ORACLE

Oracle Contract Checklist for the Central Bank of Brazil (BACEN) Resolution CMN 4,893 of February 26, 2021

June 2022

Disclaimer

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 contract(s) between you and Oracle determine(s) the scope of services provided and the related legal terms and this document is provided for reference purposes only, and is not part of, and does not otherwise create or amend, any agreement, warranties, representations or other obligations between you and Oracle. Oracle disclaims 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 meeting their legal and regulatory requirement*s*.

The information in this document was current as of June 01, 2022

Overview

Oracle has developed this document as a part of its continuing efforts to help financial services customers meet their unique obligations, particularly under the BACEN Resolution CMN 4,893 relating to the use of Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications (SaaS)[1]. We want to make it easier for you as a financial institution to identify the sections of the Oracle Cloud services contract that pertain to the requirements in Resolution 4,893. In this document, you will find a mapping of BACEN guidelines to relevant Oracle Contracting Guidelines, along with a reference to specific section(s) of the Oracle Cloud services contract and a short explanation to help you conduct customer review of the Oracle Cloud services.

The Oracle Cloud services contract includes the following customer - specific components, all of which are referenced in this document:

- Oracle Cloud services contract – an Oracle Cloud Services Agreement (CSA) or Oracle Master Agreement (OMA) with Schedule C (Cloud)
- **FSA** – The Oracle Financial Services Addendum to the Oracle Cloud Services Agreement (CSA) or Master Agreement (OMA) with Schedule C (Cloud)
- **Ordering Document** – Oracle Cloud services order
- **Services Specifications** – Service-specific components, including the Oracle Cloud Hosting and Delivery Policies with applicable Services Pillar Document(s) and the Oracle Data Processing Agreement (DPA).

BACEN Contracting Guidelines

The Central Bank of Brazil (BACEN) issued Resolution CMN No. 4,893 on February 26th, 2021 which describes several digital service requirements for regulated financial institutions including cybersecurity policy, contracting for 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. Chapter III of Resolution 4,893 prescribes relevant guidelines when contracting with data processors and cloud service providers in Brazil and abroad. These guidelines are referred to below as the BACEN Contracting Guidelines.

For more information on financial regulations in other jurisdictions please visit https://www.oracle.com/cloud/compliance/

	TOPIC REF.	DESCRIPTION OF BACEN GUIDELINE	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT	ORACLE EXPLANATION
CHAPTER III: CONTRACTING DATA PROCESSING AND STORAGE SERVICES AND CLOUD COMPUTING				
1.	**Art. 11**	The institutions referred to in art. 1 must ensure that their policies, strategies and structures for risk management provided for in the regulations are in force, specifically with regard to the decision criteria regarding the outsourcing of	• Oracle Cloud Hosting and Delivery Policies	This is primarily a customer consideration. However, Oracle provides information to assist its customers in conducting necessary risk assessments and due diligence.

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

		services, contemplate the contracting of relevant data processing and storage and cloud computing services, in the country or abroad.		Customers can access these materials through the Oracle Cloud Compliance site , Oracle Corporate Security Practices, and Oracle Cloud Hosting and Delivery Policies.
2.	**Art. 12**	The institutions mentioned in art. 1, prior to contracting relevant data processing and storage and cloud computing services, must adopt procedures that include:		
3.	Art. 12 (I)	the adoption of corporate governance and management practices proportional to the relevance of the service to be contracted and the risks to which they are exposed; and		This is primarily a customer consideration.
4.	Art. 12 (II)	verification of the potential service provider's ability to ensure:		
5.	Art. 12 (II)(a)	compliance with the legislation and regulations in force;	• Section 14 CSA • Section 14 Schedule C • Section 8 FSA	**Section 14 of the CSA and Section 14 Schedule C** sets out the governing law and jurisdiction of the agreement. See also **Section 8 of the FSA** – Compliance with Laws
6.	Art. 12 (II)(b)	the institution's access to data and information to be processed or stored by the service provider;	• Oracle Cloud Hosting and Delivery Policies (particularly sections 3.1 & 3.2)	**Section 3.1 of the** Oracle Cloud Hosting and Delivery Policies states that Oracle Cloud Services are designed to be available 24 hours a day, 7 days a week, 365 days a year, except during maintenance periods, technology upgrades and as otherwise set forth in the Oracle agreement, Customer order and this *Oracle Cloud Service Level Agreement*. Under **Section 3.2 of the** Oracle Cloud Hosting and Delivery Policies Oracle works to meet the Target Service Availability Level, or Target Service Uptime of 99.7%. This is in accordance with the terms set forth in the Cloud Service Pillar documentation for the applicable Oracle Cloud Service (or such other Target Service Availability Level or Target Service Uptime specified by Oracle for the applicable Oracle Cloud Service in such documentation).

7.	Art. 12 (II)(c)	confidentiality, integrity, availability and recovery of data and information processed or stored by the service provider;	• Sections 6 and 8 DPA • Sections 4 and 5 Schedule C • Section 4 and 5 CSA • Oracle Cloud Hosting and Delivery Policies (particularly Sections 1, 3.1 and 3.2) • Oracle SaaS Public Cloud Services Pillar Document • Oracle PaaS and IaaS Public Cloud Services Pillar Document	• **Technical and organization security measures:** - **Section 6** – Security and Confidentiality – of the Oracle Data Processing Agreement - the Oracle Cloud Hosting and Delivery Policies as well as the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, as applicable. - Oracle Corporate Security Practices • **Confidentiality and Protection of "Customer Content":** - **Section 4 of Schedule C** and **Section 4 of the CSA**, as applicable (specifically, Oracle's obligation to protect the confidentiality of "Customer Content" for as long as it resides in the Services) - **Section 5 of Schedule C** and **Section 5 of the CSA**, as applicable - **Section 8** - Incident Management and Breach Notification – of the Oracle Data Processing Agreement • **Service Availability and Service Level Agreements:** **Sections 3.1 and 3.2 of the** Oracle Cloud Hosting and Delivery Policies as well as the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, as applicable.
8.	Art. 12 (II)(d)	its adherence to certifications required by the institution for the provision of the service to be contracted;		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. These attestations provide independent assessment of the security, privacy, and compliance controls of the applicable Oracle cloud services and can assist with an institution's compliance and reporting. Such attestations include CSA STAR, SOC 1, 2, and 3, and ISO/IEC 27001,27017, 27018, 27701, 20000-1, and 9001. For more information, see Oracle Cloud Compliance site.

9.	Art. 12 (II)(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;	See row 8 above.	See row 8 above.
10.	Art. 12 (II)(f)	the provision of information and adequate management resources for monitoring the services to be provided;	• Section 3.2.2 & 3.4 of the Oracle Cloud Hosting and Delivery Policies • Section 11 Schedule C • Section 11 CSA	**Section 3.2.2 of the** Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability. Under **Section 3.4 of the** Oracle Cloud Hosting and Delivery Policies Oracle uses a variety of software tools to monitor the availability and performance of the Oracle Cloud Services and the operation of infrastructure and network components. **Section 11.1 of Schedule C and Section11.1 of the CSA, as applicable,** explains that Oracle also continuously monitors the Cloud services.
11.	Art. 12 (II)(g)	identification and segregation of the institution's customer data through physical or logical controls; and	• Section 6.1 DPA • Section 1.7 of the Oracle Cloud Hosting and Delivery Policies	**Section 6.1 of the DPA** states that Oracle has implemented and will maintain appropriate technical and organizational 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. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. Please also refer to Oracle Corporate Security Practices Under **Section 1.7 of the** Oracle Cloud Hosting and Delivery Policies. Customer Content is logically or physically segregated from the content of other customers hosted in the Oracle Cloud

				Services environments. All Oracle Public Cloud networks are segregated from Oracle's Corporate networks.
12.	Art. 12 (II)(h)	the quality of access controls aimed at protecting data and information from the institution's clients.	• Section 5 CSA • Section 5 Schedule C • Section 6 DPA	**Section 5 of the CSA** and **Schedule C** states that in order to protect Customer Content provided to Oracle as part of the provision of the Services, Oracle will comply with the applicable administrative, physical, technical and other safeguards, and other applicable aspects of system and content management and abide by applicable internal privacy policies. Under **Section 6 of the DPA**, Oracle has implemented and will maintain appropriate technical and organizational 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. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. Additionally, all Oracle authorization decisions for granting, approval, and review of access are based on the following principles: • Need to know: Does the user require this access for his job function? • Segregation of duties: Will the access result in a conflict of interest? • Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose? See also row 7 above.
13.	Art. 12 ¶1	In assessing the relevance of the service to be contracted, mentioned in item I of the heading, the contracting institution must		This is primarily a customer consideration.

		consider the criticality of the service and the sensitivity of the data and information to be processed, stored and managed by the contracted party, taking into account, including the classification carried out under the terms of art. 3, item V, item "c".		
14.	Art. 12 ¶2	The procedures mentioned in the heading, including the information related to the verification mentioned in item II, must be documented.		This is primarily a customer consideration.
15.	Art. 12 ¶3	In the case of running applications through the internet, referred to in item III of art. 13, the institution must ensure that the potential service provider adopts controls that mitigate the effects of possible vulnerabilities in the release of new versions of the application.	• Section 3.4.2 of the Oracle Cloud Hosting and Delivery Policies • Section 4 of the Oracle Cloud Hosting and Delivery Policies	Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at fostering security innovations, reducing the incidence of security weaknesses, and reducing the impact of security weaknesses. For more information, see Oracle Corporate Security Practices. Under **Section 4 of the** Oracle Cloud Hosting and Delivery Policies Oracle has cloud services change management procedures that are designed to minimize service interruption during the implementation of changes. Changes made through change management procedures include system and service maintenance activities, upgrades and updates, and customer-specific changes. For customer-specific changes and upgrades, where feasible, Oracle coordinates the maintenance periods with customers. Oracle reserved maintenance periods include the following ones: **Emergency maintenance** Oracle may be required to perform emergency maintenance to protect the security, performance, availability, or stability of Oracle cloud services. Emergency maintenance is required to address an exigent situation with a cloud service that cannot be addressed except on an emergency basis (for example, a hardware failure of the infrastructure underlying the service). Oracle works

				to minimize the use of emergency maintenance, and to the extent reasonable under the circumstances, provides 24 hours prior notice for any emergency maintenance requiring a service interruption. **Major maintenance changes** To help ensure continuous stability, availability, security, and performance of Oracle cloud services, Oracle limits major changes to its hardware infrastructure, operating software, applications software, and supporting application software under its control, typically to no more than twice per calendar year. Each such major change event is considered scheduled maintenance and may cause Oracle cloud services to be unavailable. Each such event is targeted to occur at the same time as the scheduled maintenance period. Oracle provides no less than 60 days prior notice of a major change event.
16.	Art. 12 ¶4	The institution must have the necessary resources and competences for the proper management of the services to be contracted, including for the analysis of information and use of resources provided under the terms of item "f" of item II of the heading.		This is primarily a customer consideration.
17.	**Art. 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:		
18.	Art. 13 (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;	• CSA • Ordering Document	Written Cloud services contract, referenced Service Specifications, and Ordering Document.

19.	Art. 13 (II)	implementation or execution of applications developed by the institution contracting party, or acquired by it, using the service provider's computing resources;	See row 18 above.	See row 18 above.
20.	Art. 13 (III)	execution, through the internet, of applications deployed or developed by the service provider, using the service provider's own computing resources.		Oracle Cloud Infrastructure (OCI) is a set of complementary cloud services that enable customer 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 Oracle Cloud Infrastructure, see https://docs.oracle.com/en-us/iaas/Content/home.htm Oracle Cloud Applications (SaaS) is the world's most complete, connected SaaS suite. By delivering a modern user experience and continuous innovation, Oracle is committed to the success of customers with continuous updates and innovations across the entire business: finance, human resources, supply chain, manufacturing, advertising, sales, customer service, and marketing. For more information about Oracle Cloud Applications, see https://oracle.com/applications.
21.	**Art. 14**	The contracting institution for the services mentioned in art. 12 is responsible for reliability, integrity, availability, security and secrecy in relation to contracted services, as well as compliance with legislation and regulations in force.	See row 7 above.	See row 7 above.
22.	**Art. 15**	The contracting of relevant processing, data storage and cloud computing services must be communicated by the institutions referred to in art. 1 to the Central Bank of Brazil.	• CSA • Ordering Document • Schedule C	The parties obligations with respect to the cloud services are documented in written Cloud services contract, referenced Service Specifications, and Ordering Document as well as the below resources:

			• DPA • Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services Pillar Document	- Oracle Data Processing Agreement - Oracle Cloud Hosting and Delivery Policies - PaaS/IaaS Cloud Services Pillar Document - SaaS Cloud Services Pillar Document
23.	Art. 15 ¶1	The communication mentioned in the heading must contain the following information:		
24.	Art. 15 ¶1(I)	the name of the contracted company;	See row 22 above.	See row 22 above.
25.	Art. 15 ¶1(II)	the relevant services contracted; and	See row 22 above.	See row 22 above.
26.	Art. 15 ¶1(III)	indication of the countries and regions in each country where the services can be provided and the data can be stored, processed and managed, defined under the terms of item III of art. 16, in the case of contracting abroad.	• Ordering Document	The Ordering Document or the cloud customer support portal states the data center region applicable to ordered Cloud services. Please also see the List of Oracle Affiliates: https://www.oracle.com/corporate/oracle-affiliates.html
27.	Art. 15 ¶2	The communication referred to in the heading must be carried out within ten days after the contracting the services.		This is primarily a customer consideration.
28.	Art. 15 ¶3	The contractual amendments that imply modification of the information referred to in ¶1 must be communicated to the Central Bank of Brazil within ten days after the contractual amendment.	• CSA • Schedule C • Ordering Document	Written Cloud services contract, referenced Service Specifications and Ordering Document.
29.	**Art. 16**	The contracting of relevant processing, data storage and cloud computing services provided abroad must comply with the following requirements:		

30.	Art. 16 (I)	the existence of an agreement for the exchange of information between the Central Bank of Brazil and the supervisory authorities of the countries where the services may be provided;	• Section 2.7 FSA	**Section 2.7 of the FSA** indicates that Oracle will provide customers' regulators with necessary information.
31.	Art. 16 (II)	the contracting institution must ensure that the provision of the services referred to in the heading does not cause damage to its regular operation or hinder the performance of the Central Bank of Brazil;	• CSA • Ordering Document • Schedule C • Section 8 FSA	Written Cloud services contract, referenced Service Specifications, and Ordering Document. See also **Section 8 of the FSA** – Compliance with Laws
32.	Art. 16 (III)	the contracting institution must define, prior to contracting, the countries and regions in each country where the services can be provided and the data can be stored, processed and managed; and	• Oracle Cloud Hosting and Delivery Policies • PaaS and IaaS Cloud Services Pillar Document • SaaS Cloud Pillar Document	The Ordering Document or the cloud customer support portal states the data center region applicable to ordered Cloud services. Oracle and Oracle affiliates may have access to data while providing support and services subject to the Oracle Cloud Hosting and Delivery Policies, the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, and Oracle Data Processing Agreement, as applicable. Please also see the List of Oracle Affiliates: https://www.oracle.com/corporate/oracle-affiliates.html
33.	Art. 16 (IV)	the contracting institution must provide alternatives for the continuity of the business, in the case of impossibility of maintenance or termination of the service provision contract.	• Section 5 FSA • Section 4.3 FSA • Section 2 of the Oracle Cloud Hosting and Delivery Policies	**Section 5 of the FSA** indicates that Oracle maintains business continuity plans and testing pertaining to Oracle's internal operations as utilized in the provision of Oracle Cloud services. Please see the Oracle Cloud Service Continuity Policy in **Section 2 of the** Oracle Cloud Hosting and Delivery Policies. Additionally, under **Section 4.3 of the FSA**, in the event customer requires assistance with a transition (whether to another service provider or to Customer own organization), Customer may request additional professional services from Oracle ("Transition Assistance Services"), and, Oracle will enter into good faith negotiations with

				Customer regarding such Transition Assistance Services. Any Transition Assistance Services to be performed by Oracle must be mutually agreed by the parties in a separate order.
34.	Art. 16 ¶1	In the event of no agreement under the terms of item I of the heading, the contracting institution must request authorization from the Central Bank of Brazil to:		
35.	Art. 16 ¶1(I)	contracting the service, within a minimum period of sixty days before contracting, in compliance with the provisions of art. 15, ¶1, of this Resolution; and		This is primarily a customer consideration.
36.	Art. 16 ¶1(II)	contractual amendments that imply modification of the information referred to in art. 15, ¶1, observing the minimum period of sixty days before the contractual amendment.		This is primarily a customer consideration.
37.	Art. 16 ¶2	In order to comply with items II and III of the heading, institutions must ensure that legislation and regulations in the countries and regions in each country where the services may be provided do not restrict or prevent the access of contracting institutions and the Central Bank of Brazil to data and information.		This is primarily a customer consideration.
38.	Art. 16 ¶3	Proof of compliance with the requirements referred to in items I to IV of the heading and compliance with the requirement referred to in ¶2 must be documented.		This is primarily customer consideration.
39.	**Art. 17**	Contracts for the provision of relevant processing, data storage and cloud computing services must provide for:		

40.	Art. 17 (I)	an indication of the countries and region in each country where the services may be provided and the data may be stored, processed and managed;	• Oracle Cloud Hosting and Delivery Policies • DPA • PaaS and IaaS Cloud Services Pillar Document • SaaS Cloud Pillar Document • Oracle Processor Code	The Ordering Document or the cloud customer support portal states the data center region applicable to ordered Cloud services. Oracle and Oracle affiliates may have access to data while providing support and services subject to the Oracle Cloud Hosting and Delivery Policies, the PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, and Oracle Data Processing Agreement, as applicable. Please also see the List of Oracle Affiliates: https://www.oracle.com/corporate/oracle-affiliates.html The Oracle Processor Code (Binding Corporate Rules for Processors) applies to the processing of personal information by Oracle on customers' behalf as part of the provision of services under an Oracle Cloud services contract. Under **Section 5.1 of the DPA**, without prejudice to any applicable regional data center restrictions for hosted Services specified in Customer Services Agreement, Oracle may Process Personal Information globally as necessary to perform the Services. Also refer to **Section 4.1.3** (Data Center Migrations) Oracle Cloud Hosting and Delivery Policies, stating Oracle may migrate Customer Oracle Cloud Services deployed in data centers retained by Oracle between production data centers in the same data center region as deemed necessary by Oracle or in the case of disaster recovery. For data center migrations for purposes other than disaster recovery, Oracle will provide a minimum of 30 days notice to Customer.
41.	Art. 17 (II)	the adoption of security measures for the transmission and storage of data mentioned in item I of the heading;	• Section 6.1 DPA • Section 1 of the Oracle Cloud Hosting and Delivery Policies	**Section 6.1 of the DPA** states that Oracle has implemented and will maintain appropriate technical and organizational 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. These security measures govern all areas of security applicable to

				the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. See **Section1** of Oracle Cloud Hosting and Delivery Policies as it relates to the transmission and storage of data. Please also refer to Oracle Corporate Security Practices
42.	Art. 17 (III)	maintenance, while the contract is in force, of data segregation and access controls to protect customer information;	• Sections 1.4 & 1.7 of the Oracle Cloud Hosting and Delivery Policies	Under **Section 1.4 of the** Oracle Cloud Hosting and Delivery Policies, with respect to Oracle personnel accessing the Services environment for the Cloud Services (including Customer Content residing in the Cloud Services), Oracle enforces Role Based Access Controls (RBAC) and employs the access management principles of "need to know", "least privilege" and "segregation of duties." In addition, Oracle provides a mechanism by which Customer control Customer access to Customer Cloud Services environment and to Customer Content by Customer authorized staff. Under **Section 1.7 of the** Oracle Cloud Hosting and Delivery Policies. Customer Content is logically or physically segregated from the content of other customers hosted in the Oracle Cloud Services environments. All Oracle Public Cloud networks are segregated from Oracle's Corporate networks. See also row 41 above.
43.	Art. 17 (IV)	the obligation, in the event of termination of the contract, of:		
44.	Art. 17 (IV)(a)	transfer of the data mentioned in item I of the heading to the new service provider services or the contracting institution; and	• Section 4.1 FSA • Section 9.1 DPA • Section 4.2 FSA • Section 4.3 FSA	Under **Section 4.1 of the FSA**, relating to retrieval of Customer Content, upon (a) the end of the Services Period applicable under Customer order or (b) Customer termination of the applicable cloud services in accordance with Customer Services Agreement and Customer order Oracle will provide reasonable assistance to its customers during the retrieval period to enable Customer to retrieve Customer Content from the production Services

				environment, including assistance with Customer understanding of the structure and format of the export file. Please also refer to **Section 9.1 of the** Oracle Data Processing Agreement regarding return and deletion of personal information upon termination of services. **Section 4.2 & 4.3 of the FSA** address transitional use rights as well as assistance that Oracle will provide to customers in the event of termination and transition to the customer's data center or to another service provider.
45.	Art. 17 (IV)(b)	deletion of the data mentioned in item I of the heading 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;	• Section 4.1 FSA	Under **Section 4.1 of the FSA**, without prejudice to the terms within the Service Specifications (including without limitation the Oracle Data Processing Agreement) relating to retrieval of customer content, upon (a) the end of the Services Period applicable under order or (b) termination of the applicable cloud services in accordance with Services Agreement and order (both referred to as "Termination"), and provided customer submit a service request in the Cloud Customer Support Portal designated for the cloud service (e.g., My Oracle Support) no later than 30 days following Termination, Oracle will provide reasonable assistance to customer during the retrieval period to enable customer to retrieve content from the production Services environment, including assistance with Your understanding of the structure and format of the export file. Customers may also request confirmation of data deletion from Oracle See also row 44 above.
46.	Art. 17 (V)	access by the contracting institution to:		
47.	Art. 17 (V)(a)	information provided by the contracted company, in order to verify the	• Section 1 FSA • Section 10 DPA	Please refer to **Section 1** (Customer Audit Rights) **of the FSA**

		compliance with the provisions of items I to III of the heading;		**Section 1.1 of the FSA** grants customer the same rights of access and audit for Oracle's Strategic Subcontractors. **Section 1.5 of the FSA** provides customers full access and unrestricted audits as specified in the FSA and supplements the Oracle Cloud services agreement and the Oracle Data Processing Agreement. **(Section 10)**
48.	Art. 17 (V)(b)	information regarding certifications and specialized audit reports, mentioned in art. 12, item II, items "d" and "e"; and	• Section 1.12 of the Oracle Cloud Hosting and Delivery Policies	**Section 1.12 of the** Oracle Cloud Hosting and Delivery Policies indicates that Oracle may conduct independent reviews of Cloud services utilizing third parties in the following areas (the scope of any such reviews may vary by service and country): • SOC 1 (based on Statement on Standards for Attestation Engagements (SSAE) No 18) and/or SOC 2 reports • Other independent third-party security testing to review the effectiveness of administrative and technical controls.
49.	Art. 17 (V)(c)	information and management resources suitable for monitoring the services to be provided, mentioned in art. 12, item II, item "f";	• Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies • Section 11 Schedule C • Section 11 CSA	**Section 3.2.2 of the** Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability. **Section 11.1 of Schedule C and Section 11.1 of the CSA, as applicable,** explains that Oracle also continuously monitors the Cloud services.
50.	Art. 17 (VI)	the obligation of the contracted company to notify the contracting institution about the subcontracting of services relevant to the institution;	• Section 6 FSA • Section 6.2 FSA • DPA	Per **Section 6 of the FSA** Oracle may use subprocessors or strategic subcontractors for some of its cloud services. Oracle reviews all such subcontractors that provide services to Oracle as part of its cloud services according to a published criteria to determine the status of such subcontractors. Oracle publishes a list of its subprocessors and strategic subcontractors to customers through My Oracle Support. **Section 6.2 of the FSA** include terms applicable to Oracle's use of subprocessors and strategic subcontractors, and similar to the

				Oracle Data Processing Agreement, includes a right for a customer to object to the intended involvement of a new strategic subcontractor.
51.	Art. 17 (VII)	the permission of the Central Bank of Brazil to access contracts and agreements signed for the provision of services, documentation and information regarding the services provided, stored data and information about their processing, data backups and information, as well as data and information access codes;	• Section 2 FSA	Please refer **Section 2** (Regulator Audit Rights) **of the FSA,** which grants customer's regulators the same rights of access and audit as for its customers.
52.	Art. 17 (VIII)	the adoption of measures by the contracting institution, as a result of determination of the Central Bank of Brazil; and		This is primarily a customer consideration.
53.	Art. 17 (IX)	the contracted company's obligation to keep the contracting institution permanently informed about any limitations that may affect the provision of services or compliance with legislation and regulations in force.	• Section 8.2 DPA • Section 15.2 CSA • Section 13.2 Schedule C • Section 3.2.2 of the Oracle Cloud Hosting and Delivery Policies • Section7 FSA	Refer to **Section 8.2 of the** Oracle Data Processing Agreement where it identifies that customers would be notified of a personal information breach without undue delay within 24 hours. **Section 15.2 of the CSA** and **Section 13.2 of Schedule C** discusses party notification requirements generally and how Oracle provides notices about the services via the customer portal. **Section 3.2.2 of the** Oracle Cloud Hosting and Delivery Policies indicates that Oracle will provide customers with access to a customer notifications portal for monitoring their Cloud service availability. **Section 7 of the FSA** addresses notification affecting service provisions.
54.	Art. 17 ¶1	The contracts mentioned in the heading must provide, in the case of the enactment		

		of the contracting institution's resolution regime by the Central Bank of Brazil:		
55.	Art. 17 ¶1(I)	the obligation of the contracted company to grant full and unrestricted access to the person responsible for the resolution regime to contracts, agreements, documentation and information regarding the services provided, stored data and information about their processing, backup copies of the data and information, as well as the access codes mentioned in item VII of the heading that are in the possession of the contracted company;	• Section 4.1 FSA • Section 6.1 of the Oracle Cloud Hosting and Delivery Policies • Section 7 DPA • Section 9 DPA • Section 9.4 Schedule C • Section 9.5 CSA • Section 2.4 FSA • Section 9 FSA	**Section 4.1 of the FSA** explains that Oracle will provide reasonable assistance to customers during the retrieval period to enable them to retrieve their content from the production services environment. Also see **Section 6.1 of the** Oracle Cloud Hosting and Delivery Policies**, Sections 7 and 9 of the** Oracle Data Processing Agreement**, Section 9.4 of Schedule C and Section 9.5 of the CSA**, as applicable, where Oracle also agrees to make personal information and content available for retrieval by the customer. **Section 2.4 of the FSA** acknowledges the information gathering and investigatory powers of Resolution Authorities. **Section 9 of the FSA** addresses the parties' rights and responsibilities in the event of a Resolution Event, including suspension of Oracle's termination rights and obligation to continue provision of the cloud services during the standstill period.
56.	Art. 17 ¶1(II)	the obligation to notify the person responsible for the resolution regime in advance on the contracted company's intention to interrupt the provision of services, with at least thirty days in advance of the scheduled interruption date, provided that:	• Section 9.1 FSA • Section 9.2 FSA	**Section 9.1 of the FSA** describes the customer's right to exercise a stay of termination of the cloud services following the occurrence of a resolution event, with proper notice to Oracle. Under **Section 9.2 of the FSA**, Oracle will continue to perform the cloud services during a Resolution Event and will provide assistance as requested by customer or it's Resolution Authority.
57.	Art. 17 ¶1(II)(a)	the contracted company undertakes to accept any request for an additional period of thirty days for the interruption of the service, made by the person responsible for the resolution regime; and	• Section 9 FSA	**Section 9 of the FSA** addresses the parties' rights and responsibilities in the event of a Resolution Event, including suspension of Oracle's termination rights and obligation to continue provision of the cloud services during the standstill period.

58.	Art. 17 ¶1(II)(b)	the prior notification must also occur in the situation in which the interruption is motivated by default by the contractor.	See row 57 above.	See row 57 above.