ORACLE

APRA Regulated Entity Frequently Asked Questions

ORACLE

Important Note

This document is intended as Oracle's general product/service direction. It is intended for informational purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and any development, release, and timing of any features or functionality for Oracle's products or services remains at the sole discretion of Oracle. For any reliance on specific information within this document customers must discuss applicability with Oracle, and where agreed by Oracle, such information may be incorporated into a contract.

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 is not an APRA-regulated entity (ARE). However, Oracle recognizes that some of its customers must adhere to APRA standards, and will work with its customers in a transparent and engaging manner to understand their specific requirements. Customers should evaluate whether this information meets their regulatory requirements.**

Oracle has been committed to delivering on the needs of public and private sector organisations for over four decades. Oracle Cloud reinforces and extends this commitment by enabling regulated organisations as well as government agencies to move critical resources to an in-country cloud service, which has been designed for their needs and to facilitate their compliance objectives.

Essential Information Security Themes for AREs

In Oracle's experience, the key themes outlined below are captured and summarised from the APRA customers' frequently asked questions. These themes are identified as being critical in the mitigation of risks associated with information security incidents and customer confidentiality for AREs. AREs must demonstrate compliance in fields including, but not limited to:

- Business Continuity Planning (BCP) and Disaster Recovery (DR)
    - Business Continuity Planning is an essential component of overall risk management and focuses on the preparedness of the organisation to withstand natural or other disasters that interrupt the business.
- Data Security
    - Data security is a set of technologies that protect all types of data including personally identifiable information (PII) from intentional or accidental destruction, modification or disclosure in an unauthorized manner, or by unauthorized personnel.
- Data Residency and Offshore Arrangement
    - Data residency is the requirement that the data processed and stored in an IT system must remain within a specific country's borders.
- Incident Response
    - Incident response is an organised approach for handling security incidents, breaches and cyber threats. A well-defined incident response plan allows an organisation to effectively manage incident and mitigate the impact to the business.
- Vulnerability Management
    - Vulnerability management is the process for identifying vulnerabilities in IT assets, evaluating risk and taking appropriate action. Vulnerability scanning can help organisations identify weaknesses across systems and networks.
- Risk Management
    - Risk management is a process in which businesses identify, assess and treat risks that could potentially affect their business operations.

Frequently Asked Questions

Is Oracle an APRA regulated entity?

No. However, Oracle will work with the ARE to understand the ARE's regulatory obligation. This is in an effort to provide the necessary information, so the ARE can evaluate whether the Oracle proposal complies with the ARE's regulatory requirements/obligations.

What are the international standards that Oracle complies with?

As demonstrated in the Oracle Cloud Compliance page, Oracle meets a broad set of international and industry-specific compliance standards for deployments of Oracle Cloud services – such as: ISO 27001, SOC 1, SOC 2, PCI DSS, HIPAA, and FedRAMP.

How does Oracle handle business continuity planning (BCP) and disaster recovery (DR)?

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

Oracle periodically makes backups of customer production data in Oracle Cloud Services for Oracle's sole use to minimise data loss in the event of an incident. A backup is typically retained online or offline for a period of at least 60 days after the date that the backup is made. For Oracle Cloud Services that enable our customers to configure backups in accordance with their own policies, the customer is responsible for performing backups and restores of their data, non-Oracle software, and any software that is not provided by Oracle as part of these services.

Disaster recovery (DR) services for Oracle SaaS Public Cloud Services are intended to provide service restoration capability in the event of a major disaster, as declared by Oracle. Upon Oracle's declaration of a disaster, Oracle will commence its DR plan to recover the production environments of the affected Oracle SaaS Public Cloud Services in accordance with the predefined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as described in the Oracle SaaS Public Cloud Services-Pillar Document.

How does Oracle protect customer content including personally identifiable information (PII)?

Oracle has adopted security controls and practices for Oracle Cloud Services that are designed to protect the confidentiality, integrity, and availability of customer content that is hosted by Oracle in the customer's Oracle Cloud Services environment and to protect customer content from any unauthorized processing activities such as loss or unlawful destruction of data. Oracle continually works to strengthen and improve those security controls and practices.

Oracle has implemented and will maintain appropriate technical and organisational security measures for the processing of personal information designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal information. All Oracle employees and Oracle Affiliates' employees, as well as any third party sub-processors that process personal information, are subject to appropriate written confidentiality arrangements, regular training on information protection, and compliance with Oracle policies concerning protection of confidential information.

How does Oracle handle data residency and offshore hosting requirements?

Oracle has cloud data centres throughout the world, enabling customers to observe data residency requirements, and fulfil regulatory requirements. Oracle Cloud Infrastructure is hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centres located within a region. When a customer signs up for an Oracle Cloud account, the customer must select a data region, which is a

geographic region that contains one or more Oracle Cloud data centres. When deciding upon a default data region, the customer should consider:

- The location of the data region.
- The services available in each data region.
- Any restrictions or guidelines for the country in which customer resides.

Oracle will not change the data center region without the customer's consent.

How does Oracle handle incident response?

Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to incidents. This policy authorizes 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. In the event that Oracle determines that a security incident has occurred, Oracle promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities.

Oracle has also implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets. Data centre staff are trained in incident response and escalation procedures to address any security or availability events.

Does Oracle 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 complementary security testing: operational security scanning; penetration testing; security analysis and testing of Oracle code. Also, Oracle has 3rd party vulnerability scans/penetration tests completed annually for applicable services. The summary reports are available upon request if an NDA is in place.

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 across lines of business and geographies. It authorizes a centralized 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 critical business operations. The risk management resiliency program (RMRP) objective is to establish a business-resiliency framework to help provide an efficient response to business interruption events affecting Oracle's operations.

Conclusion

Cloud technology has become a means for financial services companies to capture new customers, create new services, and reduce costs. Oracle Cloud Services meets the needs of customers that require geographically distributed regions for business continuity, disaster protection, and regional compliance requirements.

Further readings

Oracle Cloud Compliance

Oracle Cloud Hosting and Delivery Policies

Oracle SaaS Public Cloud Services Pillar Document

Oracle PaaS and IaaS Public Cloud Services Pillar Document

Oracle Cloud Services Contracts

Oracle Security Practices

Oracle Corporate Security Practices

Oracle Cloud Security Practices

Oracle Cloud Essentials – Securing SaaS

Oracle Cloud Infrastructure Security Architecture

Brief: Gain Better Security with Oracle Cloud

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