

Australian Prudential Regulation Authority (APRA) Regulated Entity and Oracle Cloud Infrastructure

Frequently Asked Questions About Australian
Prudential Regulation Authority (APRA) Regulated
Entities and Oracle Cloud Infrastructure

June 2023, version 2.0
Copyright © 2023, Oracle and/or its affiliates
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.

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. Please also note that the relevant contracts between you and Oracle determine the scope of services provided and the related legal terms, and the information provided in this document is provided as an aid to assist you in your review of your Oracle Cloud services contract. 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.

This document is for informational purposes only and is intended solely to assist you assessing your use of Oracle Cloud Infrastructure (OCI) services in the context of the requirements applicable to you under Australian Prudential Regulation Authority (APRA) Standard CPS 231 Outsourcing. You remain responsible for making your own independent assessment of the information in this document. 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.

Australian Prudential Regulation Authority's regulations and standards are subject to periodic changes or revisions by the regulator (APRA). The current version of APRA Standard CPS 231 Outsourcing is available at www.apra.gov.au.

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
June 2023	Updated
June 2020	Initial publication

Table of Contents

Introduction	4
Document Purpose	4
About Oracle Cloud Infrastructure	4
The Cloud Shared Management Model	4
Frequently Asked Questions	5
What compliance documentation does Oracle provide?	5
Has OCI implemented business continuity and disaster recovery plans?	5
Can OCI meet my data residency and offshore hosting requirements?	6
How does Oracle handle security incidents?	6
Does OCI perform vulnerability and penetration tests?	7
Can OCI customers perform security testing in their instances?	7
Does Oracle have a risk management policy?	7
Does Oracle provide audit rights to customers and their regulators?	7
Conclusion	7
Additional Resources	7

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. Oracle Cloud Infrastructure (OCI) is not an APRA-regulated entity (ARE), but Oracle recognises that some of its customers must adhere to APRA standards and may need information to evaluate OCI services.

Document Purpose

This document is intended to provide relevant information related to OCI to assist you in determining the suitability of using OCI in your operations.

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 solutions provide the benefits of the cloud, including secure and high-performance workload platforms in which to run all your workloads.

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/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 environments. By design, Oracle provides security functions for cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching. Customers are responsible for securely configuring and using their cloud resources. For more information, see the [cloud service documentation](#).

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

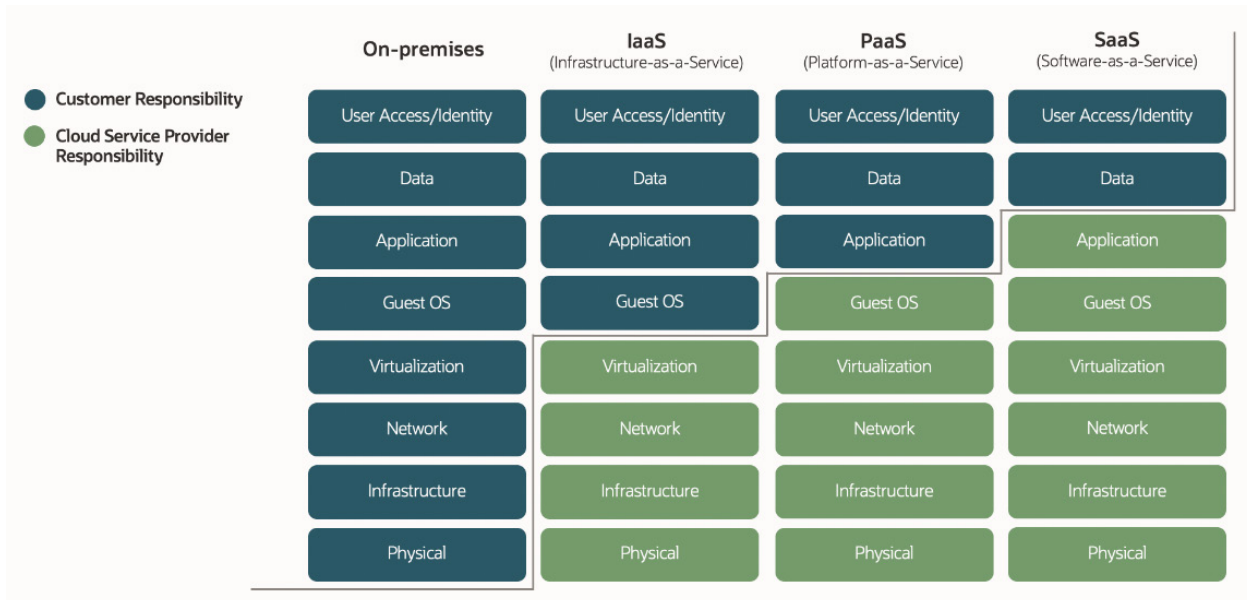


Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Frequently Asked Questions

Oracle is not an APRA-regulated entity (ARE) but recognises that some of its customers must adhere to APRA standards and may need information to evaluate OCI services. This section provides some guidance and information about OCI to assist AREs in their evaluation of whether the Oracle proposal helps them meet their regulatory requirements and obligations.

What compliance documentation does Oracle provide?

Oracle provides information about frameworks for which OCI has achieved a third-party attestation or certification for one or more of its services in the form of attestations. These attestations provide independent assessment of the security, privacy, and OCI compliance controls and can assist with compliance and reporting. Such attestations include CSA Star; SOC 1, 2, and 3; and ISO/IEC 27001, 27017, and 27018.

Oracle provides general and technical information for the use of its cloud services in the form of reference architectures and compliance advisories.

For more information, see [Oracle Cloud Compliance](#).

Has OCI implemented business continuity and disaster recovery plans?

Oracle has corporate security practices that encompass the functions related to security, safety, and business continuity for Oracle’s own internal operations and Oracle’s business operations in its provision of services to customers. They include a suite of internal information security policies and security practices that apply. [Oracle Corporate Security Practices](#) describe how Oracle protects the confidentiality, integrity, and availability of customer data and systems that are hosted in the Oracle Cloud or accessed when providing cloud services.

Oracle deploys Oracle Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in case an incident affects the services. Data centres retained by Oracle to host Oracle Cloud Services have component and power redundancy with backup generators in place.

OCI maintains a Business Impact Analysis (BIA) and Service Resiliency Plan (SRP) for each service. The plans are reviewed annually and include a defined purpose and scope, aligned with relevant dependencies. These plans are accessible to and understood by those Oracle personnel who will use them, and they have an assigned owner and include documented roles and responsibilities.

Customers are responsible for designing and implementing a cloud architecture that meets their own requirements for availability, business continuity, and disaster recovery. OCI offers the following guidance documentation for designing high-availability systems and protecting cloud resources against disasters:

- docs.oracle.com/iaas/Content/cloud-adoption-framework/high-availability.htm
- docs.oracle.com/iaas/Content/cloud-adoption-framework/disaster-recovery.htm

Customers must consider such guidance in the context of their own environment and requirements.

Can OCI meet my data residency and offshore hosting requirements?

Oracle has [cloud data centres](#) throughout the world, which helps many customers observe their data residency and hosting requirement obligations. OCI is hosted in regions and availability domains. A region is a localised geographic area, and an availability domain is one or more data centres located in a region.

When a customer signs up for an OCI account, the customer must select a data region, which is a geographic region that contains one or more Oracle Cloud data centres. When deciding on a default data region, the customer should consider the following criteria:

- Location of the data region
- Services available in the data region
- Any laws, restrictions, or guidelines applicable to the customer in its use of the cloud services

OCI will not change the data centre region without the customer's direction and consent.

How does Oracle handle security incidents?

Oracle evaluates and responds to any event when Oracle suspects that Oracle-managed customer data has been accessed by an unauthorised entity. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorises the Global Information Security (GIS) organisation to provide overall direction for incident prevention, identification, investigation, and resolution within Oracle's Lines of Business (for example, OCI).

Although incident management is a shared responsibility according to OCI's Shared Responsibility model, in the event that Oracle determines that a confirmed security incident involving information processed by Oracle has occurred, Oracle promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the [Data Processing Agreement for Oracle Services](#).

Learn more at oracle.com/corporate/security-practices/corporate/security-incident-response.html.

Does OCI perform vulnerability and penetration tests?

Yes. Oracle maintains teams of specialised 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: operational security scanning, penetration testing, and security analysis and testing of Oracle code. OCI has third-party vulnerability scans and penetration tests completed annually for applicable services. The summary of third-party-performed penetration tests for certain testing reports (if available) may be provided on a confidential basis upon request. Security testing of Oracle code is not provided, nor will a third-party perform static code assessments. Oracle does not generally permit outside security testing of Oracle corporate systems, applications, or networks.

Can OCI customers perform security testing in their instances?

Yes. Oracle Cloud Security Testing Policies describe when and how customers can conduct certain types of security testing of OCI services. For more information, see docs.oracle.com/iaas/Content/Security/Concepts/security_testing-policy.htm.

Does Oracle have a risk management policy?

Yes. Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle lines of business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle LOBs and geographies. It authorises a centralised Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation, and executive approvals for LOBs and their critical business operations. The RMRP objective is to establish a business-resiliency framework to help LOBs provide an efficient response to business interruption events that affect their operations.

Does Oracle provide audit rights to customers and their regulators?

Yes. Customers and their regulators have rights to access and audit Oracle's compliance with its obligations under their cloud services agreement as further specified in the Financial Service Addendum (FSA). Such audit rights include the right to conduct emergency audits. 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 in accordance with the FSA.

Conclusion

Cloud technology has become a means for financial services companies to capture new customers, create new services, and reduce costs. OCI offers geographically distributed regions to assist with business continuity and disaster protection.

Additional Resources

- [Outsourcing Involving Cloud Computing Services](#)
- [Oracle Cloud Compliance](#)
- [Oracle Cloud Hosting and Delivery Policies](#)
- [Oracle Corporate Security Practices](#)
- [Oracle Cloud Infrastructure Security Architecture](#)

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

Copyright © 2023, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120