ORACLE

Oracle Contract Checklist for Mexico CNSF Requirements for Insurance and Surety Institutions Under the LISF and CUSF

March 2023 | 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 requirement*s*.

The information in this document was current as of March 1, 2023

Overview

Oracle has developed this document as a part of its continuing efforts to help insurance customers in Mexico meet their obligations, particularly under the Ley de Instituciones de Seguros y de Fianzas, ("LISF") and Circular Única de Seguros y Fianzas ("CUSF") issued by the Comision Nacional de Seguros y Fianzas ("CNSF") relating to the use of Oracle Cloud Infrastructure (OCI) and Oracle Cloud Applications (SaaS)[1]. We want to make it easier for you as an insurance institution to identify the sections of the Oracle Cloud contract that may help you address the requirements in the LISF and CUSF. In this document, you will find a list of specific requirements under the LISF and CUSF along with a reference to the relevant section(s) of the Oracle Cloud contract and a short explanation to help you conduct your review of OCI and Oracle Cloud Applications (SaaS).

The Oracle Cloud 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) {Remove if addressing other industries}
- **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)
- Oracle Data Processing Agreement

Regulation Background

The CNSF is Mexico's primary insurance regulator. The LISF and CUSF issued by the CNSF, includes (but is not limited to) contractual, technical, compliance, security, and operational requirements applicable to insurance institutions when outsourcing IT services to companies such as cloud providers. The purpose of these regulations are to ensure the continued stability and security of the insurance sector as the outsourcing of technology operations becomes more pervasive. For a complete list of regulatory requirements, see LISF and CUSF.

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

NO.	CNSF REGULATION REFERENCE (LISF OR CUSF)	REGULATION REQUIREMENT/DESCRIPTION	REFERENCE TO ORACLE CLOUD CONTRACT	ORACLE EXPLANATION

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

LISF				
1.	LISF Art. 268	The CNSF, subject to the Insurance Company's right of audience, may order the total or partial, temporary or definitive suspension of the outsourced services, in case the provisions of CUSF are breached, or if the operational continuity of the Insurance Company is affected, or in order to protect the public interest; unless the CNSF approves a regularization program that meets the requirements set forth in the LISF and CUSF.	• Section 3.1 FSA	Under **Section 3.1 of the FSA**, with 30 days prior written notice, customers may terminate the services agreement if instructed by regulator, Oracle is in breach of applicable law or regulation, Oracle's ability to perform the cloud services are impeded, material changes result in an adverse impact to cloud services, and/or weaknesses are found regarding security of customer content. During the thirty-day notice period, Oracle will use commercially reasonable efforts to address the concerns raised in termination notice.
2.	LISF Art. 268	The CNSF shall formulate directly with the Insurance Companies all information requirements and, if applicable, its observations and corrective measures that result from its supervision of the activities outsourced by the Insurance Companies; in order to ensure the continuity of the services provided by the Insurance Companies to their clients, the integrity of the information, and the compliance with applicable laws and regulations. Furthermore, the CNSF has the authority to carry out, at any time, supervision and inspection activities with respect to third-party providers, and to conduct inspection on such third parties that are hired by the Insurance Companies, or to order Insurance Companies to	• Sections 7 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 • Section 2 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 in the Resources column. 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 • Oracle Cloud Applications CAIQ: oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf • **Technical and organization security measures:**

		conduct such audits to the third parties and to issue the corresponding report.		- **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. Oracle enables its customers' regulators to carry out its supervisory functions in respect of the financial institutions. Such rights are addressed in the Oracle FSA as follows: **Section 2.1 of the FSA** further provides that a customer's regulator may audit Oracle as required by applicable law. **Section 2.4 of the FSA** explicitly acknowledges the information gathering and investigatory powers of resolution authorities. Please also refer to **Section 2.5 of the FSA,** which expressly states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law. Additionally, **Section 8** (Audit Rights) **of the** Oracle Data Processing Agreement stipulates Oracle will cooperate with regulator audits with Oracle's obligation under applicable laws.
3.	LISF Art. 268	The CNSF must specify the subject matter of any inspections or audits, which in any case must refer to the outsourced service, and applicable regulations. The relevant services contracts must include the agreement of the third party to comply with the provisions of Article 268 of the LISF.	• Section 2 FSA • Section 8 DPA • Section 14 CSA • Section 13 OMA • Section 8 FSA	Oracle enables its customers' regulators to carry out its supervisory functions in respect of the financial institutions. Such rights are addressed in the Oracle FSA as follows: **Section 2.1 of the FSA** further provides that a customer's regulator may audit Oracle as required by applicable law. **Section 2.4 of the FSA** explicitly acknowledges the information gathering and investigatory powers of resolution authorities. Please also refer to **Section 2.5 of the FSA,** which expressly states that Oracle will cooperate with a customer's regulator and provide reasonable assistance in accordance with applicable law.

				Additionally, **Section 8** (Audit Rights) **of the** Oracle Data Processing Agreement stipulates Oracle will cooperate with regulator audits with Oracle's obligation under applicable laws. **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
4.	LISF Art. 269	In order to comply with its corporate governance requirements, Insurance Companies must establish the policies and procedures for the outsourced services that are approved by their Board of Directors to guarantee that the operational functions related to their contracted activity with third parties complies with all the obligations established in the LISF and CUSF.		This is a customer consideration.
5.	LISF Art. 269	The above mentioned policies must establish the requirements set forth in this Article 269, in addition to the provisions set forth in Articles 268 and 269. Also, the CNSF has the authority to verify that the Insurance Companies' corporate governance system is in accordance with the terms of Article 269.		This is a customer consideration.
6.	LISF Art. 269	Outsourcing of services shall not release the Insurance Companies or their officers, employees, representatives or agents, of their obligations to comply with applicable laws and regulations.	• Section 8 FSA	This is a customer consideration. However, see **Section 8 of the FSA** regarding Oracle's compliance with Laws

7.	LISF Art. 269	The CNSF may request third-party providers, through the Insurance Companies, information, including books, records and documents, related to the outsourced services, as well as conduct inspection visits and order the implementation of measures to the Insurance Companies, to ensure the continuity of the services provided by such entities to their clients, the information integrity and compliance with applicable laws and regulations	See row 3 above.	See row 3 above.
CUSF				
8.	CUSF Art. 12.1.6	**Insurance Companies that hire a third party to provide any services, must include within the services agreement the following:**		
9.	CUSF Art. 12.1.6(I)	**The terms and conditions to guarantee the performance of the outsourced services:**	• CSA • Ordering Document • Schedule C • DPA • Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public 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

			• Oracle SaaS Cloud Services Pillar Document	
10.	CUSF Art. 12.1.6 (II)	Terms and conditions regarding the ownership, safeguarding and confidentiality of the information and resources handled by the third party, as well as clauses regarding the responsibilities of the third-party regarding the protection and backup of data, and the resources provided by the Insurance Company. These terms and conditions shall comply with what the applicable legal, regulatory and administrative provisions require to the relevant Insurance Company in this regard.	• Sections 7 and 9 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 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 - **Section 9** - Incident Management and Breach Notification – of the Oracle Data Processing Agreement
11.	CUSF Art. 12.1.6(III)	Terms and conditions regarding intellectual or industrial property rights, where appropriate, of the outsourced services.	• Section 3 CSA • Section 3 Schedule C	**Section 3 of the CSA** and **Section 3 of Schedule C** discusses ownership rights, intellectual property rights, and restrictions regarding customer content.
12.	CUSF Art. 12.1.6(IV)	Terms and conditions regarding the verification of the fulfillment of the outsourced services;	• 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.
13.	CUSF Art. 12.1.6(V)	Terms and conditions under which the third party will implement contingency plans to address problems in the performance of the contracted services;	• Section 5 FSA • Section 2 Oracle Cloud Hosting and Delivery Policies • Oracle Cloud Hosting and Delivery Policies (particularly sections 3.1 & 3.2) • Oracle PaaS and IaaS Public Cloud Services Pillar Document (particularly section 2) • SaaS Cloud Services Pillar Document (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. **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 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 *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). **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.

14.	CUSF Art. 12.1.6(VI)	Terms and conditions under which the third party may subcontract with other persons the performance of services related to the fulfilment of the agreed obligations;	• Section 6 FSA • Section 6.2 FSA • Section 5 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** includes terms applicable to Oracle's use of subprocessors and strategic subcontractors, and similar to **Section 5** of the Oracle Data Processing Agreement, includes a right for a customer to object to the intended involvement of a new strategic subcontractor.
15.	CUSF Art. 12.1.6(VII)	The guidelines for verifying that the third party periodically receives appropriate training and information in relation to the contracted services, taking into account the nature and relevance of such services;	• Section 7.2 DPA	Oracle promotes security awareness and educates employees through regular newsletters and various security awareness campaigns. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees' jobs at Oracle and are required by company policy. Oracle maintains high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business around the world. These apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Oracle requires its employees to receive training in ethics and business conduct every two years. See also **Section 7.2** of Oracle Data Processing Agreement For more information, see https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
16.	CUSF Art. 12.1.6(VIII)	The requirements of the technical, operational and control processes that the third party must comply with, to ensure that the provision of the contracted service is carried	• Section 7.1 DPA • Section 1.7 of the Oracle Cloud Hosting and Delivery Policies	Please see row 10 above and Oracle Corporate Security Practices **Section 7.1 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

		out complying with the LISF and CUSF; and	• Section 5 CSA • Section 5 Schedule C	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. 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.
17.	CUSF Art. 12.1.6(IX)	**Acceptance of the third-party provider to:**	[redacted]	
18.	CUSF Art. 12.1.6(IX)(a)	Comply with the provisions of articles 268, 269 and 359 of the LISF;	• Section 8 FSA	See **Section 8** of the **FSA** – Compliance with Laws
19.	CUSF Art. 12.1.6(IX)(b)	Receive supervisory visits by the Insurance Company's independent external auditor or, where appropriate, by external independent actuaries who rule on the situation and sufficiency of the technical reserves of the Insurance Companies, at their request, for the purpose of carrying out the corresponding supervision over the records, information and technical support with respect to the provided outsourced services;	• Section 1 FSA • Section 10 DPA • Section 1.12 of the Oracle Cloud Hosting and Delivery Policies	Please refer to **Section 1** (Customer Audit Rights) **of the FSA** **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)** **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.

				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.
20.	CUSF Art. 12.1.6(IX)(c)	Allow access to the independent external auditor of the Insurance Company (who gives an opinion on the financial statements of the Insurance Company, or as the case may be, to the independent actuaries who give an opinion on the situation and sufficiency of the technical reserves of the same) to the books, systems, records, manuals and documents in general, related to the provided outsourced services. Likewise, allow them to have access to the responsible personnel and to their offices and facilities in general, related to the provision of the service in question.	See row 19 above.	See row 19 above.
21.	CUSF Art. 12.1.6(IX)(d)	Provide the CNSF with the information that it requires regarding the provision of services that, where appropriate, it would have subcontracted for the fulfillment of the obligations agreed with the Insurance Company in question, and	See row 19 above.	See row 19 above.

22.	CUSF Art. 12.1.6(IX)(e)	Inform the Insurance Company in question, with at least forty-five calendar days in advance, regarding any reform to its corporate purpose or in its internal organization that could affect the provision of the 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.
23.	CUSF Art. 12.1.7	In the outsourcing of services, Insurance Companies shall verify that the third-party provider has the experience, technical, financial, administrative and legal capacity as well as the material, financial and human resources that are necessary to guarantee an appropriate level of performance, control, reliability and security in the provision of the services.		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
24.	CUSF Art. 12.1.8	Insurance Companies may contract the provision of the services indicated in CUSF Article 12.1.1 with entities of the Federal or State Public Administration, only when they are empowered by their law or regulation to provide the services in question.		This is a customer consideration.
25.	CUSF Art. 12.1.9	For services related to information systems and technologies referred to in section VI of Article 12.1.1, the policies and criteria that, in terms of the provisions of section V of Article 269 of the LISF, are approved by the Board of Directors of the Insurance Companies, must foresee the possibility of conducting audits or	• Section 1 FSA • Section 2 FSA	Please refer to **Section 1** (Customer Audit Rights) **of the FSA** Please refer **Section 2** (Regulator Audit Rights) **of the FSA.**

		implementing other third party review mechanisms whose purpose is to verify the degree of compliance with the provisions of this Chapter.		
26.	CUSF Art. 12.1.10	The third parties' providers, shall be subject to the inspection and Monitoring by the CNSF, in accordance with the provisions set forth in Articles 268, 269 and 359.	See row 3 above.	See row 3 above.
27.	CUSF Art. 12.3.1	Insurance companies must have a file on each service they contract with third parties, which shall contain: (I) a copy of the power of attorney that certifies the authority of the parties' legal representatives involved in the services agreement; (II) a copy of the third party's incorporation deed (in the case of a company); (III) the services agreement to be executed; (IV) the documentation (if applicable) considered prior to the execution of the agreement to comply with the requirements set forth in Article 12.1.6;	• 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 a customer consideration, however, obligations with respect to 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

		(V) the analysis carried out by the Insurance Company to confirm that the third-party provider complies with the requirements set forth in Article 12.1.7; (VI) Where appropriate, the transfer pricing study referred to in Article 12.2.2, and (VII) the documentation supporting the activities carried out by the Insurance Company to comply with the requirements set forth in Article 12.1.9 The files referred to in this Article shall be available in the event that the CNSF requests them for inspection and monitoring purposes.		
28.	CUSF Art. 12.3.2	Insurance Companies must submit to the CNSF a report on the contracts referred to in this Title, as part of the Regulatory Report on Operations Contracted with Third Parties (RR-9) referred to in Chapter 38.1 of these Articles.		This is a customer consideration.