Advisory: Oracle Cloud Applications (SaaS) and APRA Prudential Standards CPS 231 and CPS 234

February 2024, Version 1.0

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.

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation, or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their use of Oracle services.

This document is for informational purposes only and is intended solely to assist you in assessing your use of Oracle Cloud Applications (SaaS) services and reviewing your Oracle Cloud services contract and its incorporated documents. Please also note that the relevant contract(s) between you and Oracle determine(s) the scope of services provided and the related legal terms. The entire Agreement and your order must be read to understand all applicable contractual terms.

Accordingly, this document is not part of, and does not otherwise create or amend, any agreement, warranties, representations or other obligations between you and Oracle.

Oracle contracts are updated from time to time, and you are responsible for checking any information provided herein against your specific Oracle contract. Oracle disclaims all liability arising out of your use of this document including but not limited to any terms or statements contained herein that seek to impose legal or operational requirements on Oracle for the delivery of the services. Customers acknowledge that they remain solely responsible for reviewing and assessing their contracts and meeting their legal and regulatory requirements.

The Australian Prudential Regulatory Authority (APRA) Cross-Industry Prudential Standards (CPS) referenced in this document are subject to periodic changes or revisions by APRA. The current versions of the standards referenced in this document are available through the links listed below. This document is based on information available at the time of creation, it is subject to change at the sole discretion of Oracle Corporation and may not always reflect changes in the regulations.

- CPS 234: https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
- CPS 231: https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

Table of Contents

Introduction

The Australian Prudential Regulation Authority (APRA) is the prudential regulator of financial services in Australia. APRA is responsible for issuing standards that regulate the operations of banks, credit unions, and insurance companies that operate business in Australia.

While Oracle is not an APRA regulated entity, it recognizes that some of its customers operating in Australia may be required to adhere to the provisions of APRA Prudential Standards CPS 234 and CPS 231.

Document Purpose

This document is intended to provide relevant information about Oracle Cloud Applications (SaaS) to assist you in determining the suitability of using Oracle Cloud Applications (SaaS), having regard to APRA Prudential Standard CPS 231 and CPS 234 requirements. This document should be read in conjunction with the Oracle Contract Checklist for the Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 231 on Outsourcing.

The information in this document applies to the following Oracle Cloud Applications (SaaS):

- Enterprise Resource Planning (ERP)
- Enterprise Performance Management (EPM)
- Supply Chain Management & Manufacturing (SCM)
- Human Capital management (HCM)

About Oracle Cloud Applications

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 customer needs. These solutions provide customers with the benefits of the cloud, including global, secure, and high-performance environments to run all their workloads. The cloud solutions discussed in this document are Oracle Cloud Applications (SaaS).

Oracle Cloud Applications (SaaS) provide a comprehensive and connected SaaS suite. By delivering a modern user experience and continuous innovation, Oracle is committed to our customers' success with continuous updates and innovation 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 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 environments. By design, Oracle provides security functions for cloud infrastructure and operations (e.g., cloud operator access controls, infrastructure security patching), and customers are responsible for securely configuring and using their cloud resources. For more information, you should refer to your cloud service documentation.

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

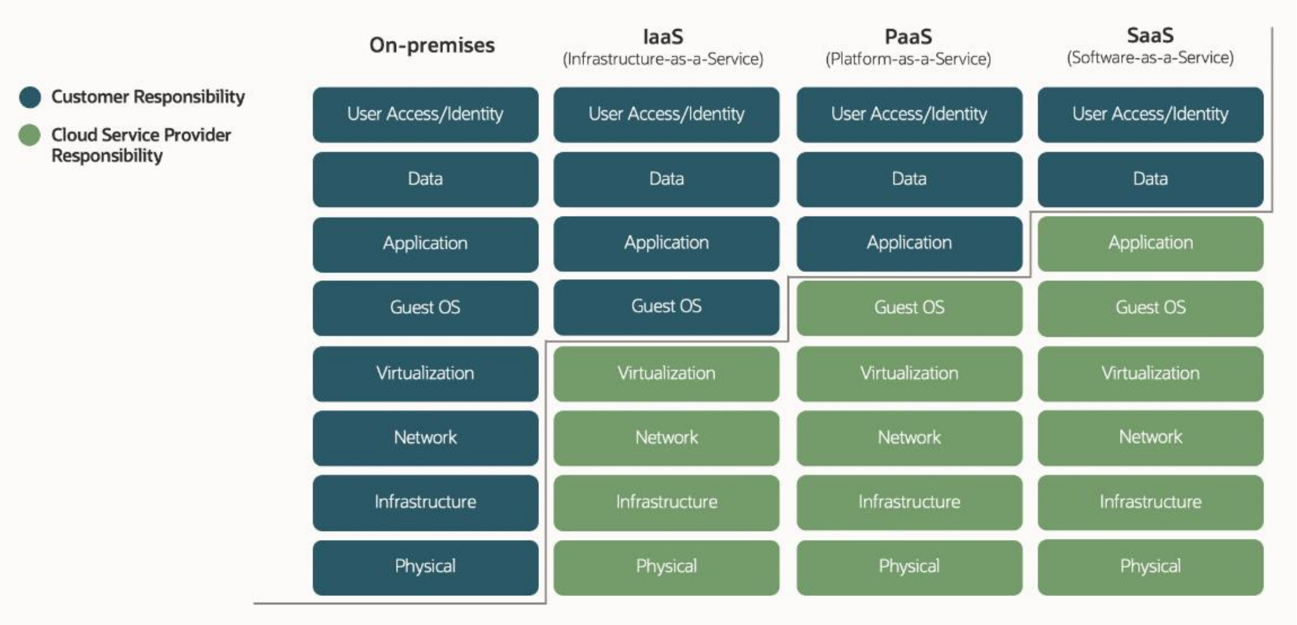

Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud service providers

Overview of APRA CPS 231 and CPS 234 requirements

This section provides an overview of select provisions of APRA Prudential Standards CPS 231 and CPS 234

Firms are responsible for determining the suitability of a cloud service in the context of all relevant requirements and their needs. They are also responsible for ensuring that their use of the cloud service and internal business processes meet these requirements. However, Oracle provides features and functions that may help organizations meet some of their requirements.

There are two parts to this section:

- Part 1 – Sets out relevant information about Oracle and Oracle Cloud Applications (as per defined scope) solutions.
- Part 2 – Addresses certain provisions of CPS 231 and CPS 234, by reference to Oracle Cloud Applications (SaaS) operational and security practices and services.

PART 1 – About Oracle and Oracle Cloud Applications

Is Oracle a regulated entity under the supervision of APRA?

No. Oracle is not under the direct supervision of APRA. However, Oracle can assist regulated customers by providing some of the information and resources that may support a regulated customer's ability to satisfy its regulatory and compliance requirements.

Does Oracle have a specific cloud contract for the financial services sector?

Yes. In addition to its comprehensive cloud hosting and delivery policies, data protection commitments, and security terms, Oracle offers the Financial Services Addendum (FSA) as an add-on to the Oracle Cloud Services Agreement (CSA) or to the Oracle Master Agreement (OMA), as applicable. The FSA addresses various topics typically requested by regulated customers in the financial services sector, including audit rights for customers and their financial services regulators, expanded termination rights, exit and transition assistance services, business continuity, and subcontracting arrangements.

What customer data will Oracle process in the context of the provision of a contracted Oracle cloud applications service?

Oracle cloud applications services typically handle two types of customer data:

- Customer account information that is needed to operate the customer's cloud account. This information is primarily used for customer account management, including billing. Oracle is a controller with regard to the use of personal information that it gathers from the customer for purposes of account management and handles such information in accordance with the terms of the Oracle General Privacy Policy.
- Customer content that customers choose to store within Oracle cloud application services, which may include personal information gathered from the customer's data subjects, such as its users, end customers, or employees.

It is important to note that Oracle does not have a direct relationship with the customer's data subjects. The customer is the controller in these situations and is responsible for data collection and data use practices. Oracle is the processor that acts on the instructions of the customer and handles personal information contained in customer content in accordance with the general processing terms of the Oracle Services Privacy Policy and the Oracle Data Processing Agreement.

Does Oracle have access to customer content?

Under the Oracle Cloud Applications (SaaS) model, authorized Oracle employees can access customer content in limited circumstances. This access is audited and logged. Oracle customers are responsible for administering their own access rights with regard to their cloud services environment.

Oracle Database Vault and Oracle Break Glass, as optional service for Oracle Fusion, provide additional security by restricting administrative access to systems and services. When a customer purchases Break Glass, Oracle Support representatives can access a customer's cloud environment only after customer approvals and relevant authorization have been obtained. For more information, see Oracle Database Vault and Break Glass for Fusion Cloud Service.

How is customer content protected against access by unauthorized third parties, including other Oracle customers?

Oracle cloud applications s are designed and operated following a defense-in-depth model. This model starts with a default-deny network-oriented configuration approach that denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source network address, and destination network address. This provides a foundation to isolate tenants from one another.

Also, access controls are implemented to govern Oracle's access to and use of resources. These controls include following a least-privilege 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. For more information, see https://www.oracle.com/corporate/security-practices/corporate/.

How does Oracle manage availability risks?

Oracle deploys its cloud services on a resilient computing infrastructure designed to maintain service availability and continuity if an adverse event affects the services. Data centres 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. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.

Oracle periodically makes backups of a customer's production data and stores such backups at the primary site used to provide the Oracle cloud services. Backups may also be stored at an alternative location for retention purposes.

For more information, see section 2 of the Oracle Cloud Hosting and Delivery Policies at oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf.

How does Oracle handle security incidents?

Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed data has been accessed by an unauthorised entity. The Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to information security events and incidents. This policy authorizes the Oracle Global Information Security (GIS) organization to provide overall direction for security event and incident preparation, detection, investigation, and resolution within Oracle's Lines of Business. In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services.

Does Oracle provide audit rights to customers and their regulators?

Yes. Customers and their financial services regulators have the right to access and audit Oracle's compliance with its obligations under their cloud services agreement as specified in the FSA. Such audit rights include the right to conduct emergency audits. In addition, Oracle grants its customers and their financial services regulators the same rights of access and audit in respect of Oracle strategic subcontractors. Such audit rights and related terms are set out in the FSA.

What compliance documentation does Oracle provide?

Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of "attestations". These attestations can assist in your compliance and reporting, providing independent assessment of the security, privacy, and compliance controls of the applicable Oracle Cloud Application. Such attestations may include CSA Star, SOC, and ISO/IEC 27001, 27017, and 27018 as applicable to the relevant Oracle Cloud Services. These attestations are generally specific to a certain cloud service and may also be specific to a certain data centre or geographic region.

Additionally, Oracle provides general information about some of the compliance frameworks listed below in the form of "advisories." These advisories are provided to help you in your determination of the suitability of using specific Oracle cloud services as well as to assist you in implementing specific technical controls that may help you address your compliance obligations.

For more information, see https://www.oracle.com/corporate/cloud-compliance/

Oracle also provides a description of its security practices for some cloud services in a Consensus Assessment Initiative Questionnaire (CAIQ). The CAIQs are publicly available at https://www.oracle.com/corporate/security-practices/cloud/, and may be used by customers to review Oracle's security practices to determine the suitability of using cloud services in light of their legal and regulatory compliance obligations.

PART 2 – Select provisions of the APRA Prudential Standards CPS 231 and CPS 234

Security Controls Implementation

Paragraph 16 of APRA CPS 234 states that "where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets." Again, paragraph 22 of CPS 234 states that "where an APRA-regulated entity's information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party's information security controls that protects the information assets of the APRA-regulated entity."

Customers are solely responsible for establishing effective information security control framework in line with their business model and risk exposures.

Oracle cloud services operate under practices which are aligned with the International Standards Organization - ISO/IEC 27002 Code of Practice for information security controls. Oracle cloud services are also aligned with ISO 27001 standards and may provide available SSAE18 SOC1/SOC2 reports issued by external third-party auditors.

Customers can obtain more information about how to access available attestations and audit reports through the cloud customer support portal or by contacting their Oracle sales representative.

For more information, see Oracle Cloud Hosting and Delivery Policies and Oracle Cloud Security Practices.

Information Security Incident Notification

Paragraph 35 of APRA CPS 234 states that "an APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident."

Customers are responsible for notifying their regulators of relevant information security incidents.

In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services.

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

Information Asset Classification

Paragraph 20 of APRA CPS 234 states that "an APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity."

Customers are responsible for establishing effective information security framework, that includes information asset classification, in line with their business model and risk exposures.

Oracle Corporate Security Practices include details on Oracle's information classification and categorization practices, and the corresponding levels of security controls that applies to each classification.

For more information, see https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification.html.

Security Control Testing

Paragraph 28 of APRA CPS 234 states that "where an APRA-regulated entity's information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, the APRA-regulated entity must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with paragraphs 27(a) to 27(e) of Prudential Standard CPS 234."

Customers are responsible for assessing Oracle's information security and controls strategy to determine its suitability with respect to their regulatory compliance obligations.

For more information, see https://www.oracle.com/corporate/security-practices/.

Outsourcing Agreement Notification

Paragraph 37 of APRA CPS 231 states that "An APRA-regulated institution must notify APRA as soon as possible after entering into an outsourcing agreement, and in any event no later than 20 business days after execution of the outsourcing agreement." Also, paragraph 38 of CPS 231 states that "when an APRA-regulated institution notifies

APRA of a new outsourcing agreement, it must also provide a summary to APRA of the key risks involved in the outsourcing arrangement and the risk mitigation strategies put in place to address these risks."

Customers are responsible for notifying their regulatory authorities where they choose to outsource services that are considered critical or important.

Oracle provides various materials through My Oracle Support (MOS) and Customer Notification Portal, that may assist customers in their correspondence with competent authorities.

Due Diligence Review

Paragraph 26 (c) of APRA CPS 231 states that "an APRA-regulated institution must be able to demonstrate to APRA that, in assessing the options for outsourcing a material business activity to a 'third party', it has undertaken a due diligence review of the chosen service provider, including the ability of the service provider to conduct the business activity on an ongoing basis."

Customers are solely responsible for conducting their own due diligence review when considering the outsourcing of services and for demonstrating such assessment to APRA.

Oracle provides several resources to assist existing and prospective customers in conducting necessary due diligence, including access to security questionnaires, audit reports, and other information about Oracle's operational and security practices.

For more information, see:

Oracle Cloud Compliance site - https://www.oracle.com/corporate/cloud-compliance/

Cloud Services Hosting and Delivery Policies – http://www.oracle.com/corporate/cloud-services-hostingand-delivery-policies

Oracle Corporate Security Practices - https://www.oracle.com/corporate/security-practices/cloud/

Consensus Assessment Initiative Questionnaire (CAIQ) https://www.oracle.com/corporate/security-practices/cloud/

Performance Monitoring

Section 26 (f) of APRA CPS 231 states that "an APRA-regulated institution must be able to demonstrate to APRA that, in assessing the options for outsourcing a material business activity to a 'third party', it has established procedures for monitoring performance under the outsourcing agreement on a continuing basis.".

Customers are solely responsible for establishing adequate procedures to monitor agreed performance levels and demonstrating such assessment to APRA.

Oracle commits to deliver the services at the agreed level of availability and offers the tool and services to support the monitoring obligations of its customers.

Customers can access metrics on the service availability for their ordered Oracle cloud services through the customer notifications portal, where available, or upon request.

For more information, see Fusion cloud application status here, https://saasstatus.oracle.com/

Contractual Agreement

Paragraph 28 of APRA CPS 231 states that "each outsourcing arrangement must be contained in a documented legally binding agreement, except where otherwise provided in this Prudential Standard. The agreement must be signed by all parties to it before the outsourcing arrangement commences."

The provision of Oracle Cloud Applications (SaaS) services and the relationship between Oracle and its financial service customers may be governed by the terms set out in the following written contractual documents:

The **Oracle Cloud Services Agreement (CSA)** covers:

- Use of the services
- Confidentiality
- Liability and Indemnification
- Governing law and jurisdiction
- Start date, term, and termination of the master agreement
- Notice period and procedures

The **Ordering Document** covers:

- Description of the cloud services
- Service-period term
- Fees
- Data centre region (for SaaS cloud services)

The Oracle **Financial Services Addendum (FSA)** covers:

- Audit rights for customers and regulators
- Additional termination rights
- Exit provisions including data retrieval, transition period, and transition services
- Business continuity
- Strategic subcontractors
- Compliance with laws applicable to Oracle's provision of services
- Assistance with regulatory obligations, including the provision of necessary information requested by the customer's competent regulator

The **Data Processing Agreement (DPA)** for Oracle Services covers key data privacy requirements for services engagements, including:

- Allocation of responsibilities between the customer and Oracle
- Assistance with handling privacy inquiries and requests from individuals
- Subprocessor management and due diligence
- Cross-border data transfers
- Security and confidentiality
- Audit rights
- Incident management and breach notification
- Return and deletion of personal information

For more information, see Oracle cloud services contracts.

Inspection and Audit

Paragraph 34 of APRA CPS 231 states that "an outsourcing agreement must include a clause that allows APRA access to documentation and information related to the outsourcing arrangement. In the normal course, APRA will seek to obtain whatever information it requires from the APRA-regulated institution; however, the outsourcing agreement must include the right for APRA to conduct on-site visits to the service provider if APRA considers this necessary in its role as prudential supervisor. APRA expects service providers to cooperate with APRA's requests for information and assistance."

Customers and their regulators have the right to access and audit Oracle's compliance with its obligations under their cloud services agreement as specified in the Financial Services Addendum (FSA).

In addition, Oracle grants its customers and their regulators the same rights of access and audit of Oracle strategic subcontractors.

Such audit rights and related terms are covered in the FSA.

Conclusion

Oracle is committed to helping customers operate globally in a fast-changing business environment and support customers evaluating their obligations under the APRA Prudential Standards CPS 231 and CPS 234. Oracle Cloud Applications (SaaS) services and capabilities provide some features that can help customers address their compliance objectives.

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