers in the course of transmission, processing or storage of such information; and
(h) concentration risk.

To assist customers in performing their own due diligence before using OCI services, Oracle provides the following resources:

- Oracle Corporate Security Practices: oracle.com/corporate/security-practices/corporate/
- Consensus Assessment Initiative Questionnaire (CAIQ) for OCI: oracle.com/a/ocom/docs/oci-corporate-caiq.pdf
- Oracle Investor Relations: investor.oracle.com/home/default.aspx

- Oracle Services Privacy Policy: oracle.com/legal/privacy/services-privacy-policy.html
- Data Processing Agreement for Oracle Services: oracle.com/corporate/contracts/cloud-services/contracts.html

10.43 *A financial institution must establish service-level agreements (SLA) when engaging third party service providers. At a minimum, the SLA shall contain the following:*

(a) access rights for the regulator and any party appointed by the financial institution to examine any activity or entity of the financial institution. This shall include access to any record, file or data of the financial institution, including management information and the minutes of all consultative and decision-making processes;
(b) requirements for the service provider to provide sufficient prior notice to financial institutions of any sub-contracting which is substantial;
(c) a written undertaking by the service provider on compliance with secrecy provisions under relevant legislation. The SLA shall further clearly provide for the service provider to be bound by confidentiality provisions stipulated under the contract even after the engagement has ended;
(d) arrangements for disaster recovery and backup capability, where applicable;
(e) critical system availability; and
(f) arrangements to secure business continuity in the event of exit or termination of the service provider.

The Oracle Data Processing Agreement (DPA) and Cloud Financial Service Addendum (FSA) provide audit rights for customers and their regulators.

Oracle may use subprocessors or strategic subcontractors for some of its cloud services. Oracle publishes a list of its subprocessors and strategic subcontractors (collectively “subcontractors”), which is available to customers through My Oracle Support (see Doc ID 111.2 on support.oracle.com/).

Oracle commits to deliver the services at the agreed level of availability and quality, and offers multiple tools and services to support monitoring obligations of its customers. Customers can access metrics on the Service Level Availability for OCI services that customers have purchased under their order through the Customer Notification Portal at ocistatus.oraclecloud.com/.

For a period of 60 days upon termination of the Oracle Cloud Services, Oracle will make available, via secure protocols and in a structured, machine-readable format, customer content residing in the production Oracle Cloud Services, or keep the service system accessible, for the purpose of data retrieval by the customer.

The Financial Service Addendum provides customers with the ability to order transition services and transition assistance to facilitate the transfer or the re-incorporation of the concerned function back to the customer or a third-party provider.

10.44 *A financial institution must ensure its ability to regularly review the SLA with its third-party service providers to take into account the latest security and technological developments in relation to the services provided.*

Financial institutions can review OCI Service Level Agreement details in the Oracle Cloud Hosting and Delivery Policies, available at oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf.

10.45 *A financial institution must ensure its third-party service providers comply with all relevant regulatory requirements prescribed in this policy document.*

Oracle will abide by all laws and regulations that govern the provision of the Oracle Cloud Infrastructure services, and the financial, operational, and compliance requirements that Oracle has established for the services.

10.46 *A financial institution must ensure data residing in third party service providers are recoverable in a timely manner. The financial institution shall ensure clearly defined arrangements with the third-party service provider are in place to facilitate the financial institution's immediate notification and timely updates to the Bank and other relevant regulatory bodies in the event of a cyber-incident.*

Customers are responsible for designing and implementing backup and replication processes in line with their requirements and policies.

Customers must choose a replication policy after activating an OCI storage service subscription. The replication policy defines the customer's primary data center and also specifies whether customer data should be replicated to a geographically distant (secondary) data center. This feature enables recovery of data in the event of any disaster at the primary data center. In this case, data is written to the primary data center and replicated asynchronously to the secondary data center.

OCI provides customers with tools to back up and restore the systems by leveraging snapshots. See docs.oracle.com/iaas/Content/File/Tasks/managingsnapshots.htm.

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 at oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html.

Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed data has been accessed by an unauthorized entity. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to security events and incidents.

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

10.47 *A financial institution must ensure the storage of its data is at least logically segregated from other clients of the third-party service provider. There shall be proper controls over and periodic review of the access provided to authorised users.*

Each OCI tenancy is logically isolated from other tenants on the network level to ensure confidentiality and integrity of data transmitted.

OCI access controls are implemented, monitored, and tested periodically by independent third-party assessors. The resulting attestation reports and certificates are available to OCI customers in the Oracle Cloud Console. For more information, see docs.oracle.com/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm.

10.48 *A financial institution must ensure any critical system hosted by third party service providers have strong recovery and resumption capability and provisions to facilitate an orderly exit in the event of failure or unsatisfactory performance by the third-party service provider.*

Customers are responsible for designing and implementing backup and replication processes in line with their requirements and policies.

Oracle Cloud contracts describe the customer's termination rights and exit provisions. The FSA includes transition services and transition assistance, data retrieval, and data deletion clauses to help customers to exit cloud services with minimal disruption to their business.

Cloud Services

10.49 *A financial institution must fully understand the inherent risk of adopting cloud services. In this regard, a financial institution is required to conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet. The assessment must specifically address risks associated with the following:*

(a) sophistication of the deployment model;
(b) migration of existing systems to cloud infrastructure;
(c) location of cloud infrastructure;
(d) multi-tenancy or data co-mingling;
(e) vendor lock-in and application portability or interoperability;
(f) ability to customise security configurations of the cloud infrastructure to ensure a high level of data and technology system protection;
(g) exposure to cyber-attacks via cloud service providers;
(h) termination of a cloud service provider including the ability to secure the financial institution's data following the termination;
(i) demarcation of responsibilities, limitations and liability of the service provider; and
(j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.

Customers are solely responsible for conducting the necessary risk assessment to determine the suitability of OCI services, features, and functionality in regard to their specific legal and regulatory requirements.

Oracle provides serveral resources to assist its customers in conducting the necessary risk assessments and due diligence:

- Oracle Corporate Securty Practices: oracle.com/corporate/security-practices/corporate/
- Oracle Cloud Compliance: oracle.com/corporate/cloud-compliance/
- Consensus Assessment Initiative Questionnaire (CAIQ) for OCI: oracle.com/a/ocom/docs/oci-corporate-caiq.pdf
- OCI Documentation: docs.oracle.com/en-us/iaas/Content/home.htm
- Oracle Cloud Services contracts: oracle.com/contracts/cloud-services/

10.51 *A financial institution is required to consult the Bank prior to the use of public cloud for critical systems. The financial institution is expected to demonstrate that specific risks associated with the use of cloud services for critical systems have been adequately considered and addressed. The risk assessment shall address the risks outlined in paragraph 10.49 as well as the following areas:*

(a) the adequacy of the over-arching cloud adoption strategy of the financial institution including:
(i) board oversight over cloud strategy and cloud operational management;
(ii) senior management roles and responsibilities on cloud management;
(iii) conduct of day-to-day operational management functions;
(iv) management and oversight by the financial institution of cloud service providers;
(v) quality of risk management and internal control functions; and
(vi) strength of in-house competency and experience;
(b) the availability of independent, internationally recognised certifications of the cloud service providers, at a minimum, in the following areas:
(i) information security management framework, including cryptographic modules such as used for encryption and decryption of user data; and
(ii) cloud-specific security controls for protection of customer and counterparty or proprietary information including payment transaction data in use, in storage and in transit; and
(c) the degree to which the selected cloud configuration adequately addresses the following attributes:
(i) geographical redundancy;
(ii) high availability;
(iii) scalability;
(iv) portability;
(v) interoperability; and
(vi) strong recovery and resumption capability including appropriate alternate Internet path to protect against potential Internet faults.

Customers are solely responsible for any interactions with the Bank regarding their use of cloud services, including addressing any risks identified in the risk assessment process covered in paragraph10.49.

The OCI information security management plan is subject to independent third-party audit on a biannual basis. Customers can access OCI attestation reports and certificates in the Oracle Cloud Console. For more information, see docs.oracle.com/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm.

Customers are given the option to deploy their instances and services in multiple geographically separated regions for redundancy, high availability, and disaster recovery. Some Oracle Cloud regions have one availability domain, while other regions have three or more availability domains that are in close physical proximity to provide minimal latency but are fault isolated and allow for synchronous replication and high uptime.

OCI secure file transfer functionality is built on commonly used network access storage platforms and uses secured protocols for transfer. The functionality can be used to upload files to a secured location, most commonly for data import and export on the OCI hosted service, or to download files at service termination. Customers can export data from OCI services and manage their own data, including industry-standard formats.

10.53 *A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.*

Customers retain all ownership and intellectual property rights to the data and applications they bring into OCI.

For more information, see Oracle Cloud Services contracts at https://www.oracle.com/contracts/cloud-services/.

Access Control

10.54 *A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems.*

Customers are solely responsible for managing access to the information assets in their environment.

OCI offers the following service that might help customers meet their identity and access management requirement:

- **Identity and Access Management (IAM)** lets customers control who has access to cloud resources. Customers can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/iaas/Content/Identity/home1.htm.

The Oracle Logical Access Control Policy is applicable to access control decisions for Oracle employees and any information-processing facility for which Oracle has administrative authority. Authorization is dependent on successful authentication, since controlling access to specific resources depends upon 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: Does the user require this access for their job function?
- Segregation of duties: Will the access result in a conflict of interest?
- Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?

For more information, see Oracle Access Control Policies and Practices.

The Logical Access Controls Policy also describes logical access control requirements for Oracle systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined users with access to Oracle systems that are not internet-facing, publicly accessible systems.

The Logical Access Controls Policy sets forth the requirements for information owners to define, document, and enforce logical access controls for the information systems for which they have responsibility and that process confidential Oracle internal, restricted, and highly restricted information, including information held on behalf of customers, partners, and other third parties. OCI policies and procedures have established security controls in support of MFA, in which two factors work together, requiring an extra layer of security to verify the user's identity and complete the sign-in process.

OCI personnel access the environments through a segregated network connection, which is dedicated to environment access control and isolated from Oracle's internal corporate network traffic. The dedicated network functions as a secured access gateway between support systems and target application and database servers.

10.55 *In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy:*

(a) adopt a "deny all" access control policy for users by default unless explicitly authorised;
(b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;
(c) employ time-bound access rights which restrict access to a specific period including access rights granted to service providers;
(d) employ segregation of incompatible functions where no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features.This may include a combination of functions such as:
(i) system development and technology operations;
(ii) security administration and system administration; and
(iii) network operation and network security;
(e) employ dual control functions which require two or more persons to execute an activity;
(f) adopt stronger authentication for critical activities including for remote access;
(g) limit and control the use of the same user ID for multiple concurrent sessions;
(h) limit and control the sharing of user ID and passwords across multipleusers; and
(i) control the use of generic user ID naming conventions in favour of more personally identifiable IDs.

Customers are responsible for implementing appropriate access control policies and procedures in their environment.

However, OCI has implemented controls to help ensure that access to the infrastructure is limited to authorized individuals.

Access to infrastructure and services that support the system requires MFA, a VPN connection, and an SSH connection with a user account and password or private key. OCI account creation, access approval, access granting, and access review are based on the principles of least privilege, need to know, and segregation of duties.

Customers can use the following OCI services and features to help implement access management capabilities:

- **Identity and Access Management (IAM)** lets customers control who has access to their cloud resources. Customers can control what type of access a group of users have and to which specific resources. Customers can write policies to control access to all the services within OCI. IAM supports MFA and identity federation with Security Assertion Markup Language (SAML) based identity providers, which can be configured by customers for additional security. Also, the customer's service environment has the ability to define password complexity and lockout requirements. Customers should protect their cloud access credentials and set up individual user accounts. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.
- **Vault** is a managed service that helps customers centrally manage encryption keys that protect their data and the secret credentials that they use to securely access resources. Vaults securely store master encryption keys and secrets that might otherwise be stored in configuration files or in code. Specifically, depending on the protection mode, keys are either stored on the server or on highly available and durable HSMs that meet FIPS 140-2 Security Level 3 security certification. For more information, see docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm

10.56 *A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate.*

Customers are solely responsible for managing the authentication process in their environment.

OCI offers the following features and services that might help customers meet their identity and access management requirements:

- **Identity and Access Management (IAM)** provides authentication and authorization for all OCI resources and services, enabling customers to control who has access to their cloud resources. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.
- **Compartments** enables customers to create and manage compartments in their tenancy to organize cloud resources and the data that they contain so that only specific groups can access them. For more information, see docs.oracle.com/iaas/Content/Identity/Tasks/managingcompartments.htm.

Additionally, 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 is dependent on successful authentication, since controlling access to specific resources depends upon 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: Does the user require this access for their job function?
- Segregation of duties: Will the access result in a conflict of interest?
- Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?

Access to the infrastructure and services that support the system requires MFA, a VPN connection, and an SSH connection with a user account and a password or private key.

Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony, and physical access.

Conclusion

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