ORACLE

Oracle Contract Checklist for Mexico CNBV Requirements for Credit Institutions (LIC/CUB)

October 2025 | Version 1.0

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 requirements.

The information in this document was current as of October 1, 2025

Overview

Oracle has developed this document to help financial services customers in Mexico review Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications (SaaS)[1] in the context of the *Ley de Instituciones de Crédito* **("LIC")** and *Disposiciones de Carácter General Aplicables a las* instituciones de Crédito **("CUB")** issued by the Comisión Nacional Bancaria y de Valores *("*CNBV*").* We want to make it easier for you as a financial institution to identify the sections of the Oracle Cloud services contract that may help you address the requirements in the applicable aforementioned CNBV regulation. In this document, you will find a list of specific requirements under each regulation, along with a reference to the relevant section(s) of the Oracle Cloud services contract and a short explanation to help you conduct your 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 agreement** – 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 **Oracle Data Processing Agreement**

Regulation Background

The CNBV is Mexico's primary banking regulator. The CNBV has issued regulations applicable to IT sourcing for credit institutions. These guidelines include (but are not limited to) contractual, technical, compliance, security, and operational requirements applicable to financial institutions when outsourcing IT services to companies such as cloud providers. The purpose of these regulations is to ensure the continued stability and security of the banking and financial sector as the outsourcing of technology operations becomes more pervasive. For a complete list of regulatory requirements, see LIC and CUB.

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

NO.	CREDIT INSTITUTIONS REG REFERENCE	REGULATION REQUIREMENT/DESCRIPTION	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT/RESOURCE	ORACLE EXPLANATION
	LIC/CUB			

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

1.	LIC Art. 46 Bis. 1	The CNBV, subject to the Institution's right of audience, may order the total or partial, temporary of definitive suspension of the outsourced services rendered by the third-party provider in case the provisions of these requirements are breached or if the operational continuity of the Institution may be affected or in order to protect the public interest, unless the CNBV approved a regularization program that meets the requirements set forth in the general provisions issued by CNBV.	• Section 2 FSA • Section 3 FSA	**Section 2 of the FSA** provides audit rights for the customer's regulators. Section 2.7 of the FSA, in particular states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law. Under **Section 3 of the FSA**, customers have the right to terminate the cloud services in the following situations: Termination due to regulatory requirements - Continued use of the services would cause customers to violate applicable law and regulation upon the conclusion made by the regulator. - Termination requested based on express instruction issued by the regulator where the services are considered as an impediment to effective supervision over the customer.
2.	LIC Art. 46 Bis. 1	The CNBV will make directly to the Institutions, all information requirements, observations and corrective measures that may result from its supervision of activities outsourced by the Institutions, in order to ensure the continuity of services provided by the Institutions to their clients, the information integrity and compliance to applicable regulations. Furthermore, the CNBV shall have the authority to carry out, at any time, supervision and inspection actions with respect to third-party providers, and to conduct audits to the third parties hired by the Institutions relating to the outsourced activities, or to order Institutions to conduct such audits to third parties, as to which the	• Sections 7 and 8 DPA • Oracle Cloud Hosting and Delivery Policies • Oracle SaaS Public Cloud Services Pillar Document • Oracle PaaS and IaaS Public Cloud Services • Section 2 FSA • Section 2.1 FSA	Oracle provides several resources to assist its customers in conducting necessary risk assessments and due diligence. Oracle provides customers with access to security questionnaires (CAIQ), audit reports, and other information regarding Oracle's operational and security practices. Customers can access these materials through the Oracle Compliance site and other sites specified below. Customers can access these materials through the **Oracle Cloud Compliance site** , **Oracle Corporate Security Practices**, and **Oracle Cloud Hosting and Delivery Policies.** CAIQs: • OCI CAIQ: **oracle.com/a/ocom/docs/oci-corporate-caiq.pdf** • Oracle Fusion Cloud Applications CAIQ: **oracle.com/a/ocom/docs/caiq-oracle-fusion-cloud-applications.pdf**

		Institutions must submit the corresponding report.		• Oracle Cloud Applications CAIQ: oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf • **Technical and organization security measures:** - **Section 7** – 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 • **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. **Section 8** (Audit Rights) **of the** Oracle Data Processing Agreement stipulates Oracle will cooperate with regulator audits with Oracle's obligation under applicable laws. Please refer to **Section 2** (Regulator Audit Rights) **of the FSA.** **Section 2.1 of the FSA** grants customer's regulators the same rights of access and audit for Oracle's Strategic Subcontractors.
3.	LIC Art. 46 Bis 1	The CNBV must specify the subject matter of any inspections or audits, which in any case must refer to the outsourced service. The relevant services contracts must include the agreement of the third party to comply with the provisions of the regulation.	• Section 14 CSA • Section 13 OMA • Section 2 and 8 FSA • Section 8 DPA	**Section 14 of the CSA** and **Section 13 of the OMA** General Terms sets out the governing law and jurisdiction of the agreement. **Section 2** (Regulator Audit Rights) **of the FSA.** See also **Section 8 of the FSA** – Compliance with Laws **Section 8** (Audit Rights) **of the** Oracle Data Processing Agreement stipulates

4.	LIC Art. 46 Bis. 2 CUB Art. 329	Outsourcing of services shall not release the Institutions or their officers, employees, representatives or agents, of their obligations to comply with the applicable regulation.		This is primarily a customer consideration. However, see **Section 8 of the FSA** regarding Oracle's compliance with Laws
5.	LIC Art. 46 Bis 2	The CNBV may request the service providers, through the Institution, information, including books, records and documents related to the outsourced services, as well as to conduct inspection visits and order measures to be implemented by the Institutions to ensure the continuity of the services provided by the Institutions to their clients, the information integrity and compliance to applicable regulation.	See row 2 above.	See row 2 above.
6.	CUB Art. 318	Institutions that intend to hire a third party to provide any services, must comply with the following requirements:		
7.	CUB Art. 318(II)	Produce a report that specifies the operational or databases and IT systems administration processes of the Institution that are the subject matter of the services to be outsourced, as well as the policies and criteria for selecting the third-party provider, which shall be aimed at evaluating the experience, technical capacity and human resources of the third party to be hired to provide the service with adequate levels of performance,		This is primarily a customer consideration, however, Oracle provides products and services that address enterprise information technology (IT) environments. Our products and services include applications and infrastructure offerings that are delivered worldwide through various flexible and interoperable IT deployment models. Our customers include businesses of many sizes, government agencies, educational institutions, and resellers. Using Oracle technologies, our customers build, deploy, run, manage, and support their internal and external products, services, and business operations. • About Oracle Corporation: oracle.com/corporate/ • Oracle Corporate Facts: oracle.com/corporate/corporate-facts.html

		reliability and safety, as well as the effects that may be produced in one or more operations carried out by the Institution.		
8.	CUB Art. 318(II)	The policies and criteria mentioned above, shall be prepared by the CEO or other officer appointed by the CEO and shall be approved by the Board of Directors of the Institution, proposed by the Risk Committee or Audit Committee. The Audit Committee shall be responsible to verify implementation of such policies and criteria.		This is a customer consideration.
9.	CUB Art. 318(III)	**Include within the services agreement or any other ancillary document the unconditional acceptance of the third-party provider to expressly:**		
10.	CUB Art. 318(III)(a)(1)	Receive supervisory visits from the Institution's external auditor, the CNBV or any third party designated by the CNBV in order to carry out such supervisory visits, with the purpose of obtaining information to verify that the outsourced services allow the Institution to comply with the applicable regulatory provisions. The Institution may appoint a representative to carry out such visits.	• Section 8 DPA • Section 1 FSA • Section 2 FSA	**Section 8** (Audit Rights) **of the** Oracle Data Processing Agreement stipulates Oracle will cooperate with regulator audits with Oracle's obligation under applicable laws. Please refer to **Section 1** (Customer Audit Rights) **of the FSA** Please refer **Section 2** (Regulator Audit Rights) **of the FSA.**
11.	CUB Art. 318(III)(a)(2)	Allow the Institution to conduct audits in connection with the outsourced services, in order to verify compliance with regulatory	See row 10 above.	See row 10 above.

		provisions applicable to the Institution.		
12.	CUB Art. 318(III)(a)(3)	Deliver upon request of the Institution, to the Institution's external auditor and to the CNBV or any third party designated by the CNBV, all books, systems, records, manuals and documents in general, related to the provision of the relevant service. Also allow access to the responsible staff and to its offices and premises in general, related to the provision of the relevant service.	See row 10 above.	See row 10 above.
13.	CUB Art. 318(III)(a)(4)	Notify the Institution at least thirty calendar days in advance of any modification to its corporate purpose or its internal organization, which affects the provision of the relevant services.	• Section 7 FSA	Per **Section 7 of the FSA,** service notifications and alerts relevant to cloud services are posted on this portal and include notification of circumstances that can reasonably be expected to have a material impact on the provision of cloud services.
14.	CUB Art. 318(III)(a)(5)	To keep as confidential, the information that is received, transferred, processed or stored during the services. Also, to accept that such information can only be used and exploited for the services purposes. Confidentiality shall also be applicable to the third-party provider's representatives, officers and employees, even when they stop working or ceased to provide services to the third-party provider.	• Sections 7 DPA • Sections 4 and 5 Schedule C • Section 4 and 5 CSA • Oracle Cloud Hosting and Delivery Policies • Oracle SaaS Public Cloud Services Pillar Document • Oracle PaaS and IaaS Public Cloud Services Pillar Document	• **Technical and organization security measures:** - **Section 7** – 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

15.	CUB Art. 318(III)(a)	Provisions in row 10 - 14 above shall also be applicable to third parties with whom the third-party provider subcontracts, directly, the Services, totally or partially.	• Section 5.1 DPA • Section 6 FSA • Section 6.1 FSA • Section 6.2 FSA • Section 1.1 FSA • Section 2.1 FSA	**Section 5.1 of the Oracle Data Processing Agreement** indicates that, to the extent Oracle engages third party subprocessors and/or Oracle affiliates to process personal information, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Oracle Cloud services contract. This section also indicates that Oracle is responsible for the performance of the Oracle affiliates and third party subprocessors' obligations in compliance with the terms of the **Oracle Data Processing Agreement** and applicable data protection law. Per **Section 6 of the FSA** Oracle may use subprocessors or strategic subcontractors for some of its cloud services. Oracle reviews all of its 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 (collectively "subcontractors") to customers through My Oracle Support. **Section 6.1 of the FSA** further indicates that all subcontractors with access to customer content will be subject to the same level of data protection and security as Oracle under the terms of the Oracle Cloud services contract. In addition, under this section, Oracle agrees to enter into written agreements with subcontractors reflecting obligations that are consistent with Oracle's obligations under the relevant terms of the Oracle Cloud services contract. Any such subcontracting will not diminish Oracle's responsibility towards its customers under Oracle Cloud services contracts and Oracle will appropriately oversee a subcontractor's performance. **6.2 of the FSA** include terms applicable to Oracle's use of subcontractors 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. **Section 1.1 of the FSA** grants customer the same rights of access and audit for Oracle's Strategic Subcontractors. **Section 2.1 of the FSA** grants customer's regulators the same rights of access and audit for Oracle's Strategic Subcontractors.

16.	CUB Art. 318(III)(b)	**In addition to the provisions above, the services agreement or any other ancillary document shall provide:**		
17.	CUB Art. 318(III)(b)(1)	Restrictions or conditions with respect to the possibility that the third-parties, in turn, subcontract the provision of services, including notification to the Institution.	• Section 6 FSA • Section 6.2.2 FSA • Section 5 DPA	Please refer to **Section 6 of the FSA** regarding subcontracting. **Section 6.2.2 of the FSA** includes 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 within 30 days. See also **Section 5** of the **Oracle Data Processing Agreement.**
18.	CUB Art. 318(III)(b)(2)	Obligations that correspond to the Institution and third-party providers, as well as procedures to supervise compliance thereof, as well as indemnities for non-compliance.	• Section 3.2.2 & 3.4 of the Oracle Cloud Hosting and Delivery Policies • Section 11 Schedule C • Section 11 CSA • Section 9.2 DPA • Section 15.2 CSA • Section 13.2 Schedule C • Section 7 FSA	**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. Refer to **Section 9.2 of the Oracle Data Processing Agreement** where it identifies that customers would be notified of an 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 7 of the FSA** addresses notification affecting service provisions.

				Depending on the service infrastructure type and notification scenario (Outage, Maintenance, Informational, Action Required), Oracle provides several different communication channels used for customer notifications including through My Oracle Support https://ocistatus.oraclecloud.com/, https://saasstatus.oracle.com/, and OCI Console.
19.	CUB Art. 318(III)(b)(3)	Mechanisms for the solution of disputes related to the service agreement.	• Section 10 FSA	See **Section 10 of the FSA** with regards to Dispute Resolution.
20.	CUB Art. 318(III)(b)(4)	Obligations and responsibilities of the parties to protect the information of the clients of the Institution, which shall consider the requirements established in the legislation for protection of personal data regarding the processing and transfer of this type of data, as well as the one related to the defense of financial services users and any other that its objective is to protect the data of the clients of the Institution.	• Section 7 DPA • Section 5.1 DPA • Section 1.7 of the Oracle Cloud Hosting and Delivery Policies • Section 5 CSA • Section 5 Schedule C	**Section 7 of the Oracle Data Processing Agreement** states that Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Information. **Section 5.1 of the Oracle Data Processing Agreement** indicates that, to the extent Oracle engages third party subprocessors and/or Oracle affiliates to process personal information, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Oracle Cloud services contract. This section also indicates that Oracle is responsible for the performance of the Oracle affiliates and third party subprocessors' obligations in compliance with the terms of the **Oracle Data Processing Agreement** and applicable data protection law. 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. **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.

21.	CUB Art. 318(III)(b)(5)	Express provision that the Institution will, at all times, take responsibility for the outsourced services provided to their customers, even when the corresponding services do not comply with the Agreement; as well as for any breach of the applicable CNBV regulation incurred by third-party providers.	• Section 7 CSA • Section 8 CSA • Section 7 Schedule C • Section 8 Schedule C	See **Section 7 & 8 of the CSA** and **Section 7 & 8 of Schedule C** regarding liability.
22.	CUB Art. 318(III)(b)(6)	Terms, conditions and procedures for the third-party provider to guarantee to the Institution the secure transfer, return and deletion of the information once the service is ceased to be provided.	• Section 4.1 and 4.3 FSA • Oracle SaaS Cloud Services Pillar Document (Section 6) • Section 10.1 DPA • Section 9.5 CSA • Section 9.4 Schedule C • Oracle Cloud Hosting and Delivery Policies (Section 6.1)	**Section 4.1 of the FSA** addresses data retrieval upon termination. **Section 4.3 of the FSA** addresses customers who require assistance with a transition. Per **Section 6 of the SaaS Cloud Services Pillar Document,** following the end of the Services Period and any applicable data retrieval period, upon Your request, Oracle will provide a confirmation when Your Content has been deleted. **Section 10.1 of the Oracle Data Processing Agreement** confirms that, on termination of an arrangement, Oracle will promptly return or delete any remaining copies of personal data, except as otherwise stated in the Oracle Cloud services contract. **Section 9.5 of the CSA and Section 9.4 of Schedule C** states at the end of the Services Period, Oracle will make Your Content (as it existed at the end of the Services Period) available for retrieval by customer during a retrieval period set out in the Service Specifications. See also, **Section 6.1 of the Oracle Cloud Hosting and Delivery Policies** - Termination of Oracle Cloud Services
23.	CUB Art. 318(III)(b)(7)	Establish corrective measures for breaches of the CNBV regulations from third-party service providers.	• Section 9.3 Schedule C • Section 9.4 CSA • Oracle SaaS Cloud Services Pillar Document (Section 3)	See **Section 9.4 of the CSA** and **Section 9.3 of Schedule C** regarding corrective actions for breaches. See **Section 3 of the PaaS/IaaS Cloud Services Pillar Document** or the **SaaS Cloud Pillar Document**, as applicable.

			• Oracle PaaS/IaaS Cloud Services Pillar Document (Section 3)	
24.	CUB Art. 318(IV)	Establish guidelines and mechanisms tending to an unaffected and adequate provision of their services to the public or the financial stability or operational continuity of the Institutions after termination of the service agreement with the third-party provider, considering those necessary to verify that such third-party provider does not maintain any information from the Institution or its customers.	• Section 4.2 FSA • Section 4.3 FSA	Under **Section 4.2 & 4.3 of the FSA**, in the event You require assistance with a transition (whether to another service provider or to Your own organization), You may request additional professional services from Oracle ("Transition Assistance Services"), and Oracle will enter into good faith negotiations with You 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.
25.	CUB Art. 318(V)	Compliance with minimum operational and safety guidelines indicated in Exhibits 52 and 58 of the CUB or Exhibit 12 of the CUCB, as applicable, for the operation of electronic means with third party providers or if the services to be outsourced refer to the use of technological infrastructure or telecommunications.	See row 2 above.	See row 2 above.
26.	CUB Art. 318(VI)	Verify that third parties, their shareholders and, if applicable, subcontractors, as well as the commissioners and their shareholders, if applicable, the Administrator of these commissioners and the shareholders of the later, are not included in the official lists issued		Oracle performs background checks on candidates for hire in accordance with local laws and regulations as well as local Oracle policy. Employees are required to complete the Ethics and Business Conduct, Information Protection Awareness, and the Anti-Corruption and Foreign Corrupt Practices Act online courses upon hire. Oracle employees are also required to complete annual security awareness training in accordance with the Information Security Policy, which outlines the process and procedures to report incidents.

		by Mexican authorities, international agencies, intergovernmental groups or foreign authorities, of people related with transactions involving illegally sourced funds, terrorism or financing, or other illegal activities. In order to prove the above, it will suffice that the Institution states in writing that the listed persons were not related with such official listings at the time of the contract. Additionally, the Institution shall state that it knows the business carried out by the commissioners.		For more information, see • Oracle Background Check process: https://www.oracle.com/corporate/careers/background-check.html#apac • Oracle Human Resources Security: https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html • Oracle Supply Chain Security and Assurance: https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
27.	CUB Art. 318(VII)	A Credit Institution must have previous approval of the Board or from the Risk Committee of the Institution to evaluate the extent to which the outsourcing of services could qualitatively or quantitatively affect the operations carried out by the Institution, according to its purpose and considering the following:	[redacted]	[redacted]
28.	CUB Art. 318(VII)(a)	The Institution's ability to maintain operational continuity and to carry out operations and services with its clients in case of contingency.	• Section 5 FSA • Section 2 Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document (particularly section 2)	For each critical line of business, Oracle maintains a business continuity plan that includes a business impact analysis (BIA), risk assessments, and disaster recovery contingency plans. The plans align with Oracle's Risk Management and Resiliency Program policy, which requires the plans to outline procedures, ownership, roles, and responsibilities to be followed if a business disruption occurs. These plans are reviewed and tested annually. See **Oracle Risk Management Resiliency Business Continuity**

			• SaaS Cloud Services Pillar Document (Section 2)	**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. Upon at least 30 days' notice by You no more than once per calendar year, Oracle will make available to You via web conference or on Oracle premises, in a guided manner, a summary of the BCP Program and applicable test information, material modifications to the BCP Program within the last 12 months and pertinent BCP governance areas, and confirmation that an internal review of these governance areas was performed within the last 12 months. Additionally, please see the Oracle Cloud Service Continuity Policy in **Section 2 of the** Oracle Cloud Hosting and Delivery Policies. **Section 2 of the** Oracle Paas and Iaas Public Cloud Services Pillar Document **Section 2 of the** SaaS Cloud Services Pillar Document addresses cloud service continuity.
29.	CUB Art. 318(VII)(b)	The complexity and timing required to find a third party that, if necessary, replaces the original third-party provider.	• Section 4.3 FSA	This is primarily a customer consideration, however, please see **Section 4.3 of the FSA** regarding transition assistance.
30.	CUB Art. 318(VII)(c)	The ability of the Institution to maintain appropriate internal controls and timeliness of the accounting recording, and to comply with regulatory requirements in case of suspension of the service by the third-party provider.	• Section 9 FSA • Section 9 CSA • Section 9 Schedule C • Oracle Cloud Hosting and Delivery Policies (Section 6) • Oracle SaaS Cloud Services Pillar Document (Section 6)	This is primarily a customer consideration, however, please refer to **Section 9 of the FSA**, **Section 9 of the CSA,** and **Section 9 of Schedule C** regarding suspension of services. See also, **Section 6.1 of the** Oracle Cloud Hosting and Delivery Policies – Suspension of Oracle Cloud Services See **Section 6 of the** PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, as applicable.

			• Oracle PaaS/IaaS Cloud Services Pillar Document (Section 6)	
31.	CUB Art. 318(VII)(d)	The impact that any suspension of the service would have on the financing situation, reputation and operations of the Institution.		This is a customer consideration.
32.	CUB Art. 318(VII)(e)	The vulnerability of the information related to the clients.		Please see row 5 above regarding security and confidentiality.
33.	CUB Art. 318(VII)	The Institutions shall establish policies for the adequate management, control and security of the information that is generated, received, transferred, processed or stored in the execution of the services that refer to the usage of technological infrastructure, telecommunications or processing of data, that is carried out, partially or totally, outside of national territory (Mexico). The establishment of such policies shall be responsibility of the CEO who might delegate such tasks to the areas in charge of the security of the information of the Institution, while the Audit Committee and the internal auditor of the Institution shall be responsible to watch over its compliance, in accordance with their respective scopes.		This is primarily a customer consideration, however, please refer to row 5 above.

34.	CUB Art. 318 Bis.	All information requirements, and if applicable, observations and corrective measures that derive from the supervision activities carried out by the CNBV under the CUB, will be made directly to the Institution. Furthermore, the CNBV may, at any time, order the performance of the visits and audits indicated in the CNBV regulations, indicating any and all aspects to be contemplated therein, and the Institution must submit to the CNBV a report thereof.	See row 10 above.	See row 10 above.
35.	CUB Art. 318 Bis.1	At least once every two years, the Institution must conduct audits that have the purpose to verify the degree of compliance with these requirements, as applicable, when it deals with commissions to perform operations referred to in these regulations, or for the provision of services to perform operational processes, administration of databases or informatic systems, as well as of the infrastructure, controls and operations of the computing center of the third-party provider. Notwithstanding the foregoing, the CNBV may order the performance of such audits at any time, when the CNBV considers that there are risk conditions regarding operation and information security.	See rows 10 & 18 above.	See rows 10 & 18 above.
36.	CUB Art. 326/327	**Institutions that intend to hire a third party to perform any**		

		operational process or to manage databases or IT systems must notify the CNBV at least 20 days business days in advance. The notification/authorization should include:		
37.	CUB Art. 326/327	The notification/authorization must be signed by the Institution's CEO. If the services to be outsourced relate to the use of technological or telecommunications infrastructure, the notification must also include a technical report specifying the type of transactions or services to be executed using the technological platform provided by the third party and explaining how minimum operational and security requirements will be complied with.		This is a customer consideration.
38.	CUCB Art. 326/327	A draft of the services agreement, indicating the estimated date of execution.	• CSA • Ordering Document • Schedule C • DPA • Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services Pillar Document	The 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: - **Oracle Data Processing Agreement** - **Oracle Cloud Hosting and Delivery Policies** - **PaaS/IaaS Cloud Services Pillar Document** - **SaaS Cloud Services Pillar Document**

39.	CUB Art. 328	The Institutions require the authorization from the CNBV (CNBV) to hire a third party to perform any operational process or to manage databases or IT systems, if the relevant services were to be rendered or executed partially or totally outside Mexico of by foreign residents, regardless of whether the relevant processes may or may not affect in a qualitative or quantitative manner one or more of the operations that the Institution performs.	• Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services Pillar Document	This is primarily a customer consideration, however, 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 Services Pillar Document.**
40.	CUB Art. 328	Institutions shall request CNBV's authorization at least 20 business days in advance. The request for authorization must comply with the same requirements set forth in Articles 326 and 327 of the CUB for the Notification to the CNBV, and must include documentation evidencing compliance with requirements set forth in Article 318 of the CUB, as well as the following:	[redacted]	[redacted]
41.	CUB Art. 328(I)	The third-party provider is a resident of a country which laws provide for personal data protection, securing confidentiality, or the residence country of the third-party provider has international agreements with Mexico regarding personal data protection and information exchange among regulators of financial institutions.		Oracle Corporation is organized under the laws of the State of Delaware in the USA, where protection of data is regulated by laws enacted on both the federal and the state level.

42.	CUB Art. 328(II)	That the Institution warrants that they maintain at their principal offices in Mexico, and at least the documents and information related to the evaluations, audit results and performance reports. Also, if required by the CNBV, such information shall be delivered in Spanish.		This is a customer consideration.
43.	CUB Art. 328(III)	That the Institution has obtained the approval from its Board of Directors, or, if applicable, its Audit Committee of risk committee, which approval must provide for: (a) hiring the services does not pose a risk as to the adequate compliance of provisions applicable to the Institution, (b) that the third-party provider's practices are consistent with the operation of the Institution, (c) that the services will not affect the financial stability or operations continuity of the Institution due to the geographical distance, and, if applicable, the language used in the provision of services, and (d) measures to be implemented in case the operations of the Institution may be affected qualitatively or quantitatively as a result of the outsourcing of services, in any aspect listed in paragraph VII of Article 318 of the CUB.		This is a customer consideration.

44.	CUB Art. 328	The CNBV may require the Institution to provide a draft of the services agreement and a copy of the executed version, with a Spanish translation.	• CSA • Ordering Document • Schedule C • DPA • Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services Pillar Document	This is primarily a customer consideration, however the 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: - **Oracle Data Processing Agreement** - **Oracle Cloud Hosting and Delivery Policies** - **PaaS/IaaS Cloud Services Pillar Document** - **SaaS Cloud Services Pillar Document**
45.	CUB Art. 329	Operations carried out by the Institutions through outsourcing must comply with applicable regulations.	• Section 14 CSA • Section 13 OMA • Section 8 FSA	**Section 14 of the CSA** and **Section 13 of the OMA** General Terms sets out the governing law and jurisdiction of the agreement. See also **Section 8 of the FSA** – Compliance with Laws
46.	CUB Art. 329	The Institution's CEO or the person appointed by the latter, shall be responsible for filing the notice referred to in article 326		This is a customer consideration.
47.	CUB Art. 329	The CNBV may order measures it considers necessary so that the Institutions maintain operational terms and conditions that do not affect the adequate provision of their services to the public or the financial stability or operational continuity of the Institutions.	• Section 2.7 FSA	**Section 2.7 of the FSA**, states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law.
48.	CUB Art. 331	The Institutions shall suspend services provided through any third-party, when Institutions	• Section 9 FSA • Section 9 CSA	please refer to **Section 9 of the FSA**, **Section 9 of the CSA,** and **Section 9 of Schedule C** regarding suspension of services.

		become aware of changes in the operations of such third-party which could affect in a qualitative or quantitative manner the terms and conditions of the services contract, or of any breach by the third-party of the applicable regulation.	• Section 9 Schedule C • Oracle Cloud Hosting and Delivery Policies (Section 6) • Oracle SaaS Cloud Services Pillar Document (Section 6) • Oracle PaaS/IaaS Cloud Services Pillar Document (Section 6)	See also, **Section 6.1 of the** Oracle Cloud Hosting and Delivery Policies – Suspension of Oracle Cloud Services See **Section 6 of the** PaaS/IaaS Cloud Services Pillar Document or the SaaS Cloud Pillar Document, as applicable.
49.	CUB Art. 332	The CNBV, subject to the Institution's right of audience, may order the total or partial, temporary or definitive, suspension of the outsourced services rendered by the third-party provider when in the CNBV's judgment, the financial stability, the security of the information of the clients or of the Institution, the operational continuity of the Institution or in order to protect the public interest, or in case the Institution breaches any applicable regulations, including the provisions set forth in the CUB. The aforementioned, unless the Institution submits a regularization program that meets certain requirements set forth in Article 332 of the CUB, and such program is approved by the CNBV, within 30 non-business days, from the date the Institution submits the		**Section 2.7 of the FSA**, states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law. See also row 48 above.

		corresponding authorization, to resolve accordingly.		
50.	CUB Article 168 Bis 11	The Director(s) of the Credit Institution will be responsible for the implementation of the internal control system regarding Information Security that ensures confidentiality, integrity, and availability. Audit records should be kept a minimum of three years.		This is a customer consideration. Oracle Cloud Applications maintains audit security logs for a minimum of 3 years.
51.	CUB Article 168 Bis 12	The general director of the Institution shall be responsible for compliance with the following obligations in relation to the Technological Infrastructure: I.Approve the Security Master Plan, which must be aligned with the business strategy of the Institution, as well as define and prioritize the projects in matters of information security, with the objective of reducing the exposure to technological risks and the materialization of Information Security Incidents to acceptable levels under the terms defined by the Board, based on an analysis of the current situation II. Carry out security reviews, focused on verifying the adequacy of the controls applicable to the Technological Infrastructure.		This is a customer consideration.

		III. To draw up an annual schedule for the performance of vulnerability scanning tests of the components of the Technological Infrastructure that store, process or transmit information, prioritizing them according to the result of the information classification exercise referred to in Article 86, section III, subsection b), paragraph 3. IV. To hire an independent third party, with personnel who have proven technical capacity through specialized industry certifications in the field, to perform penetration tests on the different systems and applications of the Institution in order to detect errors, vulnerabilities, unauthorized functionality or any code that puts or may put at risk the information and assets of customers and of the Institution itself. V. Classify the vulnerabilities detected in accordance with the methodology approved by the risk committee. VI. Develop remediation plans with respect to the findings of the reviews and tests referred to in sections II, III and IV above, considering the classification of section V of this article, as well as implement defense mechanisms that prevent unauthorized access		

		and use of the Technological Infrastructure. VII. Implement follow-up processes for compliance with the remediation plans referred to, which shall be verified by the chief information security officer. VIII. Implement the annual training programs referred to in Section V of Article 69 of these provisions, as well as the information security awareness programs, directed to all personnel and clients, including, if applicable, third parties that provide services, in which, among other aspects, the roles and responsibilities that the Users of the Technological Infrastructure have in this respect are contemplated. IX. Carry out, in a proactive and iterative manner, the search for fraud alerts, as well as threats, such as fraudulent e-mail campaigns, fake Internet sites, disclosure of databases with information of the Public User, alteration of ATMs or point-of-sale terminals and identity theft, among others, that could affect the security of the information of the Public User, as well as actions for its protection X. Implement controls that allow the Institution to ensure the confidentiality, integrity and availability of the information of the		

		Public User and the Institution itself or the access to the Technological Infrastructure, by its employees or personnel that have access to it, that guarantee that such information and Technological Infrastructure are not altered or cause an affectation to the Institution or to the resources of its clients. Said controls must be implemented from the respective contracting and until its termination.		
52.	CUB Article 168 Bis 16	Financial Institutions must notify the CNBV of Information Security Incidents within 15 days. In the event of an Information Security Incident that meets any of the requirements referred to in paragraphs a) to d) of Section I of this Article in: (i) the components of the Technological Infrastructure of the Institution; (ii) the channels of attention to the public, such as Electronic Media, Banking Offices or commission agents of the Institution or, (iii) the technological infrastructure of any third party that affects the operation or the Technological Infrastructure of the Institution, the general director of the Institution shall: I. Provide for the necessary measures to immediately notify the Commission of the Information Security Incidents, by means of e-mail sent		This is a customer consideration.

		to the account CiberseguridadCNBV@cnbv.gob.mx or through other means indicated by the Commission itself, generating an electronic acknowledgment of receipt.		
53.	CUB Article 168 Bis 17	Credit Institutions must keep records of information security incidents for at least 10 years.		This is a customer consideration.