ORACLE

Advisory: Oracle Cloud Infrastructure and Central Bank of Brazil (BACEN) CMN Resolution No. 4,893 of February 26, 2021

Select Description of Oracle Cloud Infrastructure Security Practices in the Context of the BACEN CMN Resolution No. 4,893 of February 26, 2021

August 2022, 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.

This document is for informational purposes only and is intended solely to help you assess your use of Oracle cloud services in the context of the Central Bank of Brazil (BACEN) National Monetary Council (CMN) Resolution No. 4,893 of February 26, 2021. This document might also help you to assess Oracle as an outsourced 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 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.

The BACEN CMN Resolution No. 4,893 of February 26, 2021 is subject to periodic changes or revisions by BACEN. The current version of the resolution is available at bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893.

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.

Table of Contents

Introduction **4**

Document Purpose **4**

About Oracle Cloud Infrastructure **4**

The Cloud Shared Management Model **4**

Summary of BACEN CMN Resolution No. 4,893 of February 26, 2021 **5**

Chapter III Contracting Services for Data Processing and Storage Services and Cloud Computing 5

Article 11 5

Article 12 6

Article 13 7

Article 14 7

Article 17 8

Chapter IV General Provisions 9

Article 20 9

Article 21 9

Article 22 9

Conclusion **10**

Introduction

The Central Bank of Brazil (BACEN) issued National Monetary Council (CMN) Resolution No. 4,893 of February 26, 2021, which describes several digital service requirements for regulated financial institutions, including cybersecurity policy and contracting data processing, storage, and cloud computing services. This resolution is intended to guide financial institutions in evaluating cloud service providers and establish controls to manage this relationship. For more information, see the resolution.

Document Purpose

This document is intended to provide relevant information related to Oracle Cloud Infrastructure (OCI) to help you determine the suitability of using OCI in relation to the BACEN CMN Resolution No. CMN 4,893 of February 26, 2021 and should be read in conjunction with the Oracle Contract Checklist for BACEN Regulations and Guidelines.

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 solutions provide customers the benefits of the cloud, including global, secure, and high-performance environments in which to run all their workloads. The cloud offerings discussed in this document include OCI.

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 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 available in the Oracle Help Center.

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

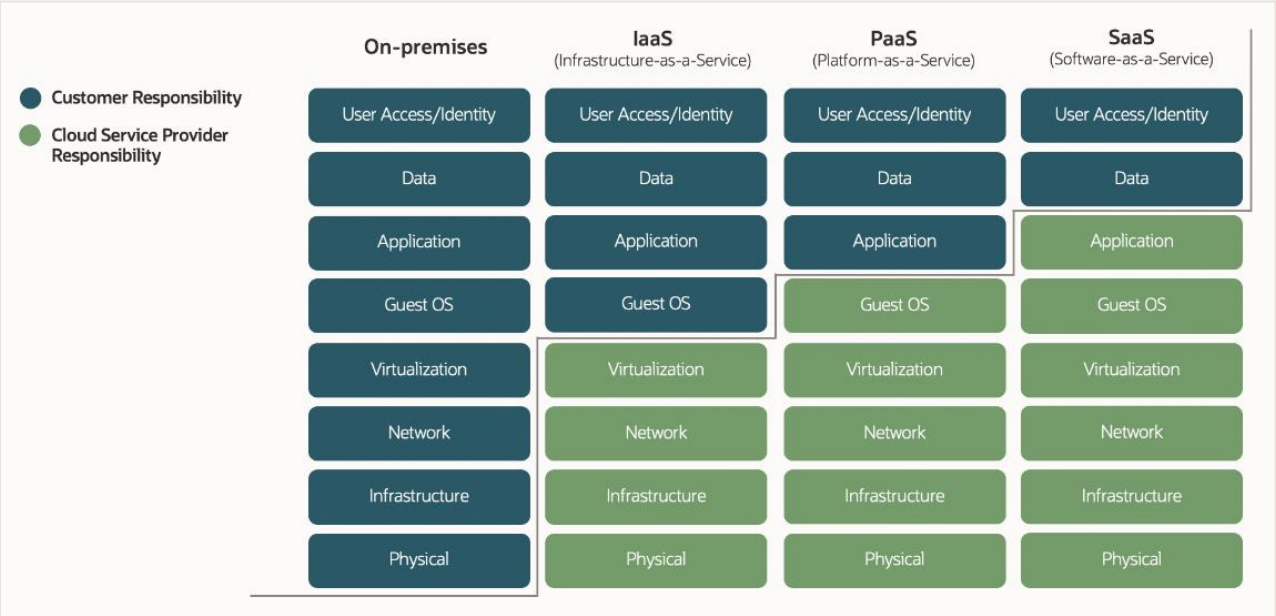

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Summary of BACEN CMN Resolution No. 4,893 of February 26, 2021

This section includes general summaries and excerpts from some of the most relevant provisions of the BACEN CMN Resolution No. 4,893 pertaining to cloud operations and security. Beginning with Chapter III, "Contracting Services for Data Processing and Storage Services and Cloud Computing," each section describes applicable OCI operational and security practices and services that might help customers meet the resolution requirements.

Chapter III Contracting Services for Data Processing and Storage Services and Cloud Computing

Article 11

"The institutions referred to in art. 1 ["This Resolution provides for the cyber security policy and the requirements for contracting data processing and storage and cloud computing services to be observed by institutions authorized to operate by the Central Bank of Brazil"] must ensure that their policies, strategies and structures for risk management provided for in the regulations in force, specifically with regard to the selection criteria regarding the outsourcing of services, contemplate the contracting of relevant data processing and storage and cloud computing services, in the country or abroad."

Customers are solely responsible for conducting their own risk assessment when considering the outsourcing of services.

Oracle provides several resources to help customers conduct necessary risk assessment and due diligence:

- Consensus Assessment Initiative Questionnaire (CAIQ) for OCI: oracle.com/a/ocom/docs/oci-corporate-caiq.pdf
- Oracle Cloud Compliance site: oracle.com/cloud/compliance/
- Oracle Corporate Security Practices: oracle.com/corporate/security-practices/corporate/

Article 12

"The institutions mentioned in art. 1, prior to contracting relevant data processing and storage and cloud computing services, must adopt procedures that include: ...

II – verification of the potential service Provider's ability to ensure: ...

b) the institution's access to data and information to be processed or stored by the service provider;

c) confidentiality, integrity, availability and recovery of data and information processed or stored by the service provider;

d) its adherence to certifications required by the institution for the provision of the services to be contracted;

e) access by the contracting institution to the reports prepared by an independent specialized auditing company contracted by the service provider, relating to the procedures and controls used in the provision of the services to be contracted;

f) the provision of information and adequate management resources for monitoring the services to be provided;

g) identification and segregation of the institution's customer data through physical or logical controls; and

h) the quality of access controls aimed at protecting data and information from the institution's clients."

Customers are solely responsible for access to their data and information stored or processed in OCI.

Oracle has adopted security controls and practices that are designed to protect the confidentiality, integrity, and availability of customer data that is hosted in OCI. OCI implements multiple levels of security checks, testing, threat and risk assessments, vulnerability scanning, and penetration testing to assess system controls. These controls are guided by industry standards and are deployed across the corporate infrastructure by using a risk-based approach. For more information, see the Oracle Cloud Hosting and Delivery Policies at oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf.

OCI provides customers with the capability to restrict access to information stored or processed in their application in accordance with their confidentiality commitments and requirements. Customers can use OCI services such as Identity and Access Management (IAM) to manage access to their cloud environment. See docs.oracle.com/en-us/iaas/Content/Identity/getstarted/identity-domains.htm.

OCI operates under policies that are generally aligned with the International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 27002 code of practice for information security controls. The internal controls of OCI are subject to periodic testing by independent third-party audit organizations. Such audits may be based on the following standards:

- Statement on Standards for Attestation Engagements (SSAE) 18, Reporting on Controls at a Service Organization (SSAE 18)
- International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization (ISAE 3402),
- ISAE No. 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information (ISAE 3000)
- Other third-party auditing standards or procedures applicable to OCI

For more information about OCI compliance attestations, see oracle.com/corporate/cloud-compliance/#attestations.

Customers can access metrics on the service availability level for Oracle cloud services that they have purchased under their order through the Customer Notifications Portal. OCI status by service and data region are located at ocistatus.oraclecloud.com/#/.

OCI uses network devices to control access between the internet and Oracle cloud by allowing only authorized traffic. Network devices are deployed in a layered approach to perform packet inspection with security policies configured to filter packets based on protocol, port, source, and destination IP address to identify authorized sources, destinations, and traffic types. Additionally, OCI has multiple monitoring programs in place to assess against image baselines.

For more information, see oracle.com/a/ocom/docs/oci-corporate-caiq.pdf.

Article 13

"For the purposes of this Resolution, cloud computing services cover the availability to the contracting institution, on demand and in a virtual manner, of at least one of the following services:

I – data processing, data storage, network infrastructure and other computing resources that allow the contracting institution to deploy or run software, which may include operating systems and applications developed by the institution or acquired by it;

II – implementation or execution of applications developed by the contracting institution, or acquired by it, using the service provider's computing resources; or

III – execution, through the internet, of applications deployed or developed by the service provider, using the service provider's own computing resources."

Oracle offers a comprehensive suite of cloud computing services available on-demand and delivered virtually worldwide. This suite includes compute, storage, networking, data management, analytics, and application development services. For more information about OCI services, see docs.oracle.com/iaas/Content/home.htm

Article 14

"The institution contracting the services mentioned in art. 12 is responsible for reliability, integrity, availability, security and secrecy in relation to the contracted services, as well as compliance with legislation and regulations in force."

Oracle commits to delivering the services at the contract-agreed level of availability and quality, and offers multiple tools and services to support the monitoring obligations of its customers.

Customers can access metrics on the service availability level for Oracle cloud services that they have purchased under their order through the Customer Notifications Portal. For more information about OCI Service Level Agreement (SLA), see oracle.com/cloud/sla/.

Oracle implements a variety of technical security controls designed to protect the confidentiality, integrity, and availability of corporate information assets. These controls are guided by industry standards and are deployed across the corporate infrastructure by using a risk-based approach. Oracle has corporate standards that define approved cryptographic algorithms and protocols. Oracle products and services are required to use only up-to-date versions of approved security-related implementations, as guided by industry practice.

Oracle's security policies cover the management of security for both Oracle's internal operations and the services that Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are generally aligned with the ISO/IEC 27002:2013 and ISO/IEC 27001:2013 standards and guide all areas of security within Oracle. Oracle also 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 an independent assessment of the security, privacy, and compliance controls of the applicable OCI services and can assist with compliance and reporting. Such attestations include CSA Star, SOC, and ISO/IEC 27001, 27017, and 27018. For more information, see oracle.com/corporate/security-practices/corporate/.

Article 17

"Contracts for the provision of relevant processing, data storage and cloud computing services must provide for:

I – indication of the countries and region in each country where the services can be provided and the data can be stored, processed and managed;

II – the adoption of security measures for the transmission and storage of the data mentioned in item I;

III – maintenance, while the contract is in force, of data segregation and access controls to protect customer information;

IV – the obligation, in the event of termination of the contract, of:

a) transfer of the data mentioned in item I to the new service provider or contracting institution; and

b) deletion of the data mentioned in item I by the substituted contracted company, after the transfer of the data provided for in item "a" and confirmation of the integrity and availability of the data received; . . ."

The required rights and obligations of each party are set out in contract documents that are signed by the customer and Oracle before the provisioning of cloud services. Oracle Cloud Service contracts are available at oracle.com/corporate/contracts/cloud-services/contracts.html.

The location of a customer tenancy is determined by the customer when cloud services are provisioned. When setting up their account, customers choose a home region in which to locate their tenancy. Their data stays in that region unless they choose to move it. For more information about regions, availability domains, and setting up your tenancy, see docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm and docs.cloud.oracle.com/iaas/Content/GSG/Concepts/settinguptenancy.htm.

The Oracle Cloud Hosting and Delivery Policies include the Oracle Cloud Security Policy, which describes security measures including data segregation and access controls. See oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf.

The Oracle Cloud Hosting and Delivery Policies include the Oracle Cloud Suspension and Termination Policy, which describes responsibilities when a contract is terminated. For a period of 60 days after termination, Oracle makes available—by means of secure protocols and in a structured, machine-readable format—customers' content that resides in the production cloud services environment, or keeps the cloud service system accessible, for data retrieval. Oracle provides reasonable assistance to customers to retrieve their content from the production services environment and provides help to understand the structure and format of the export file. After the retrieval period expires, Oracle deletes the data from the Oracle cloud services environments unless otherwise required by applicable law. Additionally, the Oracle Financial Services Addendum (FSA) provides customers with the ability to order transition services and transition assistance to help transfer or re-incorporate a concerned function back to the customer or to a third party

OCI also offers the following resources to guide customers in deleting, managing, and terminating an instance:

- Deleting a volume: docs.oracle.com/iaas/Content/Block/Tasks/deletingavolume.htm
- Managing objects: docs.oracle.com/iaas/Content/Object/Tasks/managingobjects.htm
- Managing files systems: docs.oracle.com/iaas/Content/File/Tasks/managingfilesystems.htm
- Terminating an instance: docs.oracle.com/iaas/Content/Compute/Tasks/terminatinginstance.htm

Chapter IV General Provisions

Article 20

"The procedures adopted by institutions for risk management provided for in the regulations in force must include, with regard to business continuity:

I – the treatment provided to mitigate the effects of the relevant incidents referred to in item IV of art. 3 and the interruption of the relevant processing, data storage and cloud computing services contracted;"

Customers are solely responsible for creating their business continuity procedures.

Oracle corporate business continuity policy, standards, and practices are governed by the Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and are generally aligned with ISO 22301 Business Continuity Management Systems guidance. For more information about the centralized RMRP program and the risk management activities within geographies and lines of business, see oracle.com/corporate/security-practices/corporate/resilience-management.

Oracle backs up critical internal infrastructure systems. Additionally, Oracle cloud service data centers are designed to help protect the security and availability of customer data. Oracle cloud service data centers align with American National Standards Institute/Telecommunications Industry Association (ANSI/TIA)-942-A Tier 3 or Tier 4 standards and follow an N2 redundancy methodology for critical equipment operation. For more information, see oracle.com/corporate/security-practices/corporate/physical-environmental.html.

Article 21

"The institutions referred to in art. 1 must institute monitoring and control mechanisms in order to ensure the implementation and effectiveness of the cyber security policy, the action plan and incident response and the requirements for contracting data processing and storage and computing services in cloud..."

Customers are solely responsible for assessing, monitoring, and reporting risks in their environment.

OCI offers the following services and features that might help you meet this requirement:

- **Cloud Guard** helps you monitor, identify, achieve, and maintain a strong security posture on OCI. Use this cloud native service to examine OCI resources for security weaknesses related to configuration, and OCI operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist with, or take corrective actions, based on the configuration. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.
- **Monitoring** helps customers actively and passively monitor their cloud resources by using metrics and alarms that notify them when metrics meet alarm-specific triggers. For more information, see docs.oracle.com/iaas/Content/Monitoring/home.htm.

Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to security incidents. This policy authorizes the Oracle Global Information Security organization to provide overall direction for incident prevention, identification, investigation, and resolution.

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

Article 22

"Without prejudice to the duty of secrecy and free competition, the institutions mentioned in art. 1 must develop initiatives to share information about the relevant incidents referred to in art. 3, item IV."

Customers are solely responsible for creating their incident reporting policies.

If 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 requirements. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared. For more information, see oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html.

When an incident is discovered, OCI 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 that improve security posture and defense in depth. Formal procedures and systems are used to collect information and maintain a chain of custody for evidence during incident investigation. For more information, see oracle.com/corporate/security-practices/corporate/security-incident-response.html.

Conclusion

Oracle is committed to helping customers operate globally in a fast-changing business environment and address the challenges of technology risks. Before deploying Oracle cloud services, Oracle strongly recommends that cloud customers formally analyze their cloud strategy to determine the suitability of using the applicable Oracle cloud services considering their own legal and regulatory compliance obligations. For more information, see oracle.com/corporate/cloud-compliance/.