ORACLE

# Advisory: Oracle Cloud Applications and the Monetary Authority of Singapore Cyber Hygiene Requirements Notice 655

Description of Oracle Cloud Applications (SaaS) in the Context of the Monetary Authority of Singapore Cyber Hygiene Notice 655

February 2022, Version 2.0

Public

## Disclaimer

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

This document is for informational purposes only and is intended solely to assist you assessing your use of Oracle Cloud Applications (SaaS) in the context of the requirements applicable to you under the MAS Cyber Hygiene Requirements Notice 655. This may also help you to assess Oracle as an outsourced service provider. You remain responsible for performing your own independent assessment of the information in this document as the information in this document is not intended and may not be used as legal advice about the content, interpretation or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

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

The MAS Cyber Hygiene Requirements Notice 655 is subject to periodic changes or revisions by the Monetary Authority of Singapore. The current version of the MAS Cyber Hygiene Requirements Notice 655 is available at: Monetary Authority of Singapore Notice on Cyber Hygiene.

This document is based upon information available at the time of drafting, it is subject to change at the sole discretion of Oracle Corporation and may not always reflect changes in the regulations.

## Table of Contents

## Introduction

The Monetary Authority of Singapore (MAS), created with the passing of the MAS Act in 1970, is Singapore's central bank and integrated financial regulator. MAS has provided a list of guidelines applicable to financial institutions operating in Singapore with regards to risk management, cyber security, and IT outsourcing. For more information, see https://www.mas.gov.sg/regulation/regulations-and-guidance.

## Document Purpose

This document is intended to provide relevant information related to Oracle Cloud Applications to assist you in determining the suitability of using Oracle Cloud Applications in relation to the MAS Cyber Hygiene Requirements Notice 655.

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 Applications (SaaS)

Oracle's mission is to help people see data in new ways, discover insights, unlock endless possibilities. Oracle provides a number of cloud solutions tailored to customers' needs. These cloud offerings provide customers the benefits of the cloud including global, secure, and high-performance environments to run all their workloads. The cloud offerings discussed in this document include Oracle Cloud Applications (SaaS)[1].

Oracle offers a complete cloud suite of SaaS applications which brings consistent processes and a single source of truth across the most important business functions. By delivering a modern user experience and continuous innovation, Oracle is committed to the success of your organization with continuous updates and innovations across the entire business: finance, human resources, supply chain, manufacturing, advertising, sales, customer service, and marketing. For more information on Oracle Cloud Applications, see https://www.oracle.com/applications.

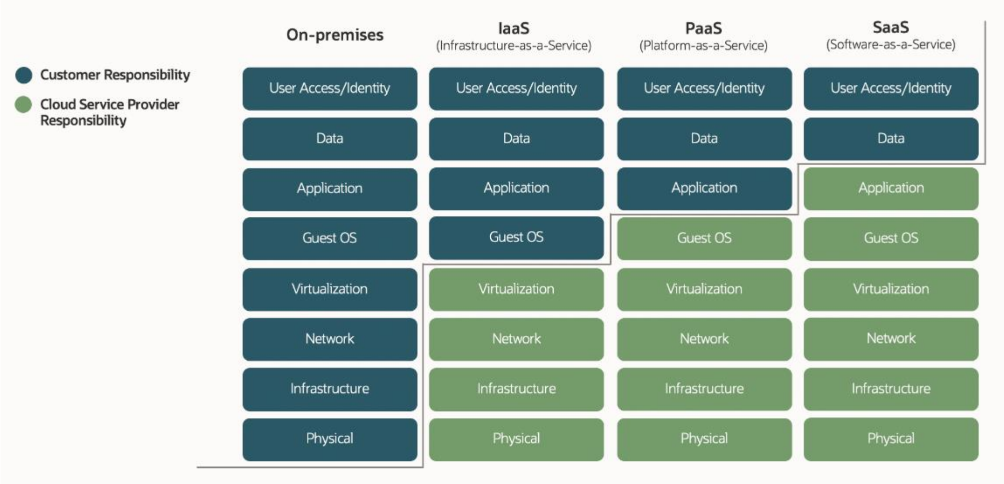
## The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different to 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 (e.g., cloud operator access controls, infrastructure security patching, etc.), and customers are responsible for securely configuring and using their cloud resources. For more information, please refer to the cloud service documentation.

[1] Note that Oracle GBU SaaS, NetSuite and Advertising SaaS Services are not included in the scope of this document.

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



🟦 Customer Responsibility<br>
🟩 Cloud Service Provider Responsibility

| On-premises | IaaS (Infrastructure-as-a-Service) | PaaS (Platform-as-a-Service) | SaaS (Software-as-a-Service) |
|---|---|---|---|
| 🟦 User Access/Identity | 🟦 User Access/Identity | 🟦 User Access/Identity | 🟦 User Access/Identity |
| 🟦 Data | 🟦 Data | 🟦 Data | 🟦 Data |
| 🟦 Application | 🟦 Application | 🟦 Application | 🟩 Application |
| 🟦 Guest OS | 🟦 Guest OS | 🟩 Guest OS | 🟩 Guest OS |
| 🟦 Virtualization | 🟩 Virtualization | 🟩 Virtualization | 🟩 Virtualization |
| 🟦 Network | 🟩 Network | 🟩 Network | 🟩 Network |
| 🟦 Infrastructure | 🟩 Infrastructure | 🟩 Infrastructure | 🟩 Infrastructure |
| 🟦 Physical | 🟩 Physical | 🟩 Physical | 🟩 Physical |

Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers

## MAS Cyber Hygiene Requirements Notice 655

This section provides an overview of the key regulatory considerations specified by the MAS Cyber Hygiene Requirements Notice 655 that regulated customers should consider.

| TOPIC REFERENCE | COMPLIANCE REQUIREMENTS | DESCRIPTION OF ORACLE PRACTICES | ORACLE RESOURCES |
|---|---|---|---|
| **4.1 Administrative Accounts** | | | |
| | A relevant entity must ensure that every administrative account in respect of any operating system, database, application, security appliance or network device, is secured to prevent any unauthorised access to or use of such account. | Oracle  prioritizes protecting the integrity and security of products and services. Oracle cloud services are designed and operated following a defense-in-depth model. This model starts with a default-deny network-oriented approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination. As a result, tenants are isolated from one another and from Oracle.<br>Access controls are implemented to govern access to and use of resources. Examples of resources include a physical server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol. These controls include following a least-privilege model designed as a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.<br>Oracle user access is provisioned through an account-provisioning system that is integrated with Oracle's Human Resources database. | Oracle Access Control practices:<br>https://www.oracle.com/corporate/security-practices/corporate/access-control.html<br>Oracle Identity Access Management product:<br>https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm |

| | | | |
|---|---|---|---|
| | | Access privileges are granted based on job roles and require management approval.<br>Additionally, all Oracle authorization decisions for granting, approval, and review of access are based on the following principles:<br>• Need to know: Does the user require this access for his job function?<br>• Segregation of duties: Will the access result in a conflict of interest?<br>• Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose? | |
| **4.2 Security Practices** | | | |
| (a) | A relevant entity must ensure that security patches are applied to address vulnerabilities to every system and apply such security patches within a timeframe that is commensurate with the risks posed by each vulnerability. | Oracle SaaS has a robust patch management solution that ensures vulnerabilities are evaluated, and patches are deployed across the environment based upon criticality. Oracle SaaS vulnerability severity is assessed based upon Common Vulnerability Scoring System (CVSS) scoring, and remediation SLAs timelines are based upon the assigned severity and possible business impact. | Oracle Cloud Applications CAIQ:<br>https://www.oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf |
| (b) | Where no security patch is available to address a vulnerability, the relevant entity must ensure that controls are instituted to reduce any risk posed by such vulnerability to such a system. | In order to provide the best security posture to all Oracle customers, Oracle addresses security vulnerabilities based on the likely risk they posed to customers. As a result, the issues with the most severe risks are fixed first.<br>Oracle institutes additional mitigating controls based on specific system type and risk exposure. Additionally Oracle regularly performs risk assessments to confirm that the correct and effective mitigation controls are in place and maintained in order to reduce the effect of any risk. | Oracle Cloud Applications CAIQ:<br>https://www.oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf |
| **4.3 Security Standards** | | | |

| | | | |
|---|---|---|---|
| (a) | A relevant entity must ensure that there is a written set of security standards for every system. | 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. To ensure that Oracle products are developed with consistently high security assurance, and to help developers avoid common coding mistakes, Oracle employs formal secure coding standards, additionally:<br>• Oracle Cloud Services operates under practices which are aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which a comprehensive set of controls are selected. Oracle Cloud Services are aligned with National Institute of Standards and Technology ("NIST") 800-53 and 800-171.<br>• Oracle's enterprise architecture organization defines and maintains guidance documentation and secured configurations for use within Oracle's corporate systems and in Oracle cloud. This guidance applies across layers of Oracle environments, including hardware, storage, operating systems, databases, middleware, and applications.<br>• 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 Cloud Applications CAIQ:<br>https://www.oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf<br>Oracle Software Security Assurance:<br>https://www.oracle.com/corporate/security-practices/assurance/<br>Oracle Hosting & Delivery Policy:<br>https://www.oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf |
| (b) | Subject to sub-paragraph (c), a relevant entity must ensure that every system conforms to the set of security standards. | Oracle Cloud Applications (SaaS) use approved systems for managing access and integrity of device configurations. Change controls are in place to ensure only approved changes are applied. Regular audits are performed to confirm compliance with security and operational procedures. Also, internal scans are performed on the infrastructure to ensure compliance against information security baselines and standards. | Oracle Cloud Applications CAIQ:<br>https://www.oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf |
| (c) | Where the system is unable to conform to the set of security standards, the relevant entity must ensure that | Oracle has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets. Additionally, Oracle regularly performs risk assessments to confirm that the correct and effective | Oracle Cloud Applications CAIQ:<br>https://www.oracle.com/a/ocom/docs/caiq- |

| | | | |
|---|---|---|---|
| | controls are instituted to reduce any risk posed by such non-conformity. | mitigation controls are in place and maintained in order to reduce the effect of identified risk. | oracle-cloud-applications.pdf |
| **4.4 Network Perimeter Defense** | | | |
| | A relevant entity must implement controls at its network perimeter to restrict all unauthorised network traffic. | To enable deep packet inspection by Oracle SaaS Intrusion Detection Systems (IDS), inbound network traffic is decrypted at the load balancers.<br>IDS sensors are deployed to monitor suspicious network traffic. IDS alerts are routed to a centralized monitoring system that is managed by the security operations teams 24x7x365. | Oracle Cloud Applications CAIQ:<br>https://www.oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf |
| **4.5 Malware Protection** | | | |
| | A relevant entity must ensure that one or more malware protection measures are implemented on every system, to mitigate the risk of malware infection, where such malware protection measures are available and can be implemented. | Oracle Cloud Applications (SaaS) deploy security detection systems, including the Network Intrusion Detection Systems (IDS), anti-malware, and D-DoS system configured to auto-update at least weekly.<br>Oracle Cloud Applications (SaaS) Support and Operations Staff, along with all Oracle employees and contractors who provide cloud support, are required to use company approved laptop or desktop computers that have been equipped with additional controls that include antivirus and malware protection. | Oracle Cloud Applications CAIQ:<br>https://www.oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf |
| **4.6 Multi-factor Authentication** | | | |
| | A relevant entity must ensure that multi-factor authentication is implemented for the following: | [redacted] | [redacted] |
| (a) | All administrative accounts in respect of any operating system, database, application, security appliance or network device that is a critical system; and | Oracle Cloud Applications (SaaS) has policies and procedures with established security controls in support of multi-factor authentication (MFA) for administrative accounts. Two factors work together to verify the user's identity and complete the sign-in process. | Oracle Cloud Applications CAIQ:<br>https://www.oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf |
| (b) | All accounts on any system used by the relevant entity to | Oracle Cloud Applications (SaaS) has policies and procedures with established security controls that leverage multi-factor | Oracle Cloud Applications CAIQ: |

| | | | |
|---|---|---|---|
| | access customer information through the internet. | authentication (MFA) for accounts that access customer information over the internet.<br>Multifactor authentication can be achieved through a subscription to Identity Cloud Service (IDCS), which supports multi-factor authentication using third-party providers for multi-factor authentication and password-less authentication (i.e., FIDO or YubiKey). Customers have the option of subscribing to Identity Cloud Service (IDCS) and may also pass their multi-factor verified credentials through standard federation and SAML. Customers are responsible for their end user accounts. | https://www.oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf |

## Conclusion

Oracle enables customers to become more agile, collaborative, and insightful while striving to support them in meeting their own obligations under the MAS Cyber Hygiene Requirements Notice 655. Oracle Cloud Applications (SaaS) can accelerate innovation for financial institutions operating in Singapore.

Connect with us

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

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