VOVE ID

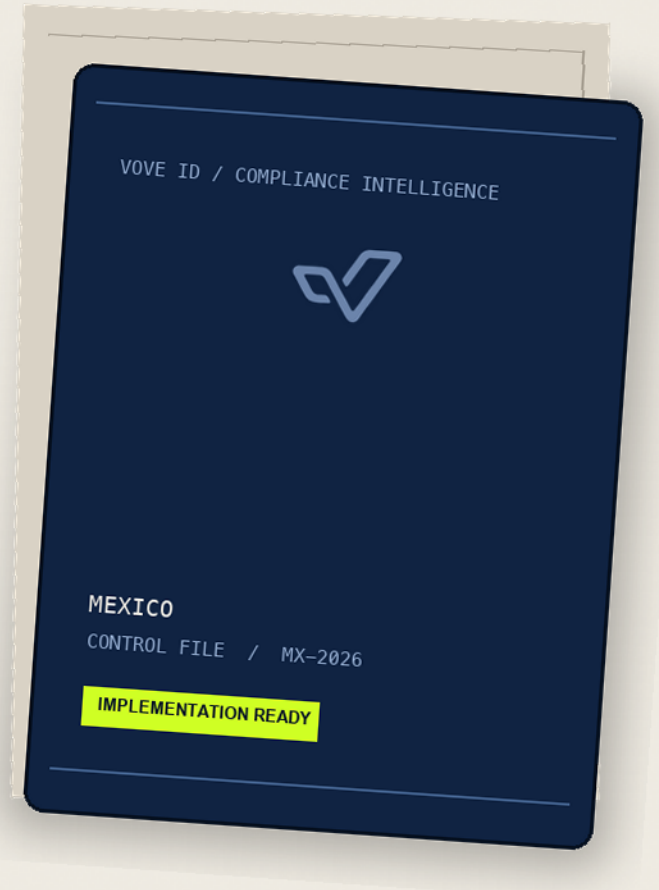
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

MEXICO

MEXICO / MX



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Mexico KYC, KYB & AML Compliance Checklist

An implementation checklist for Mexico's split AML/CFT framework. It separates sector-specific financial-entity rules from the LFPIORPI regime for designated vulnerable activities, incorporates the 16 July 2025 reform and its staged secondary-rule transition, and maps company, beneficial-owner, privacy, sanctions, payments, fintech and virtual-asset controls.

National FIU	**Unidad de Inteligencia Financiera (UIF) within SHCP**
Core framework	**LFPIORPI, last reformed 16 July 2025, plus sector financial laws and general provisions**
Vulnerable-activity 24-hour notices	**Legacy cases remain operative; broadened 2025 scenarios, including attempted operations, depend on updated official notice annexes**
Routine vulnerable-activity notices	**By the 17th day of the immediately following month when the applicable article 17 notice threshold is met**
Retention	**At least 10 years for financial entities and, after the 2025 reform, generally for vulnerable-activity records**
Beneficial owner	**LFPIORPI control includes more than 25% voting rights; the separate tax-accounting test in the Federal Fiscal Code uses more than 15%**
Vulnerable-activity thresholds	**Activity-specific multiples of the daily UMA; apply the current UMA and six-month aggregation rule**
Financial-sector reporting	**Sector-specific relevant, unusual, internal-concern, 24-hour and other reports through the applicable supervisor channel**
Privacy authority	**Secretaria Anticorrupcion y Buen Gobierno under the 2025 private-sector data law**
Fintech authorization	**CNBV authorization, with inter-institutional approval, is required to organize and operate as an ITF**
FATF status	**FATF member; not named on the public call-for-action or increased-monitoring lists reviewed 31 July 2026**

Scope and legal framework

LFPIORPI applies to financial entities and the non-financial vulnerable activities listed in article 17; Financial entities follow their sector statutes and SHCP general provisions, supervised through CNBV, CNSF or CONSAR as applicable; The 16 July 2025 LFPIORPI reform expanded beneficial-owner, PEP, suspicious-notice, governance, monitoring, audit and registry duties, with transitional limits for official formats and filing routes; The broadened article 18(VI) notice

scenarios depend on updated official annexes, and article 18(VII-XI) duties commence on dates set by revised general rules; current SAT and Diario Oficial instruments must be checked before implementation; The Federal Fiscal Code, company law, private-sector data law and Fintech Law create parallel obligations that do not replace AML CDD

FATF context

Mexico has been a FATF member since 2000 and is also assessed with GAFILAT. Mexico was not named on the FATF increased-monitoring or call-for-action public lists reviewed 31 July 2026. Its 2023 follow-up ratings and forthcoming fifth-round evaluation remain relevant risk and control inputs; absence from a public list is not a finding that country risk is low.

IMPORTANT	General regulatory information, not legal advice, an authorization decision or a substitute for the operative Spanish text, sector provisions, official forms or regulator instructions. Reviewed 31 July 2026. Thresholds expressed in UMA change with the applicable official value. Confirm entity, activity, customer, transaction, aggregation, reporting channel, commencement date, sanctions route, privacy role and later developments with qualified Mexican counsel and the relevant authority before launch.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

For every row, assign an owner, confirm whether the control applies, link the evidence, record gaps, and set a remediation date. A checked box is not evidence by itself.

01 / SCOPE	02 / DESIGN	03 / EVIDENCE	04 / REVIEW
Confirm institution, supervisor, product, customer and risk scope.	Map each obligation to a policy, system control or human review.	Retain the document, decision, timestamp, owner and rationale.	Test the control and update it when rules or risks change.

Checklist legend

CONTROL tells you what outcome to cover. IMPLEMENTATION ACTION translates that outcome into operational work. EVIDENCE suggests what an auditor or reviewer should be able to inspect. SOURCE points back to the primary rule or regulator guidance.

Minimum review record

Keep a compact decision record for each checklist row so a later reviewer can reconstruct what applied, who decided, and what evidence was inspected.

APPLICABILITY	OWNERSHIP	TRACEABILITY
Applicable, not applicable, or pending legal confirmation, with a short rationale.	Named control owner, reviewer, approval date and next review date.	Evidence link, source version, test result, gap status and remediation ticket.

Scope, authorities and licensing

Mexico has no single operating rulebook for every business. Resolve whether the entity is a regulated financial entity, an article 17 vulnerable-activity operator, both, or outside those perimeters before configuring controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Financial entities are subject to LFPIORPI and the special laws and general provisions governing their sector.	Classify the exact legal entity, product and activity; map SHCP, UIF, CNBV, CNSF, CONSAR and Banco de Mexico responsibilities and use the current sector rule set.	Perimeter memorandum, authorization and register extracts, authority matrix, current-rule inventory and counsel approval.	LFPIORPI arts. 13-16
Non-financial vulnerable activities are the activities and thresholds listed in LFPIORPI article 17, including covered real estate, credit, professional services, value instruments and virtual-asset services.	Test each Mexican and Mexico-directed service against every relevant article 17 limb, including activities conducted through trusts or other legal arrangements.	Activity map, threshold analysis, six-month aggregation logic, cross-border nexus assessment and signed applicability decision.	LFPIORPI arts. 17-19; SAT LFPIORPI criteria
A person carrying on a vulnerable activity must register and maintain its SAT portal status when the operative official format covers that person and activity.	For covered categories, complete registration before the first notice using valid RFC and e.firma credentials. Track the Regulation's Third Transitory deferral for article 17(XII)(D), persons acting through trusts or other legal arrangements, customs agencies and specified article 17(XIV) legal persons until the format expressly identifies them.	Applicability and transition check, registration receipt where available, portal profile, credential-control record, updates, owners and monitoring log.	LFPIORPI art. 18(IV Bis); 27 March 2026 Regulation decree transitory art. 3; SAT SPPLD obligations
Organizing and operating as a financial-technology institution requires CNBV authorization following the statutory inter-institutional process.	Do not market or operate regulated crowdfunding or electronic-payment-fund services without the required authorization; verify the live CNBV register and any Banco de Mexico permissions.	Perimeter opinion, application, authorization, register extract, conditions, launch approval and continuing-obligation map.	Fintech Law arts. 3, 11 and 35-45

Governance, risk assessment and transition

Financial-sector governance is set by sector provisions. For vulnerable activities, distinguish duties already in force from the staged article 18(VII-XI) duties whose commencement depends on revised general rules.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A legal person or legal arrangement carrying on vulnerable activities must designate and maintain a compliance representative; absent an accepted designation, statutory responsibility falls to the persons identified in article 20.	File and maintain the designation, protect the representative's identity, document deputies and escalation, and ensure annual training required by article 20.	Portal acceptance, appointment, role description, board minutes, confidentiality controls, training and succession plan.	LFPIORPI arts. 20 and 38
The 2025 reform added vulnerable-activity risk assessment, internal manual, group policy, annual training, automated monitoring and risk-based annual audit duties.	Build these controls now, but label their statutory commencement accurately and monitor revised general rules and SAT criteria for the applicable dates and minimum elements.	Transition tracker, official-source snapshots, risk assessment, manual, group standard, training plan, system specification and audit plan.	LFPIORPI art. 18(VII-XI); 16 July 2025 reform transitory arts. 2-3; SAT criteria
Financial entities and ITFs must maintain risk-based policies, automated systems, responsible governance, training and annual independent or internal review under their applicable sector provisions.	Map each requirement to the entity's exact general provisions and authorization conditions; do not transplant a bank threshold or deadline into another sector.	Enterprise and customer-risk methods, approved manual, committee records, officer certification, system tests, training and annual audit.	LFPIORPI art. 15; Fintech Law art. 58; applicable SHCP general provisions
Policies must cover customers, users, representatives, beneficial owners, products, channels, geography, PEPs, high-risk relationships and attempted operations.	Create legal-entity and sector-specific risk taxonomies and approval paths; record why simplified, standard or enhanced measures apply.	Risk factors, scoring method, overrides, approvals, quality assurance, model validation and change log.	LFPIORPI arts. 3, 18 and 20; applicable sector general provisions

Natural-person KYC and representatives

Identification evidence and thresholds vary by sector and vulnerable activity. The control must bind a real person to reliable evidence and preserve the information required by the applicable official annex or sector provision.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A vulnerable-activity operator must directly identify and know its customer or user, verify identity using officially recognized documents or means, and retain a copy as required by the general rules.	Collect the applicable identity data, authenticate the evidence, bind it to the applicant, screen it for fraud and retain the required record before the activity proceeds.	Identity file, document images, authenticity result, biometric or liveness output where used, timestamps, reviewer and exceptions.	LFPIORPI art. 18(I); LFPIORPI General Rules annexes
For a business relationship, vulnerable-activity operators must obtain occupation or activity information, including by reference to RFC registration and updates.	Capture occupation, employer or business activity, purpose, expected activity and source information proportionate to risk; reconcile material inconsistencies.	RFC evidence, customer profile, purpose, expected activity, discrepancy resolution, approval and refresh schedule.	LFPIORPI art. 18(II)
A representative must be identified and their authority to act must be validated under the applicable identification rules.	Verify the representative as a natural person, obtain the mandate or power, check its scope and validity and link it to the customer file.	Representative KYC, power or mandate, registry or notarial check, authority analysis, expiry and approval.	LFPIORPI art. 18; General Rules annexes; applicable sector general provisions
If a vulnerable-activity customer or user refuses information or documents required by LFPIORPI, the operator must abstain from carrying out the act or operation.	Prevent completion, preserve the refusal and attempted-operation record, assess any operative legacy 24-hour notice case and the staged broadened article 18(VI) scenario, and avoid prohibited disclosure.	System block, refusal record, escalation, transition-aware notice decision, filing receipt if applicable and communication log.	LFPIORPI arts. 18(VI), 21 and 38; 27 March 2026 Regulation decree transitory art. 5

KYB, registries and beneficial ownership

Customer KYB, the customer's own corporate and tax filing duties, and AML beneficial-owner verification are separate controls. A registry result does not replace ownership and control analysis.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
For a legal person, trust or other legal arrangement, a vulnerable-activity operator must obtain officially recognized evidence identifying the beneficial owner.	Trace ownership and control to natural persons, identify the person on whose behalf the act occurs and corroborate customer declarations with reliable independent sources.	Constitutional documents, RPC and PSM results, ownership chart, control analysis, declarations, corroboration and reviewer sign-off.	LFPIORPI arts. 3(III), 18(III) and 33 Bis-33 Quater
The LFPIORPI control test includes the ability to exercise more than 25% of voting rights, but also covers appointment power, contractual control and direction of administration, strategy or principal policies.	Do not use 25% as the sole beneficial-owner test; evaluate direct, indirect, contractual and de facto control and the ultimate beneficiary of the act or service.	Cap table, indirect calculations, voting and shareholder agreements, board rights, control memorandum and escalation.	LFPIORPI art. 3(III)
The Federal Fiscal Code creates a separate accounting record and on-request disclosure regime using a more-than-15% voting-control limb and a 15-calendar-day update duty after changes.	Maintain a distinct tax beneficial-controller file, update changes within 15 calendar days and be ready to respond to an SAT request within the statutory period.	Tax BO register, source documents, change log, 15-day control, SAT response pack and delivery receipt.	Federal Fiscal Code arts. 32-B Ter, 32-B Quater and 32-B Quinquies
Mercantile companies must maintain corporate ownership records and comply with applicable electronic notices, while the RPC and PSM publish different categories of corporate information.	Query the national RPC and PSM, obtain current corporate books and filings and reconcile inconsistencies; do not assume either public system is a complete AML beneficial-owner register.	RPC folio, PSM notices, shareholder or quota register, transfer records, discrepancy analysis and remediation.	General Law of Commercial Companies arts. 73, 128-129; LFPIORPI arts. 33 Bis-33 Ter; RPC and PSM guidance

5. PEPS, EDD AND REMOTE ONBOARDING

PEPs, EDD and remote onboarding

PEP and enhanced measures depend on the applicable sector rules and, for the new vulnerable-activity framework, the revised general rules. Remote identity does not reduce the accountable entity's duty.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
LFPIORPI now defines domestic and foreign PEPs and requires vulnerable-activity internal policies to identify and follow transactions involving PEPs.	Screen customers, users, representatives and beneficial owners; document the public function, relationship, risk, approval, source of wealth and source of funds where proportionate and required.	PEP screening, role and relationship analysis, approval, wealth and funds evidence, monitoring plan and review date.	LFPIORPI arts. 3(IX Bis) and 18(VIII)
High-risk and PEP customers require intensified monitoring under the added vulnerable-activity automated-monitoring provision once its staged commencement applies.	Implement intensified review now as a prudent control and track the general-rule commencement date before labelling it a currently operative statutory duty.	Transition note, high-risk flags, scenario settings, alert history, periodic review and approval.	LFPIORPI art. 18(X); 16 July 2025 reform transitory art. 3
Remote onboarding must satisfy the identity, authentication, record and technology conditions in the entity's applicable sector provisions or LFPIORPI rules.	Map each remote flow to the controlling annex or authorization, test presentation attacks and impersonation, provide accessible fallback and govern vendor changes.	Remote-onboarding legal map, vendor assessment, biometric tests, device and liveness results, accessibility testing and monitoring.	LFPIORPI art. 18(I); Fintech Law art. 56; applicable sector general provisions
Reliance on a vendor, agent or group service does not transfer the regulated entity's legal responsibility.	Contract for evidence access, audit rights, incident notice, data controls and exit; independently test the service and retain reconstructable decisions.	Contract, due diligence, control mapping, service reports, sample testing, incidents and exit plan.	LFPIORPI arts. 18 and 20; Fintech Law arts. 54-58; applicable sector provisions

Monitoring, suspicious notices and confidentiality

Mexico uses different report classes and channels. A vulnerable-activity notice under LFPIORPI is not the same as a financial entity's unusual-operation report under sector provisions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Vulnerable-activity operators must use the operative 24-hour route for legacy cases supported by current rules and formats; the 2025 expansion to broader suspicion and attempted-operation scenarios awaits the official annex update required by the 2026 Regulation transition.	Escalate all suspicion and attempted activity immediately, preserve the knowledge timestamp, file any currently supported legacy 24-hour notice, and obtain a current legal and format check for a broadened article 18(VI) scenario rather than assuming SPPLD accepts it.	Alert, facts and indicators, escalation time, rule and annex version, transition decision, filing and acknowledgement where applicable, attempted-operation flag and rationale.	LFPIORPI art. 18(VI); LFPIORPI Regulation art. 7 Bis; 27 March 2026 Regulation decree transitory art. 5; SAT SPPLD guidance
Financial entities submit unusual, 24-hour and other required reports to SHCP/UIF through the applicable supervisory channel and sector timetable.	Maintain a sector-specific reporting matrix and live portal credentials; do not use the vulnerable-activity day-17 rule for a bank, ITF, insurer or other financial entity.	Rule and report inventory, alert-to-filing timeline, report, supervisor receipt, quality review and regulatory correspondence.	LFPIORPI art. 15; Fintech Law art. 58; applicable SHCP general provisions
Financial-sector 24-hour reports apply in defined fact-based circumstances and to applicable blocked-person-list events under sector provisions.	Route facts immediately to the certified officer, apply the required restriction or suspension, file within the sector deadline and preserve the legal basis.	Knowledge timestamp, match adjudication, restriction record, report, acknowledgement, legal analysis and release authority.	Banking General Provisions 41 and blocked-person-list provisions; Fintech Law art. 58
Notice and report information, filer identities and protected compliance identities are confidential; staff must not disclose protected reporting information to unauthorized persons.	Apply least-privilege access, separate customer communications from reporting decisions, train personnel and obtain legal approval for any permitted disclosure.	Access logs, confidentiality labels, scripts, training, disclosure register and incident response.	LFPIORPI arts. 38-41 Bis; Fintech Law art. 58

Threshold notices, payments, wires and agents

Identification thresholds, article 17 notice thresholds, financial-sector relevant-operation reports and article 32 cash restrictions are different legal controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Routine vulnerable-activity notices are due by the 17th day of the immediately following month when the applicable article 17 notice threshold is met.	Maintain an activity-by-activity UMA matrix, apply the correct event date and six-month aggregation logic, file electronically and retain the receipt.	Threshold table, current UMA source, aggregation report, calendar, filing, acknowledgement and exception approval.	LFPIORPI arts. 17, 23-24; SAT threshold and SPPLD guidance
Certain cash, currency and precious-metal payments are prohibited at the article 32 UMA thresholds even if payment passes through a financial entity.	Block prohibited payment methods before settlement and distinguish the cash restriction from an article 17 notice or a sector relevant-operation report.	Payment-method rule, threshold test, invoices, settlement evidence, block logs and legal review.	LFPIORPI arts. 32-33
Financial-sector relevant-operation and other objective reports use sector-specific instruments, amounts, periods and channels.	Configure each licensed entity from its current general provisions; for banks, distinguish relevant cash-instrument reports, international-transfer reports, US-dollar cash reports and suspicious reports.	Sector configuration, report taxonomy, test cases, reconciliations, filings and supervisory receipts.	Banking General Provisions 34-41 and applicable formats; CNBV reporting guidance
Covered transfers require originator and beneficiary information under applicable financial-sector rules; article 17 virtual-asset operators must obtain and retain precise originator, recipient and beneficial-owner information as specified by general rules.	Capture required payer and payee data before execution, validate completeness, control intermediary data loss, reject or investigate deficient transfers and monitor secondary-rule detail.	Message fields, validation output, exception decision, repair record, screening, travel-rule mapping and audit sample.	Banking General Provisions; LFPIORPI art. 17(XVI)

8. TARGETED FINANCIAL SANCTIONS AND BLOCKED PERSONS

Targeted financial sanctions and blocked persons

The confidential Mexican blocked-person-list mechanism and public UN sanctions material are not interchangeable. The exact freeze, suspension, report and challenge process depends on the entity and sector rule.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Financial entities and ITFs must act on the confidential blocked-person list communicated by SHCP under their applicable statutes and provisions.	Screen at onboarding, before transactions and on list updates; adjudicate matches promptly, suspend or restrict as legally required, file the required report and release only on competent authority instruction.	List version, screening logs, match analysis, suspension record, report, authority communication and release approval.	Credit Institutions Law arts. 115 and 116; Fintech Law art. 58; applicable sector provisions
Current SAT guidance supports legacy 24-hour notices for specified fact-based or recognized-list cases; broadened article 18(VI) scenarios remain subject to the official-annex transition.	Do not assume a DNFBP has the same account-freeze power as a bank. Escalate immediately, file promptly where the current format supports the legacy case, document the transition analysis and obtain counsel for the exact measure.	List source, match rationale, legal authority, applicable annex version, transaction decision, notice if fileable, receipt and escalation.	LFPIORPI art. 18(VI); LFPIORPI Regulation art. 7 Bis; 27 March 2026 Regulation decree transitory art. 5; SAT guidance
UN Security Council sanctions lists and updates are authoritative screening inputs, but domestic implementation must follow Mexican law and the competent-authority route.	Monitor UN updates and Mexican communications, map each programme to the applicable domestic control and avoid releasing or freezing assets without documented authority.	UN list version, domestic mapping, screening results, authority contacts, licences or directions and decision log.	UN Security Council Consolidated List; applicable Mexican sector provisions
Blocked-person and sanctions information must be handled with confidentiality, procedural accuracy and controlled customer communications.	Use approved scripts, restrict the match file, preserve challenge and authority correspondence and prevent unauthorized disclosure of confidential list content.	Access control, communication script, case chronology, authority notices, challenge handling and quality review.	Credit Institutions Law arts. 115-116; Fintech Law art. 58

9. RECORDS, AUDIT AND REGULATOR ACCESS

Records, audit and regulator access

Retention starts and interruption rules differ. Preserve enough information to reconstruct the customer, authority, transaction, analysis, report and decision.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Financial entities must retain customer-identification and reported-activity records for at least ten years, subject to longer or more specific sector rules.	Map each record class and trigger, place legal holds where required and keep records readable, searchable and exportable for the full period.	Retention schedule, legal basis, trigger field, storage controls, retrieval test, holds and disposal approvals.	LFPIORPI art. 15(IV); applicable sector provisions
Vulnerable-activity operators generally must preserve supporting, identity, reconstruction, correspondence and analysis records for at least ten years from the activity; litigation interrupts and restarts the period as article 18 specifies.	Store physical or electronic records at the registered location as required, capture the activity date and implement litigation-hold interruption and restart logic.	Record inventory, registered-location control, transaction reconstruction, hold log, final-resolution date and disposal evidence.	LFPIORPI art. 18(IV)
SHCP and relevant supervisors may request information and conduct verification or supervision within their legal competence.	Maintain a regulator-response protocol, authenticate requests, preserve privilege where applicable, produce only responsive records and log every disclosure.	Request, authority validation, scope review, production set, delivery receipt, privilege log and remediation tracker.	LFPIORPI arts. 16, 22 Bis, 25 and 34-36; Fintech Law art. 58
Required annual audit or independent review must test effectiveness, not merely document existence, under the applicable sector rule or staged vulnerable-activity duty.	Set independence and competence criteria, sample end-to-end files, test reporting timeliness and data lineage, track findings and verify closure.	Audit scope, independence, workpapers, sample results, report, management actions and closure validation.	LFPIORPI art. 18(XI) and reform transitory art. 3; Fintech Law art. 58

Privacy, biometrics and transfers

AML duties can supply a legal basis or exception for necessary processing, but they do not remove privacy principles, security, transparency, purpose limitation or data-subject rights.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
The 2025 Federal Law on Protection of Personal Data Held by Private Parties governs private-sector processing and is overseen by the Secretaria Anticorrupcion y Buen Gobierno.	Identify the controller and processors, document lawful grounds and exceptions, provide a compliant privacy notice and reconcile ARCO rights with mandatory AML retention and reporting.	Data inventory, role map, legal-basis register, privacy notice, consent or exception record, ARCO procedure and retention reconciliation.	LFPDPPP arts. 1-15 and 38-39
Financial or patrimonial data generally requires express consent and sensitive data requires express written consent, subject to statutory exceptions including processing required by law or legal relationship.	Classify identity, biometric, financial, sanctions and investigation data; document the exact legal requirement or consent and minimize collection to the stated purpose.	Data classification, consent evidence, statutory-exception memo, field minimization, access restrictions and periodic review.	LFPDPPP arts. 7-9 and 12
Controllers must maintain administrative, technical and physical security and immediately inform affected persons of breaches that significantly affect their patrimonial or moral rights.	Use risk-based security for identity and biometric data, maintain incident detection and an immediate notification workflow, and document whether the statutory significance test is met.	Security assessment, control set, incident log, impact analysis, notification, timestamps and post-incident remediation.	LFPDPPP arts. 18-20
Domestic and international transfers must follow the privacy notice and transfer rules, with consent unless a statutory exception applies; the recipient assumes corresponding obligations.	Map every vendor, group and authority transfer, flow down privacy obligations, document the exception or consent and control onward transfers and deletion.	Data-flow map, transfer register, notice, consent or exception, contract, due diligence and deletion confirmation.	LFPDPPP arts. 35-36

Payments, fintech, virtual assets and launch evidence

Authorization, AML status and virtual-asset treatment must be resolved separately. A technology label does not avoid a reserved financial activity or article 17 virtual-asset perimeter.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
ITFs must maintain an AML risk methodology, customer controls, automated systems, committee and certified compliance officer, annual review, reports and at least ten-year records.	Map the product and operating model to Fintech Law article 58 and current general provisions, including blocked-person suspension and report taxonomies.	Authorization conditions, risk method, manual, committee minutes, officer certificate, system tests, audit and filings.	Fintech Law art. 58
ITFs and banks may conduct statutory virtual-asset operations only with the assets and prior Banco de Mexico authorization allowed under the Fintech Law and Circular 4/2019 framework.	Do not infer retail permission from use of distributed-ledger technology; obtain a written perimeter analysis and the required Banco de Mexico authorization before any covered operation.	Legal opinion, asset classification, Banco de Mexico correspondence or authorization, restrictions, customer disclosures and launch gate.	Fintech Law arts. 30-32 and 88; Banco de Mexico Circular 4/2019
A non-financial platform habitually and professionally exchanging, transferring, safeguarding or storing covered virtual assets for Mexican customers can fall within LFPIORPI article 17(XVI), including Mexico-directed services from abroad.	Assess territorial nexus, register if applicable, apply the 210-UMA transaction and 4-UMA fee notice limbs and aggregation, build originator-recipient data capability, and handle 24-hour cases under the current-format transition described in section 6.	Nexus opinion, registration, threshold engine, originator and recipient fields, applicable annex version, notices, receipts and change monitoring.	LFPIORPI art. 17(XVI); SAT virtual-asset criterion; 27 March 2026 Regulation decree transitory art. 5
Launch requires a current, source-backed decision for every applicable row and evidence that reporting, sanctions, privacy, record and incident workflows work end to end.	Run controlled dry tests without submitting fictional personal data to production regulator portals, close blockers and obtain legal, compliance, privacy, security and product sign-off.	Completed checklist, primary-source register, test results, defects and closure, approvals, effective dates and monitoring owner.	LFPIORPI arts. 15-25; Fintech Law arts. 11 and 58; LFPDPPP arts. 13-20

SOURCES AND FURTHER READING

Verify against current official material

Primary law and regulator guidance control. Contextual VOVE ID reading is included to help teams operationalize the requirements and is not legal authority.

LFPIORPI - current consolidated text
Chamber of Deputies · Primary legislation
Open official source

LFPIORPI reform history and 16 July 2025 decree
Chamber of Deputies · Primary legislative history
Open background material

LFPIORPI Regulation reform of 27 March 2026
Diario Oficial de la Federacion · Primary regulation
Open official source

Current LFPIORPI reform implementation criteria
SAT Prevention of Money Laundering Portal · Official current interpretation
Open official source

Vulnerable-activity obligations and reporting deadlines
SAT Prevention of Money Laundering Portal · Official compliance guidance
Open official source

Vulnerable-activity electronic reporting portal
SAT Prevention of Money Laundering Portal · Official reporting channel
Open official source

Cash-use restrictions and UMA thresholds
SAT Prevention of Money Laundering Portal · Official threshold guidance
Open official source

Vulnerable-activity frequently asked questions
SAT Prevention of Money Laundering Portal · Official compliance guidance
Open official source

SAT criterion for Mexico-directed foreign virtual-asset services
SAT Prevention of Money Laundering Portal · Official territorial-scope interpretation
Open official source

UIF role and mandate
Unidad de Inteligencia Financiera · Official authority description
Open official source

UIF legal framework directory
Unidad de Inteligencia Financiera · Official legal directory
Open official source

CNBV current normativity directory
Comision Nacional Bancaria y de Valores · Official supervisory directory
Open official source

Banking AML general-provisions amendment of 24 February 2017
Diario Oficial de la Federacion · Historical primary regulatory instrument
Open official source

Latest banking article 115 AML general-provisions amendment, July 2026
Diario Oficial de la Federacion · Current primary regulatory instrument
Open official source

Credit Institutions Law
Chamber of Deputies · Primary legislation
Open official source

CNBV AML/CFT supervisory and blocked-person-list description
Comision Nacional Bancaria y de Valores · Official supervisor guidance
Open official source

Fintech Law - current consolidated text
Chamber of Deputies · Primary legislation
Open official source

Circular 4/2019 - virtual-asset operations
Banco de Mexico · Primary regulatory instrument
Open official source

Federal Fiscal Code - current consolidated text
Chamber of Deputies · Primary legislation
Open official source

General Law of Commercial Companies
Chamber of Deputies · Primary legislation
Open official source

Public Registry of Commerce - SIGER 2.0
Secretaria de Economia · Official company registry
Open official source

What the Public Registry of Commerce records
Secretaria de Economia · Official registry guidance
Open official source

Electronic Publications System for Commercial Companies
Secretaria de Economia · Official filing guidance
Open official source

Federal Law on Protection of Personal Data Held by Private Parties
Chamber of Deputies · Primary legislation
Open official source

FATF Mexico country and assessment page
Financial Action Task Force · Official international assessment
Open official source

FATF jurisdictions under increased monitoring, 19 June 2026
Financial Action Task Force · Official current-status source
Open official source

FATF high-risk jurisdictions subject to a call for action, 19 June 2026
Financial Action Task Force · Official current-status source
Open official source

United Nations Security Council Consolidated List
United Nations Security Council · Official sanctions list
Open official source

Document control

Version 1.2 / Published 31 July 2026 / Last reviewed 31 July 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice, an authorization decision or a substitute for the operative Spanish text, sector provisions, official forms or regulator instructions. Reviewed 31 July 2026. Thresholds expressed in UMA change with the applicable official value. Confirm entity, activity, customer, transaction, aggregation, reporting channel, commencement date, sanctions route, privacy role and later developments with qualified Mexican counsel and the relevant authority before launch.