ORACLE

Oracle Contract Checklist for Mexico CNBV Requirements for Financial Technology Institutions Under the LTF and CUF

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 financial service customers in Mexico meet their obligations, particularly under the *Ley para Regular las Instituciones de Tecnología Financiera* ***("LTF")*** and *Disposiciones de Carácter General Aplicables a las Instituciones de Tecnología Financiera* ***("CUF")*** issued by the Comisión Nacional Bancaria y de Valores ("*CNBV*") 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 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) {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 CNBV is Mexico's primary banking regulator. The CNBV has issued regulations applicable to IT sourcing for fintechs. These guidelines (LTF and CUF) 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 are to ensure the continued stability and security of the financial sector as the outsourcing of technology operations becomes more pervasive. For a complete list of regulatory requirements, see LTF and CUF.

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

NO.	FINTECH REFERENCE (LTF/CUF)	REGULATION REQUIREMENT/DESCRIPTION	REFERENCE TO ORACLE CLOUD SERVICES CONTRACT/RESOURCE	ORACLE EXPLANATION

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

	LTF/CUF			
1.	LTF Art. 54	Outsourcing of services shall not release the Fintech Company or their officers, employees, representatives or agents, of their obligations to comply with the applicable regulations.		This is a customer consideration.
2.	CUF Art. 85	**Agreements between Crowdfunding Institutions and third parties that imply the following need authorization from the CNBV:**		
3.	CUF Art. 85(1)	the transfer, storage, processing, safeguarding or custody of sensitive information, images of identifications or biometric information of clients; provided, that such third party has privileges to (i) access the information itself, (ii) the security configuration of the information or (iii) manages access controls; or	• Section 1.2 of Oracle Cloud Hosting and Delivery Policies • Section 1.3 & 1.4 of Oracle Cloud Hosting and Delivery Policies	**Please refer to row 5 below.** **Section 1.2 of the** Oracle Cloud Hosting and Delivery Policies mentions physical security safeguards. **Section 1.3 & 1.4 of the** Oracle Cloud Hosting and Delivery Policies discusses system and data access controls. Oracle access controls are described within Oracle Corporate Security Practices
4.	CUF Art. 85(2)	provision of offshoring of accounting, treasury, or client transaction record services for the Crowdfunding Institution.	• Ordering Document	This is a customer consideration. Please refer to Ordering Document regarding data center processing locations.
5.	CUF Art. 85	Crowdfunding Institutions must ensure that all service providers maintain confidentiality over its transactions.	• Sections 7 and 9 DPA • Sections 4 and 5 Schedule C • Section 4 and 5 CSA • Oracle Cloud Hosting and Delivery Policies	• **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":**

			• Oracle SaaS Public Cloud Services Pillar Document • Oracle PaaS and IaaS Public Cloud Services Pillar Document	- **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
6.	CUF Art. 85	Engagement of services with third parties shall be approved by the CEO of each Crowdfunding Institution.		This is a customer consideration.
7.	CUF Art. 85	The Crowdfunding Institution must maintain third-party supplier information in the suppliers registry mentioned in article 88 of the CUF.		This is a customer consideration.
8.	CUF Art. 86	**A request for authorization to enter into an agreement under Article 85 of the CUF shall be accompanied by:**		
9.	CUF Art. 86(I)	A detailed description and flow charts of the processes of the services that will be hired, considering the activities that will be performed by the Crowdfunding Institution and the services provider		Please refer to https://www.oracle.com/cloud/ for a detailed description of Oracle Cloud Infrastructure and Oracle Cloud Applications (SaaS) services.
10.	CUF Art. 86(II)	The draft services agreement in which shall be established (i) the date that it will be executed, and (ii) the rights and obligations of the parties, including determinations regarding the intellectual property regarding designs, developments and used processes for the service provision. Such agreement shall be in Spanish.	• 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 **Section 3 of the CSA** and **Section 3 of Schedule C** discusses ownership rights, intellectual property rights, and restrictions regarding customer content.

			• Oracle SaaS Cloud Services Pillar Document • Section 3 CSA • Section 3 Schedule C	
11.	CUF Art. 86	**In this regard, the third-party services provider shall expressly accept the following obligations:**		
12.	CUF Art. 86(II)(a)	To conform with article 54 of the LTF	• 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
13.	CUF Art. 86(II)(b)	In case of a due diligence to be performed by the Crowdfunding Institution, external auditor, or the CNBV, the services provider shall deliver the books, systems, registries, manuals and documents, related to the relevant services, as well as allowing the independent external auditor or the CNBV's personnel to access its offices and facilities.	• Sections 7 and 8 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 • Section 7 DPA • Section 8 DPA • Section 1 FSA • 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 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:**

				- **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 in accordance with Oracle's obligation under applicable laws. Please refer to **Section 1** (Customer Audit Rights) **of the FSA.** 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.
14.	CUF Art. 86(II)c)	To inform, with at least 30 days before such modification, the Crowdfunding Institution regarding any modification in its corporate purpose or any other change that may affect the service provision.	• Section 7 FSA	Primarily a customer consideration, however, 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.
15.	CUF Art. 86(II)(d)	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.	See row 5 above.	See row 5 above.

16.	CUF Art. 86(II)(e)	If the third-party sub-contracts the services, such third party must notify the Crowdfunding Institution.	• Section 6.1 FSA • Section 6.2 FSA • Section 6.2.2 FSA • Section 5 DPA	**Sections 6.1 and 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 6.2.2 of the FSA** provides an "opt-out" option as stated, "Within 30 calendar days of Oracle providing such notice to You under the preceding paragraph, You may object to the intended involvement of the relevant Strategic Subcontractor in the provision of the cloud services, by submitting a "service request" via My Oracle Support…." See also **Section 5** of the Oracle Data Processing Agreement.
17.	CUF Art. 86(II)(f)	Comply with the terms, conditions and processes that guarantee the return, transfer and elimination of the information.	• Section 4.1 and 4.3 FSA • Oracle SaaS Cloud Services Pillar Document (Section 6) • Oracle PaaS/IaaS 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 and PaaS/IaaS 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 FI 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
18.	CUF Art. 86(II)(g)	Keep within the audit registries detailed information regarding the access or access intents and the operations and activities performed by the use.		This is primarily a customer consideration. However, Identity and Access Management (IAM) lets you control who has access to cloud resources. You can control what type of access a group of users has and to which specific resources. For more information, see https://docs.oracle.com/en-us/iaas/Content/Identity/home1.htm

19.	CUF Art. 86(II)(h)	Have information control access to the information and profiles determined by the Crowdfunding Institution.	See row 18 above.	See row 18 above.
20.	CUF Art. 86(II)(i)	Allow the Crowdfunding Institution to perform specific security revisions set forth in the CUF.	See row 5 above.	See row 5 above.
21.	CUF Art. 86(III)	**The following documents regarding the Technological Infrastructure:**		
22.	CUF Art. 86(III)(a)	Description of the communication links used between the third-party and the Crowdfunding Institution.		Please see Accessing Oracle Cloud Infrastructure: https://docs.oracle.com/en-us/iaas/Content/GSG/Concepts/baremetalintro_topic-Accessing_Oracle_Cloud_Infrastructure.htm
23.	CUF Art. 86(III)(b)	Telecommunications diagram whereby the connection between all suppliers and Crowdfunding Institution is reflected		Oracle has published reference architecture to help customer design certain technologies in the cloud. For more information about Oracle cloud architecture, please see: https://www.oracle.com/cloud/architecture-center/
24.	CUF Art. 86(III)(c)	Address where the services will be performed, as well as, the data centers, primary and secondary, in which the data will be stored and processed. Such information shall include street name, number, county, state, zip code.	• Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document • Oracle SaaS Cloud Services 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 Services Pillar Document.**
25.	CUF Art. 86(III)(d)	Interrelationship application or systems subject of the service, including the Crowdfunding Institution.		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.

26.	CUF Art. 86(III)(e)	The continuity mechanisms of the hired service.	• Section 5 FSA • Section 2 Oracle Cloud Hosting and Delivery Policies • Oracle PaaS and IaaS Public Cloud Services Pillar Document (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 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.
27.	CUF Art. 86(IV)	Mechanisms that allow the Crowdfunding Institution to maintain in its facilities the detailed registries of all Transactions, as well as its accounting records.		This is a customer consideration.
28.	CUF Art. 86(V)	When the third party has access privileges to the images of official identifications or biometric information of the Clients, present evidence of the controls that it will maintain to guarantee the	See row 3 above.	See row 3 above.

		confidentiality, integrity and availability of this information.		
29.	CUF Art. 86(VI)	**When hiring Cloud services, the following shall be described:**		
30.	CUF Art. 86(VI)(a)	Type of cloud, public, private or hybrid.		Within OCI, customers are allowed the flexibility to deploy across multiple clouds. For more information, see https://www.oracle.com/a/ocom/docs/cloud/oci-for-the-modern-enterprise.pdf
31.	CUF Art. 86(VI)(b)	Specific regions where it will be stored and processed.		For information on Cloud Regions, see https://www.oracle.com/cloud/cloud-regions/ See also row 24 above.
32.	CUF Art. 86(VI)(c)	Other schemes of public cloud or shared infrastructure, the description of the mechanisms of control used to guarantee the confidentiality, integrity and availability of the sensitive information.	See row 5 above.	See row 5 above.
33.	CUF Art. 86(VII)	The description of the mechanisms to monitor the performance of the third-party and the compliance with its contractual obligations, including at least, those set forth in the CUF.	• 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 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 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 https://ocistatus.oraclecloud.com/, https://saasstatus.oracle.com/, and OCI Console.
34.	CUF Art. 86(VIII)	Plans to evaluate and report to the Administration Organ or the surveillance committee of the Crowdfunding Institution, depending on the importance of the hired service, the third-party performance and the compliance of the regulations applicable to the service.		This is a customer consideration.
35.	CUF Art. 86(IX)	Evidence that allows to verify that the third-party have and implement data privacy and confidentiality policies that allow the Crowdfunding Institution to comply with applicable legal provisions. If the services are provided abroad, documentation that evidences that the country where such third-parties reside grants protection to personal data and its confidentiality is safeguarded.		Oracle provides information about frameworks for which an Oracle lines of business have achieved a third - party attestation for one or more of its services. These attestation reports or certificates provide an independent assessment of the security, privacy, and compliance controls of the applicable Oracle Cloud services, and can assist with compliance and reporting. Such attestations include CSA Star, SOC, and ISO/IEC 27001,27017, and 27018. For more information see, https://www.oracle.com/corporate/cloud-compliance/ 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

36.	CUF Art. 87	**The Crowdfunding Institutions that hire third party services subject to the CNBVs authorization, as well as, those related with operative process and data base administration and IT systems shall comply with the following:**		
37.	CUF Art. 87(I)	For services related with operative process and data base administration and IT systems, to convene what is set forth in II of article 86.	• 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 • Section 3 CSA • Section 3 Schedule C	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 **Section 3 of the CSA** and **Section 3 of Schedule C** discusses ownership rights, intellectual property rights, and restrictions regarding customer content.
38.	CUF Art. 87(II)	To perform, at least once a year, internal or external audits regarding the hired services or to have evidence that the third party has performed them.	• 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.
39.	CUF Art. 87(III)	To maintain in its principal office, at least, information and		This is a customer consideration.

		documentation regarding evaluations, audit results, and in its case cure plans, as well as, performance results.		
40.	CUF Art. 87(IV)	To update the description or documentation regarding any modification that is considered as a relevant impact regarding the provided service or that are related with the systems, equipment and applications subject of the hired services.	• Section 4 of the Oracle Cloud Hosting and Delivery Policies	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.

41.	CUF Art. 87(V)	**Regarding the technological infrastructure and the information security, to have:**		
42.	CUF Art. 87(V)(a)	the technical characteristics description of systems, equipment and application subject of the service.		Please refer to https://www.oracle.com/cloud/ for a detailed description of Oracle Cloud Services. Please also refer to the relevant program documentation: https://docs.oracle.com/en/
43.	CUF Art. 87(V)(b)	Mechanisms that assure the transfer and storage of the coded information, including the Coded protocol and technological infrastructure security components.	• Section 1.5 of Oracle Cloud Hosting and Delivery Policies	Customers are responsible for their own encryption, however, under **Section 1.5 of the** Oracle Cloud Hosting and Delivery Policies Your access to Oracle Cloud Services is through a secure communication protocol provided by Oracle. If access is through a Transport Layer Security (TLS) enabled connection, that connection is negotiated for at least 128 bit encryption. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configurable for all web-based TLS-certified applications deployed at Oracle.
44.	CUF Art. 87(V)(c)	The type of sensitive information that will be stored by the third-party in its equipment and facilities.		This is a customer consideration. Customers are responsible for the classification of the data they place in Oracle Cloud.
45.	CUF Art. 87(V)(d)	The control and surveillance mechanisms to access the computer systems and to the sensitive information transferred, stored, processed and custodied in such systems, as well as such reports, data base and security configurations.	See row 33 above.	See row 33 above.
46.	CUF Art. 87(V)(e)	Evidence of the control and control mechanisms regarding sub-index V and VI of article 86 of the CUF.	See rows 3 & 5 above.	See rows 3 & 5 above.
47.	CUF Art. 87(VI)	Evidence mentioned in sub-index IX of article 86 of the CUF.		For evidence regarding applicable attestations and/or certifications, please see https://www.oracle.com/corporate/cloud-compliance/
48.	CUF Art. 87	The CEO or Sole Director of the Institution will be responsible of the implementation of the evaluations		This is a customer consideration.

		and cure plans set forth in this article.		
49.	CUF Art. 88	Crowdfunding Institutions shall keep a detailed record of all of their third party providers, which shall not be limited to services rendered and regulated under article 85 of the Fintech Regulations.		This is a customer consideration.