ORACLE

Advisory: Oracle Cloud Infrastructure and the Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework

Description of Oracle Cloud Infrastructure (OCI) Practices and Capabilities in the Context of the SAMA Cyber Security Framework Version 1.0

February 2023, version 2.0

Public

Disclaimer

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

This document is for informational purposes only and is intended solely to assist you in assessing your use of Oracle Cloud Infrastructure in the context of the requirements applicable to you under the SAMA Cyber Security Framework. This document might also help you to assess Oracle as a cloud 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 upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

The SAMA Cyber Security Framework is subject to periodic changes or revisions by the Saudi Arabian Monetary Authority. The current version of the SAMA Cyber Security Framework is available at sama.gov.sa/en-US/RulesInstructions/Pages/Cybersecurity.aspx.

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

Revision History

The following revisions have been made to this document.

DATE	REVISION
February 2023	Updated
December 2019	Initial publication

Table of Contents

Introduction

The Saudi Arabian Monetary Authority (SAMA) is the central bank of the Kingdom of Saudi Arabia and the supervisory authority for banks, payment providers, insurance companies, finance companies, and credit bureaus operating within the Kingdom. SAMA has established a Cyber Security Framework to enable SAMA-regulated financial institutions to effectively identify and address risks related to cyber security. For more information, see sama.gov.sa/en-US/RulesInstructions/Pages/Cybersecurity.aspx.

Document Purpose

This document is intended to provide relevant information related to Oracle Cloud Infrastructure (OCI) to assist you in determining the suitability of using OCI in relation to the SAMA Cyber Security Framework. You may read it in conjunction with the Oracle Contract Checklist for Saudi Arabian Monetary Authority Rules on Outsourcing.

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 regarding their specific legal and regulatory requirements.

About Oracle Cloud Infrastructure

Oracle's mission is to help people see data in new ways, discover insights, and unlock endless possibilities. Oracle provides several cloud solutions tailored to customers' needs. These cloud solutions provide customers the benefits of the cloud, including global, secure, and high-performance environments in which to run all their workloads. The cloud solutions discussed in this document are OCI infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) products.

OCI is a set of complementary cloud services that enable customers to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance compute capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from an on-premises network. OCI delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI, see docs.oracle.com/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 Oracle's secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle Cloud 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 a high level.

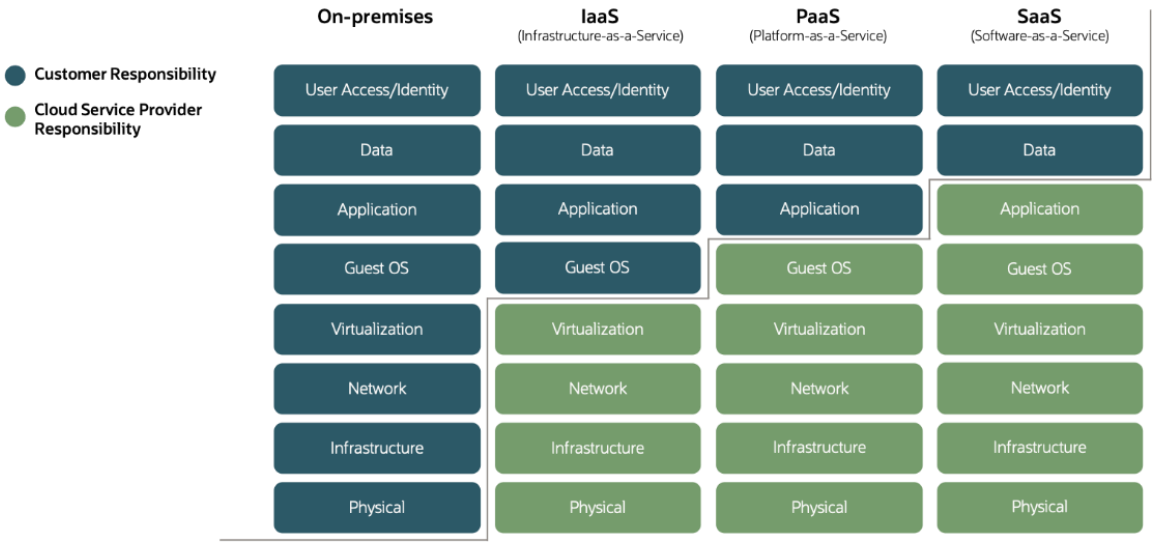

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Provider

Summary of the SAMA Cyber Security Framework

The SAMA Cyber Security Framework consists of four main control domains:

- Cyber Security Leadership and Governance
- Cyber Security Risk Management and Compliance
- Cyber Security Operations and Technology
- Third Party Cyber Security

This section provides an overview of select topics from the *Cyber Security Operations and Technology* and *Third Party Cyber Security* domains that financial institutions regulated by SAMA (the "Member Organizations") should consider in the context of cloud computing. Customers are solely responsible for determining the suitability of cloud infrastructure in the context of the SAMA Cyber Security Framework. The Oracle practices and resources provided here might assist in the evaluation of OCI within the shared management model.

The complete SAMA Cyber Security Framework v1.0 is available at sama.gov.sa/en-US/RulesInstructions/Pages/Cybersecurity.aspx.

3.3 Cyber Security Operations and Technology

This section provides an overview of select topics from the *Cyber Security Operations and Technology* control domain.

3.3.1 Human Resources

"The Member Organization should incorporate cyber security requirements into human resources processes."

Member Organizations are solely responsible for incorporating these cyber security requirements into their human resources processes.

Oracle has implemented its own policies, practices, and controls to ensure appropriate oversight of human resources processes. Oracle has ongoing initiatives intended to help minimize risks associated with human error, theft, fraud,

and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.

Oracle employees are required to maintain the confidentiality of customer data. All employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment.

OCI employees are required to complete Security Awareness Training when hired and annually thereafter. The training instructs employees on their obligations under Oracle privacy and security policies, data-privacy principles and data-handling practices that might apply to employees' jobs at Oracle and are required by company policy.

For more information, see Human Resources Security at oracle.com/corporate/security-practices/corporate/human-resources-security.html.

3.3.2 Physical Security

"The Member Organization should ensure all facilities which host information assets are physically protected against intentional and unintentional security events."

Member Organizations are solely responsible for ensuring the physical security of their facilities and information assets.

Oracle provides secured computing facilities for its office locations and cloud infrastructure data centers. Oracle Cloud 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. This evaluation 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.

Oracle Cloud data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow an N2 redundancy methodology for critical equipment operation. Data centers that house OCI services use redundant power sources and maintain generator backups in case a widespread electrical outage occurs. 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 might arise.

The Supplier Co-Location Security Standard details additional requirements for Oracle Cloud colocation providers, including, but not limited to, physical entry controls, CCTV monitoring, and environmental protections.

For more information about Oracle Physical and Environmental Security, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.

3.3.3 Asset Management

"The Member Organization should define, approve, implement, communicate and monitor an asset management process, which supports an accurate, up-to-date and unified asset register"

Member Organizations are solely responsible for implementing and monitoring an asset management program within their environment.

OCI offers several features and services that customers can use to manage their cloud resources:

- **Resource Manager** enables customers to automate the process of provisioning their OCI resources. For more information, see docs.oracle.com/iaas/Content/ResourceManager/Concepts/resourcemanager.htm.
- **Tagging** lets customers add metadata to resources by defining keys and values and associating them with resources. Customers can use the tags to organize and list resources based on business needs. For more information, see docs.oracle.com/iaas/Content/Tagging/Concepts/taggingoverview.htm.

Additionally, the Oracle Information Systems Asset Inventory Policy requires that lines of business, including OCI, maintain accurate and comprehensive inventories of information systems, hardware, and software. This policy applies to all information assets held on any Oracle system, including enterprise systems and cloud services. Oracle policy specifies the data (or fields) that must be maintained about these information systems in the approved system inventory.

The Cloud Compliance Standard for Asset Management defines the process for monitoring and maintaining OCI assets. This process includes asset registration, classification, handling, lifecycle management, controlled maintenance, retirement and removal, and roles and responsibilities.

3.3.4 Cyber Security Architecture

"The Member Organization should define, follow and review the cyber security architecture, which outlines the cyber security requirements in the enterprise architecture and addresses the design principles for developing cyber security capabilities."

Member Organizations are solely responsible for defining and maintaining their own cyber security architecture and network documentation.

Oracle's Corporate Security Architecture organization helps set the technical direction of internal information security. It also guides Oracle's IT departments and lines of business towards deploying information security and identity management solutions that advance Oracle's information security goals. Corporate Security Architecture manages a variety of programs and uses multiple methods of engaging with leadership and operational security teams responsible for Oracle operations, services, cloud, and all other lines of business.

Following are some examples of the programs for managing the security of Oracle's architecture:

- **Corporate Security Solution Assurance Process (CSSAP)** helps to accelerate the delivery of innovative cloud solutions and corporate applications by requiring appropriate reviews to be done throughout the project lifecycle.
- **Oracle Cloud Program** is a cross-organization working group focused on security architecture, with the goal of collaboratively guiding security for Oracle Cloud services. Participation includes members from Oracle Cloud service development, operations, and governance teams.
- **Oracle Software Security Assurance (OSSA)** is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers or delivered through Oracle Cloud. Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience.

For more information about the Oracle Corporate Security Program, see oracle.com/corporate/security-practices/corporate/governance.html.

3.3.5 Identity and Access Management

"The Member Organization should restrict access to its information assets in line with their business requirements based on the need-to-have or need-to-know principles."

Member Organizations are solely responsible for managing access to the information assets 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 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 supporting the system requires multifactor authentication, 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 to validate 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.

3.3.6 Application Security

"The Member Organization should define, approve and implement cyber security standards for application systems. The compliance with these standards should be monitored and the effectiveness of these controls should be measured and periodically evaluated."

Member Organizations are solely responsible for implementing and maintaining cyber security standards for the applications that they develop and run on OCI.

The Oracle Software Security Assurance (OSSA) program is Oracle's methodology for building security into the design, build, testing, and maintenance of Oracle products, whether they are used on-premises by customers or delivered through Oracle Cloud.

For more information, see oracle.com/corporate/security-practices/assurance/.

3.3.7 Change Management

"The Member Organization should define, approve and implement a change management process that controls all changes to information assets. The compliance with the process should be monitored and the effectiveness should be measured and periodically evaluated."

Member Organizations are responsible for implementing a change management process that controls changes to information assets in their environment.

The Oracle Cloud Change Management Policy is detailed in the Oracle Cloud Hosting and Delivery Policies. Changes to infrastructure configurations and services that support the system follow the Cloud Compliance Standard for Change Management. This standard documents the procedure and requirements for changes to infrastructure configurations and services. All change requests are documented in an electronic, access-controlled ticketing system. A workflow and mandatory fields are implemented in the ticketing system to help ensure compliance with change management requirements. Fields include, but are not limited to, impacted systems, impact of the change, test plans, rollback plan, and postimplementation verification. OCI achieves segregation of duties by ensuring that change development and peer reviews are performed by separate and appropriate personnel.

The Cloud Compliance Standard for Change Management is reviewed annually, at a minimum, and outlines the processes and procedures to be followed for each change.

3.3.8 Infrastructure Security

"The Member Organization should define, approve and implement cyber security standards for their infrastructure components. The compliance with these standards should be monitored and the effectiveness should be measured and periodically evaluated."

Member Organizations are responsible for implementing cyber security standards for their infrastructure components.

OCI offers several security services that might help customers meet their infrastructure security requirements:

- **Cloud Guard** enables customers to monitor their OCI resources for security weakness related to configuration, and to examine operators and users for risky activities. Upon detection, Cloud Guard suggests corrective actions, and can be configured to automatically take certain actions. 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.
- **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/Security/Concepts/security_features.htm#security_features_topic-Threat_Intel.
- **Web Application Firewall (WAF)** is a cloud-based security service that protects applications from malicious and unwanted internet traffic. WAF can protect any internet-facing endpoint, providing consistent rule enforcement across applications. For more information, see docs.oracle.com/iaas/Content/Security/Concepts/security_features.htm#web_application_firewall.

Additionally, Oracle's Corporate Security Program takes a holistic approach to information security by implementing a multilayered defense security strategy in which network, operating system, database, and software security practices and procedures complement one another with strong internal controls, governance, and oversight. For more information, see the Oracle Corporate Security Practices at oracle.com/corporate/security-practices/corporate/.

OCI operates under policies that are generally aligned with the ISO/IEC 27002 Code of Practice for information security controls. OCI's internal controls are subject to periodic testing by independent third-party audit organizations. For a complete list of OCI compliance attestations, see oracle.com/corporate/cloud-compliance/.

3.3.9 Cryptography

"The use of cryptographic solutions within the Member Organizations should be defined, approved and implemented."

Member Organizations are responsible for implementing cryptographic solutions to meet their objectives.

The following OCI services enable at-rest data encryption by default, by using the Advanced Encryption Standard (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 via encryption, and the Cloud Compliance Standard for Encryption establishes appropriate encryption methods to protect the confidentiality, integrity, and availability of customer-owned data.

3.3.10 Bring Your Own Device (BYOD)

"When the Member Organization allows the use of personal devices (e.g., smartphones, tablets, laptops) for business purposes, the use should be supported by a defined, approved and implemented cyber security standard, additional staff agreements and a cyber security awareness training."

Member Organizations are solely responsible for implementing a cyber security standard for their staff's use of personal devices for business purposes.

Oracle has a mobile-device management program and associated solutions for protecting data on employee-owned mobile devices. These solutions support all common mobile-device operating systems and platforms. Oracle IT and corporate security organizations regularly promote awareness of mobile-device security and good practice. For more information about Oracle's Endpoint Device Security Policy, see oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html.

Additionally, the Oracle Cloud Hosting and Delivery Policies prohibits (through both policy and technical controls) the use of personal devices to access the Oracle Cloud Network and the services environment for the Oracle Cloud services.

3.3.11 Secure Disposal of Information Assets

"The information assets of the Member Organization should be securely disposed when the information assets are no longer required."

Member Organizations are responsible for securely disposing of information assets in their environment.

Oracle's Information Protection Policy and Media Sanitation and Disposal Policy define requirements for 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. All excess, obsolete, and nonperforming equipment must be disposed of through an approved Oracle asset disposal process.

OCI tracks and authorizes all equipment, information, and software that enters OCI facilities and data halls. Media is prohibited from being removed from a data hall without prior authorization or before the destruction process is complete.

OCI instances are securely wiped after customers release the hardware. This secure wipe restores hardware to a pristine state. When the underlying hardware has reached end-of-life, the hardware is securely destroyed. Before leaving data centers, drives are rendered unusable by using industry-leading media destruction devices.

3.3.14 Cyber Security Event Management

"The Member Organization should define, approve and implement a security event management process to analyze operational and security loggings and respond to security events. The effectiveness of this process should be measured and periodically evaluated."

Member Organizations are solely responsible for implementing a security event management process in their environment. Member Organizations are also responsible for monitoring their tenancies for indicators of compromise and responding to security events in their environment.

OCI offers security services, including the following ones, which might help customers meet their event management requirements:

- **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/Security/Concepts/security_features.htm#security_features_topic-Threat_Intel.
- **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.

Additionally, Oracle evaluates and responds to events that create suspicion of unauthorized access to or handling of customer data, whether the data is held on Oracle hardware assets or on the personal hardware assets of Oracle employees and contingent workers. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to incidents. This policy authorizes the Oracle Global Information Security (GIS) organization to serve as the primary contact for security incident response, as well as to provide overall direction for incident prevention, identification, investigation, and resolution.

Upon discovery of an incident, Oracle defines an incident response plan for rapid and effective incident investigation, response, and recovery, and promptly notifies any impacted customers in accordance with its contractual and regulatory responsibilities. OCI service teams maintain and continuously evaluate their resiliency plan for operations to meet the need of critical system operations in the event of a disruption. OCI exercises service resiliency plans no less than annually.

3.3.15 Cyber Security Incident Management

"The Member Organization should define, approve and implement a cyber security incident management that is aligned with the enterprise incident management process, to identify, respond to and recover from cyber security incidents. The effectiveness of this process should be measured and periodically evaluated."

Member Organizations are solely responsible for monitoring their instances for security incidents.

Oracle evaluates and responds to security incidents when Oracle suspects that Oracle-managed customer data has been improperly handled or accessed. The Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to such security incidents. Upon discovery of a security incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures to improve security posture and defense in depth.

Security incidents affecting OCI are assigned a severity level and tracked to resolution by the Detection and Response Team (DART). OCI has a comprehensive Corrective Action/Preventive Action (CAPA) incident follow-up and reporting procedure for Severity 1 incidents. For information about severity definitions, see the Oracle Cloud Hosting and Delivery Policy.

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

3.3.16 Threat Management

"The Member Organization should define, approve and implement a threat intelligence management process to identify, assess and understand threats to the Member Organization information assets, using multiple reliable sources. The effectiveness of this process should be measured and periodically evaluated."

Member Organizations are responsible for implementing a threat-intelligence management strategy for the information assets in their environment.

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 uses 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, including 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.

3.3.17 Vulnerability Management

"The Member Organization should define, approve and implement a vulnerability management process for the identification and mitigation of application and infrastructural vulnerabilities. The effectiveness of this process should be measured and the effectiveness should be periodically evaluated."

Member Organizations are solely responsible for implementing vulnerability management processes in their environment.

OCI offers the following service that might help customers implement effective vulnerability management processes in their environment:

- **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 regularly performs penetration testing and security assessments against cloud infrastructure, platforms, and applications to validate and improve the overall security of Oracle Cloud services. An independent third party conducts a penetration test of OCI at least annually. A commercial vulnerability scanning tool scans external IP addresses and internal nodes weekly, and after significant project launches or major network changes. Identified threats and vulnerabilities are investigated and tracked to resolution.

For more information about OCI's security testing policy, see docs.oracle.com/iaas/Content/Security/Concepts/security_testing-policy.htm.

3.4 Third Party Cyber Security

This section provides an overview of select topics from the *Third Party Cyber Security* control domain.

3.4.1 Contract and Vendor Management

"The Member Organization should define, approve, implement and monitor the required cyber security controls within the contract and vendor management processes."

The required rights and obligations of each party are documented in a written contract. For more information, see the Oracle Cloud Service contracts at oracle.com/corporate/contracts/cloud-services/contracts.html.

Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. For more information about Oracle Supply Chain Security and Assurance, see oracle.com/corporate/security-practices/corporate/supply-chain/.

3.4.2 Outsourcing

"The Member Organization should define, implement and monitor the required cyber security controls within outsourcing policy and outsourcing process. The effectiveness of the defined cyber security controls should periodically be measured and evaluated."

Oracle offers several resources to assist its customers in evaluating and monitoring the effectiveness of OCI security controls, including independent third-party audit reports and certifications, and supporting documentation. In addition, as required by applicable law or regulation, Oracle provides customers and their regulators with necessary information (including summaries of reports and documents) regarding the activities outsourced to Oracle.

The following resources might assist customers in their assessment of OCI in the context of applicable cyber security requirements:

- **Oracle Cloud Compliance:** oracle.com/corporate/cloud-compliance/
- **Oracle Corporate Security Practices:** oracle.com/corporate/security-practices/corporate/
- **Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Infrastructure:** oracle.com/a/ocom/docs/oci-corporate-caiq.pdf
- **SAMA Rules on Outsourcing Contract Checklist:** Oracle provides a detailed contract checklist to help customers identify the sections of the Oracle Cloud services contract that pertain to the requirements in the SAMA circular on outsourcing. See oracle.com/a/ocom/docs/contract-checklist-sama-rules-on-outsourcing.pdf.

3.4.3 Cloud Computing

"The Member Organization should define, implement and monitor the required cyber security controls within the cloud computing policy and process for hybrid and public cloud services. The effectiveness of the defined cyber security controls should periodically be measured and evaluated."

Member Organizations are responsible for implementing and monitoring the effectiveness of cyber security controls within their environment and ensuring that all functions and staff within the Member Organization are aware of the required processes for public cloud services.

When using OCI, customers are responsible for establishing a geographic location (region) in which to locate their tenancy. A customer's data stays within this region unless the customer chooses to move data outside the region. OCI offers powerful cloud services that might operate across tenancies or regions. Through the OCI Console and API, customers are informed when their actions might cause data to move to another tenancy or region. Each OCI tenancy is logically isolated from other tenants on the network level to ensure confidentiality and integrity of data transmitted.

Oracle has also implemented security controls to protect the confidentiality, integrity, and availability of customer applications and data running on OCI. These controls are examined and tested regularly by independent third-party assessors, and attestation reports and certifications are made available to customers via the Oracle Cloud Console through the Compliance Documents service.

To help customers meet their monitoring and oversight obligations, Oracle provides the Oracle Cloud Observability and Management Platform, which is a comprehensive set of management, diagnostic, and analytics services that help customers manage their OCI tenancy while reducing troubleshooting time, reducing likelihood of outages, and enabling IT to manage applications. The platform provides visibility across applications by using advanced analytics to automatically detect anomalies and enable quick remediation in near-real time. The platform includes services such as Logging, Monitoring, Notifications, Database Management, and Application Performance Monitoring.

Additionally, Oracle deploys its cloud services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services. Data centers retained by Oracle to host OCI services have component and power redundancy with backup generators in place, and Oracle may incorporate redundancy in one or more layers, including network infrastructure, program servers, database servers, and storage.

Oracle Cloud Service contracts describe the rights and obligations of each party, including but not limited to data use limitations, audit rights, and termination rights. For more information, see the Oracle Cloud Service contracts at oracle.com/corporate/contracts/cloud-services/contracts.html.

Conclusion

Oracle is committed to helping customers become more agile, operate in a dynamic global business environment, and meet their obligations under the SAMA Cyber Security Framework. OCI services and capabilities can accelerate innovation for financial organizations operating in the Kingdom of Saudi Arabia.