VOVE ID

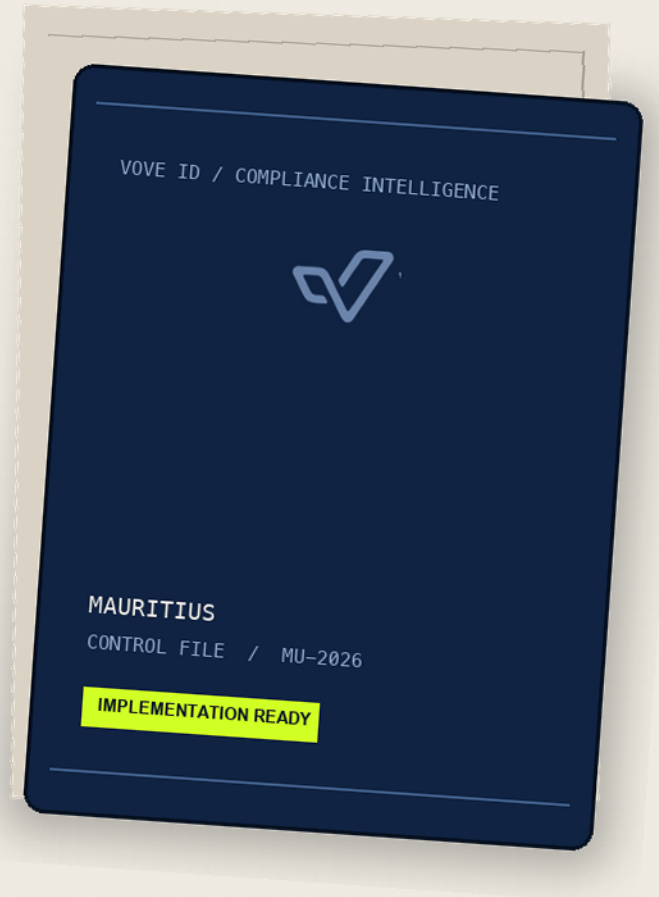
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

MAURITIUS

MAURITIUS / MU



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Mauritius KYC, KYB & AML Compliance Checklist

An implementation-focused checklist for fintechs, banks, payment service providers, FSC licensees and other reporting persons operating in Mauritius. It translates the Financial Intelligence and Anti-Money Laundering Act 2002 as currently amended, the FIAML Regulations 2018, current FIU reporting procedures, sector guidance from the Bank of Mauritius and Financial Services Commission, beneficial-ownership rules, targeted-financial-sanctions controls, payment licensing and data-protection requirements into operational actions and audit evidence.

Primary AML law	**FIAMLA 2002, as amended**
Financial intelligence unit	**FIU Mauritius**
Banking and payment supervisor	**Bank of Mauritius**
Non-bank financial supervisor	**Financial Services Commission**
Core AML record period	**At least 7 years**
STR deadline	**Within 5 working days after suspicion arose**
FATF status	**Not under increased monitoring**

Scope and legal framework

Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA), as currently amended; Financial Intelligence and Anti-Money Laundering Regulations 2018; Financial Intelligence and Anti-Money Laundering (Registration by Reporting Person) Regulations 2019; Financial Intelligence and Anti-Money Laundering (Administrative Penalties) Regulations 2025; Bank of Mauritius Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation (2020); FSC AML/CFT Handbook, as updated; Companies Act 2001, as amended through the Finance Act 2025; United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, as amended; National Payment Systems Act 2018 and National Payment Systems (Authorisation and Licensing) Regulations 2021, as amended in 2024; and Data Protection Act 2017 with the Data Protection (Fees) Regulations 2020.

FATF context

Mauritius is not on the FATF list of jurisdictions under increased monitoring as of the FATF statement dated 19 June 2026. FATF removed Mauritius from increased monitoring in October 2021. This status does not displace Mauritius's domestic risk-based requirements, the 2025 national risk assessment or enhanced controls for higher-risk customers, products, channels, transactions and geographies.

IMPORTANT

This checklist is general information, not legal advice. It reflects official materials available on 15 July 2026. Applicability depends on the entity, licence, product, customer and sector. Confirm current requirements, reporting formats, supervisory expectations, payment permissions, sanctions notices and privacy filings with FIU Mauritius, the Bank of Mauritius, the Financial Services Commission, the National Sanctions Secretariat, the Corporate and Business Registration Department, the Data Protection Office and qualified Mauritian counsel 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.

1. CONFIRM SCOPE, AUTHORITIES AND PERMISSIONS

Confirm scope, authorities and permissions

Start with the statutory reporting-person perimeter, then apply the rules and guidance of the authority supervising the particular entity and activity.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Document whether each entity and activity is a reporting person under FIAMLA.	Map every legal entity, product and customer journey to the FIAMLA definition and Schedule, including financial institutions and the specified designated non-financial businesses and professions. Record the applicable regulatory body or supervisory authority; do not assume that every Mauritius business has identical FIAMLA duties.	Signed perimeter memorandum; entity-product matrix; reporting-person classification; supervisor map.	FIAMLA, ss. 2 and 14; Schedule, as amended
Recognise FIU Mauritius as the national financial intelligence unit and STR recipient.	Maintain a controlled channel for FIU registration, electronic STR filing, FIU requests and feedback. FIU is the central agency established under FIAMLA to receive, request, analyse and disseminate relevant financial information.	FIU registration; goAML organisation profile; nominated contacts; request log.	FIAMLA, ss. 9-10 and 14C; Registration by Reporting Person Regulations 2019
Keep Bank of Mauritius and FSC scopes separate.	Apply the Bank's AML/CFT/CPF Guideline to banks, non-bank deposit-taking institutions, cash dealers, money lenders and National Payment Systems Act licensees within its stated scope. Apply the FSC AML/CFT Handbook to financial institutions under FSC's non-bank and global-business purview. Treat each as sector guidance issued under supervisory powers, not as a universal replacement for FIAMLA or the Regulations.	Licence inventory; supervisor-to-obligation matrix; sector-guidance applicability opinion.	Bank of Mauritius AML/CFT/CPF Guideline 2020, paras. 2.01-2.06; FSC AML/CFT Handbook, chs. 1-2
Obtain the required financial-services or payment permission before operating.	Classify banking, deposit-taking, cash-dealer, money-lending, payment, securities, insurance, global-business, management-company and virtual-asset activities under the relevant enabling law. Verify the licence on the competent authority's current register and map each service to the permission actually granted.	Licence or authorisation; legal perimeter opinion; service-to-permission map; regulator-register check.	Banking Act 2004; National Payment Systems Act 2018; Financial Services Act 2007; VAITOS Act 2021, where applicable
Assign accountable owners across AML, sanctions, company, payment and privacy regimes.	Maintain a RACI covering FIU and goAML, Bank or FSC supervision, CBRD beneficial-ownership filings, National Sanctions Secretariat notices, payment licensing and Data Protection Office registration and incident reporting.	Approved RACI; appointment records; committee terms; regulatory calendar.	FIAMLA; FIAML Regulations 2018; Companies Act 2001; Sanctions Act 2019; NPS Act 2018; Data Protection Act 2017

2. BUILD A RISK-BASED AML/CFT/CPF PROGRAMME

Build a risk-based AML/CFT/CPF programme

The statutory programme must connect documented risk assessment, senior-approved controls, competent officers, training and independent assurance.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a written, current business risk assessment.	Assess customer, country, product, service, transaction, delivery-channel, third-party and technology risks, considering the current national and sector risk assessments. Document methodology, inherent risk, controls, residual risk and action owners; update for material change and before new products or technologies launch.	Business risk assessment; methodology; data pack; change triggers; mitigation plan.	FIAMLA, s. 17(1)-(4); Mauritius Second National ML/TF Risk Assessment 2025
Establish senior-approved policies, controls and procedures proportionate to the business.	Cover CDD, beneficial ownership, ongoing monitoring, PEPs, sanctions, STRs, records, reliance, outsourcing, employee screening, training and independent audit. Monitor implementation, review and enhance the controls, and preserve a written record of the policies, changes and internal communication.	Senior-approved policy suite; control library; version history; communication and training records.	FIAMLA, s. 17A
Appoint the required Compliance Officer, MLRO and Deputy MLRO with suitable seniority and access.	Document appointments and reporting lines, provide unrestricted access to books, records and staff, and separate compliance oversight from the MLRO's internal-disclosure assessment and external-reporting role. Apply any sector-specific approval or notification requirement imposed by the Bank or FSC.	Appointment letters; fit-and-proper records; board minutes; access test; succession plan.	FIAML Regulations 2018, regs. 22, 26-27; applicable Bank or FSC requirements
Screen employees, train relevant staff and test the programme independently.	Apply risk-sensitive recruitment screening and continuing role-based training. Maintain an independent audit function that tests legal compliance and control effectiveness; set scope and frequency according to risk and applicable supervisory guidance rather than assuming a single statutory calendar for all sectors.	Screening files; training curriculum and attendance; independent audit plan and reports; remediation log.	FIAML Regulations 2018, reg. 22; FSC AML/CFT Handbook, chs. 12-13; Bank AML/CFT/CPF Guideline 2020
Apply group-wide and foreign-branch controls where relevant.	For a financial group, implement group policies, information-sharing safeguards and consistent controls across branches and majority-owned subsidiaries, subject to local-law constraints. Escalate any host-country impediment to the home supervisor and apply additional risk measures.	Group policy; jurisdiction gap analysis; information-sharing protocol; supervisor correspondence.	FIAML Regulations 2018, regs. 23-24; applicable Bank or FSC guidance

3. IDENTIFY AND VERIFY INDIVIDUAL CUSTOMERS

Identify and verify individual customers

CDD must establish the customer, anyone acting for the customer, the beneficial owner and the intended relationship using reliable, independent evidence.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Do not establish or maintain anonymous or fictitious-name accounts.	Configure onboarding and account controls to require a verified legal identity and to block fabricated, placeholder or materially inconsistent identity information.	Account-opening rules; blocked test cases; exception log.	FIAMLA, s. 17B
Identify and verify the customer and beneficial owner using reliable, independent sources.	Collect the prescribed natural-person information and verify it through valid official documents, data or information appropriate to the risk and channel. Identify and verify any representative and confirm the representative's authority to act.	Customer file; identity evidence; verification provenance; mandate or authority record.	FIAML Regulations 2018, regs. 3-4 and 8
Understand the purpose and intended nature of the relationship or occasional transaction.	Record the expected products, activity, counterparties, source and destination patterns and commercial rationale needed to create a defensible customer-risk and monitoring profile.	Purpose statement; expected-activity profile; risk score and rationale.	FIAML Regulations 2018, reg. 3(1)(d)
Apply CDD at every statutory trigger.	Trigger CDD when establishing a business relationship; conducting an occasional transaction at or above the prescribed threshold, including linked transactions, or a wire transfer in the circumstances specified by the Regulations; where ML/TF is suspected; and where there are doubts about previously obtained identification data. Keep any prescribed amount in a controlled legal register rather than hard-coding an unsupported universal threshold.	CDD trigger matrix; threshold register; workflow configuration; test results.	FIAML Regulations 2018, reg. 8
Verify identity before or during establishment and tightly control any permitted deferral.	Complete verification before or during establishment of the relationship or the occasional transaction. Defer completion only where the Regulation's conditions are met: it is essential not to interrupt normal business, verification occurs as soon as reasonably practicable and ML/TF risks are effectively managed. Use documented risk limits that prevent unrestricted use before completion.	Verification timestamps; deferral approval; restricted-service controls; completion monitoring.	FIAML Regulations 2018, reg. 9
Do not proceed where required CDD or EDD cannot be completed.	Do not open the account, commence the relationship or perform the transaction, or terminate the relationship as applicable, and file an STR where required. Preserve the decision without alerting the customer to an STR or related analysis.	Decline or exit record; investigation file; STR decision and filing reference; access restrictions.	FIAML Regulations 2018, regs. 12(3) and 13; FIAMLA, ss. 14 and 16

4. VERIFY BUSINESSES AND BENEFICIAL OWNERS

Verify businesses and beneficial owners

KYB must establish legal existence, governing powers, ownership and control, then trace the customer to the natural persons who ultimately own or control it.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify the legal person's identity, status and authority structure.	Obtain and verify the name, legal form and proof of existence, constitutional or governing instruments, powers that regulate and bind the entity, registered office and principal place of business, and relevant senior managing persons and authorised signatories.	Current CBRD or foreign-registry extract; constitutional documents; director and signatory records; address checks.	FIAML Regulations 2018, regs. 3 and 5
Apply the statutory legal-person beneficial-owner cascade accurately.	Identify and take reasonable measures to verify every natural person who ultimately has an ownership interest of 20 per cent or more. Where ownership does not identify the beneficial owner or there is doubt, identify control through other means; if no natural person is identified, record the relevant senior managing official. Preserve the actions taken and difficulties encountered.	Layered ownership chart; percentage calculation; control analysis; senior-manager fallback rationale; verification record.	FIAML Regulations 2018, reg. 6
Identify all relevant parties to trusts and similar arrangements.	For a trust, identify and reasonably verify the settlor, trustee, beneficiaries or class of beneficiaries, and where applicable the protector or enforcer, plus any other natural person exercising ultimate effective control. Identify equivalent persons for other legal arrangements.	Trust deed; party register; control chart; verified identity files; change undertaking.	FIAML Regulations 2018, reg. 7
Reconcile CBRD information without treating the registry as conclusive CDD.	Compare registry, constitutional, customer and independent evidence, investigate discrepancies and document why the identified natural persons satisfy the AML cascade. Obtain current information rather than relying only on a certificate or customer declaration.	CBRD search; discrepancy log; corroborating evidence; approved BO conclusion.	FIAML Regulations 2018, regs. 5-7; Companies Act 2001, ss. 11 and 91
Meet the company's own beneficial-ownership register and filing duties.	For a Mauritius company, maintain the separate, accurate and up-to-date register required by section 91, including the ownership structure and applicable nominee information; preserve records of identification action and the beneficial owner's written declaration; make information available forthwith to competent authorities. Confirm CBRIS filing events and deadlines, including the current change-filing rules. Companies incorporated before the relevant 2025 amendment had to meet the new declaration requirement by 30 June 2026.	Section 91 register; written BO or UBO declarations; CBRIS receipts; change log; authority-access procedure.	Companies Act 2001, ss. 11 and 91, as amended by Act 10 of 2024 and Finance Act 2025

5. APPLY PEP, ENHANCED AND REMOTE DUE DILIGENCE

Apply PEP, enhanced and remote due diligence

Higher-risk relationships require stronger information, approval, source and monitoring controls, while remote onboarding must achieve reliable identity assurance.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Detect foreign, domestic and international-organisation PEPs, including applicable family members and close associates.	Use risk-based systems to determine whether the customer or beneficial owner is a PEP and establish the connected-person relationship. Do not use database screening as a substitute for customer and ownership analysis.	PEP screening result; relationship analysis; match disposition; review history.	FIAML Regulations 2018, regs. 2 and 15
Apply the full foreign-PEP measures and risk-based domestic or international-organisation PEP measures.	For a foreign PEP who is a customer or beneficial owner, obtain senior-management approval, take reasonable measures to establish source of wealth and source of funds, and conduct enhanced ongoing monitoring. Apply those measures to domestic and international-organisation PEPs where the relationship is higher risk, in accordance with regulation 15.	Senior approval; source-of-wealth and source-of-funds corroboration; enhanced monitoring plan.	FIAML Regulations 2018, reg. 15
Apply enhanced CDD whenever higher ML/TF risk is identified.	Obtain additional customer, ownership, purpose, source-of-funds or source-of-wealth and transaction information, obtain senior approval where appropriate and increase monitoring in proportion to the identified risk. Apply relevant measures for countries identified by competent authorities or FATF, without treating nationality alone as a conclusion.	EDD checklist; enhanced evidence; approval; monitoring configuration; review schedule.	FIAML Regulations 2018, reg. 12; applicable Bank or FSC guidance
Use simplified CDD only for a substantiated lower-risk case.	Document why the lower risk is consistent with the latest national or supervisory risk assessment and apply measures commensurate with that risk. Do not use simplified CDD where there is knowledge, suspicion or reasonable grounds concerning ML/TF or another person acting behind the transaction.	Lower-risk rationale; NRA mapping; approved simplified measures; exclusion tests.	FIAML Regulations 2018, reg. 11
Control non-face-to-face and new-technology risk before launch.	Assess impersonation, document fraud, device, cyber, data, outsourcing and transaction risks; implement proportionate authentication, liveness or equivalent presence controls where used, reliable document checks, fraud controls and escalation. Follow the additional Bank or FSC expectations applicable to the licensee.	Channel risk assessment; vendor due diligence; model and liveness tests; exception and incident logs.	FIAMLA, s. 17(3); FIAML Regulations 2018; Bank AML/CFT/CPF Guideline 2020; FSC AML/CFT Handbook

6. MONITOR ACTIVITY AND REPORT SUSPICION

Monitor activity and report suspicion

Monitoring must stay aligned with current customer information and route suspicious completed, proposed and attempted activity confidentially to FIU through goAML.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Conduct ongoing monitoring throughout every business relationship.	Scrutinise transactions, including source of funds where necessary, for consistency with the customer, business and risk profile; keep CDD data current and relevant, with particular attention to higher-risk customers.	Monitoring scenarios; alert history; customer reviews; profile updates; tuning decisions.	FIAML Regulations 2018, reg. 3(1)(e)
Examine complex, unusually large, unusual-pattern and apparently purposeless activity.	Investigate background, purpose, parties, source and destination; record the analysis and determine whether an internal disclosure and external STR are required. Calibrate monitoring to the business model rather than relying on generic rules alone.	Case file; supporting information; analyst rationale; escalation decision.	FIAML Regulations 2018, regs. 12 and 28-29; applicable Bank or FSC guidance
File an STR within 5 working days after suspicion arose.	The reporting person or auditor must file electronically with FIU through the production goAML environment no later than 5 working days after the suspicion arose. Cover completed, proposed and attempted transactions where the statutory suspicion test is met; do not wait for proof of an offence.	Suspicion timestamp; MLRO assessment; goAML acknowledgement; deadline-control report.	FIAMLA, s. 14(1); FIU STR reporting page; FIU Guidance Note 4
Register the reporting person and maintain production goAML readiness.	Complete FIU organisation registration through the MLRO, maintain authorised users, delegation and current contact details, test access and retain a controlled contingency process consistent with FIU instructions.	Registration acceptance; user register; access test; delegation record; continuity exercise.	FIAMLA, s. 14C; Registration by Reporting Person Regulations 2019; FIU goAML guides
Protect STR confidentiality and prevent tipping off.	Restrict STR, internal disclosure and FIU-request information to authorised personnel; ensure customer communications, exits and information requests do not reveal that an STR has been or will be made or that an investigation is underway.	Need-to-know matrix; confidential case repository; disclosure log; staff training.	FIAMLA, ss. 16 and 16A; FIU Guidance Note 4
Respond promptly and completely to lawful FIU and supervisory requests.	Preserve data lineage, identify an accountable response owner, authenticate the request, provide complete records securely and retain the request, response and approval trail without compromising confidentiality.	Request register; response package; approval and delivery evidence; legal hold.	FIAMLA, ss. 10, 19E and 19J-19K

7. IMPLEMENT TARGETED FINANCIAL SANCTIONS

Implement targeted financial sanctions

UN and domestic designations require screening, immediate prohibitions and freezing, prescribed reporting and strict controls against making assets or services available.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen against both listed-party and designated-party information.	Screen customers, beneficial owners, controllers, counterparties, payees and relevant transaction parties at onboarding, before execution and promptly after list updates. Use the National Sanctions Secretariat and UN lists and record fuzzy-match and ownership-control logic.	List inventory; screening logs; update timestamps; match procedures; control tests.	Sanctions Act 2019, ss. 7, 18-25 and 41; National Sanctions Secretariat guidance
Apply prohibitions and freezes immediately.	Where the Act requires a prohibition or freeze, do not deal with the funds or other assets and do not make funds, assets or services available, directly or indirectly, to or for the benefit of the listed or designated party. In the Act, immediately means without delay and no later than 24 hours.	Freeze timestamp; blocked-transaction record; asset inventory; legal and compliance decision.	Sanctions Act 2019, ss. 18-25 and definition of immediately
Submit the prescribed match and asset reports to the correct authorities.	Report screening outcomes, including funds or no funds identified where required by the applicable procedure, to the National Sanctions Secretariat and the AML/CFT supervisor. Where information relating to a listed party is known to a reporting person, submit it immediately to FIU under the statutory route and file an STR where required.	NSSEC report; supervisor report; FIU STR acknowledgement; zero-asset or positive-asset evidence.	Sanctions Act 2019, ss. 25 and 39-41; FIU TFS FAQ; applicable Bank or FSC procedure
Do not release frozen assets without lawful authority.	Maintain the freeze until delisting, lapse, court or statutory authorisation, and process permitted expenses or other exceptions only through the prescribed procedure. Verify delisting before unfreezing and preserve the approval trail.	Freeze register; licence or order; delisting verification; unfreeze approval and timestamp.	Sanctions Act 2019, ss. 26-34; National Sanctions Secretariat guidance
Test sanctions controls independently.	Test list ingestion, aliases, transliteration, ownership and control, rescreening, payment interdiction, case escalation, reporting and unfreezing. Document gaps and remediate without waiting for a live match.	Sanctions test plan; seeded-match results; issue register; remediation evidence.	Sanctions Act 2019, ss. 40-41; Bank TFS implementation page; FSC TFS guidance

8. RETAIN RECORDS AND SUPPORT RECONSTRUCTION

Retain records and support reconstruction

AML records must remain complete, retrievable and sufficient to reconstruct customers, decisions and transactions over the statutory period.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain customer and beneficial-owner records for at least 7 years after the relationship ends.	Keep identification and verification evidence, ownership and control analysis, customer risk assessments and business correspondence for at least 7 years after termination of the business relationship, subject to any longer lawful hold or sector rule.	Retention schedule; lifecycle configuration; sample retrieval; legal-hold register.	FIAMLA, s. 17F; FIAML Regulations 2018, reg. 14
Retain domestic and international transaction records for at least 7 years after completion.	Preserve sufficient originator, beneficiary, amount, currency, date, account, channel, agent, screening and decision data to reconstruct each transaction and answer FIU or supervisory requests swiftly.	Transaction archive; data-lineage map; reconstruction test; access log.	FIAMLA, s. 17F; FIAML Regulations 2018, reg. 14
Retain each STR and its supporting record for at least 7 years from filing.	Store the internal disclosure, MLRO assessment, supporting evidence, filed report, acknowledgement and any FIU correspondence in a segregated, access-controlled repository.	STR archive; goAML receipt; access matrix; retrieval test.	FIAML Regulations 2018, regs. 14 and 27-29; FIU Guidance Note 4
Extend retention when a competent authority requires it.	Implement legal holds capable of overriding ordinary deletion where FIU, the Bank, FSC, an investigatory authority or another competent authority requires records to be preserved for longer.	Legal-hold notice; system lock; release approval; audit trail.	FIAML Regulations 2018, reg. 14; applicable FIU, Bank or FSC requirement
Make records swiftly available without weakening confidentiality.	Index records by customer, beneficial owner, account, transaction and case; test retrieval and controlled export; ensure only authorised persons can access STR and sanctions information.	Retrieval service levels; access logs; test reports; secure-delivery procedure.	FIAML Regulations 2018, regs. 14 and 22(2); FIAMLA, ss. 16 and 19J-19K

9. PROTECT PERSONAL AND BIOMETRIC DATA

Protect personal and biometric data

KYC, screening and monitoring data remain subject to the Data Protection Act 2017 even where processing is necessary for a legal AML obligation.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Register as a controller and, where applicable, as a processor before processing.	Complete the Data Protection Office registration applicable to each legal role. Registration certificates are valid for 3 years; renew them and notify changes in registered particulars within 14 days. Designate the officer responsible for data-protection compliance.	Controller or processor certificate; renewal calendar; change notices; DPO appointment.	Data Protection Act 2017, ss. 14-18 and 22(2)(e); Data Protection (Fees) Regulations 2020
Map every KYC processing purpose to a lawful basis and minimise collection.	Document purposes, lawful grounds, necessity, data categories, recipients, retention, rights and security for identity, biometric, device, transaction, screening and investigation data. Separate mandatory compliance processing from optional analytics and marketing.	Record of processing; lawful-basis assessment; privacy notice; minimisation review.	Data Protection Act 2017, ss. 22-23 and 27-33
Apply special-category safeguards to biometrics, offences and PEP-related data.	Treat biometric data uniquely identifying a person and offence or alleged-offence information as special-category data. Document the section 28 lawful basis and the additional section 29 condition, limit access and protect templates and source images throughout their lifecycle.	Special-category assessment; biometric architecture; access controls; deletion and security tests.	Data Protection Act 2017, ss. 2, 28-29 and 31
Complete a DPIA before high-risk identity or monitoring processing.	Perform a data-protection impact assessment before processing likely to create high risk, including large-scale special-category processing or systematic and extensive automated evaluation with significant effects. Consult the Office where residual high risk or another consultation trigger remains.	DPIA; necessity and proportionality assessment; mitigation plan; consultation record.	Data Protection Act 2017, ss. 34-35
Control transfers of personal data outside Mauritius.	Map every cloud, verification, screening and support location and satisfy one of the section 36 transfer conditions. Where appropriate safeguards cannot be provided, obtain the Office's prior authorisation under section 35 rather than relying on an undisclosed offshore processor.	Transfer map; safeguards; contracts; explicit-consent record where applicable; DPO authorisation.	Data Protection Act 2017, ss. 35-36
Operate the statutory personal-data-breach workflow.	Require processors to notify the controller without undue delay. Unless the breach is unlikely to create risk to rights and freedoms, notify the Commissioner no later than 72 hours after awareness, explain delay where applicable and communicate high-risk breaches to affected persons as required.	Incident log; awareness timestamp; DPO notification; data-subject communication; lessons learned.	Data Protection Act 2017, ss. 25-26

10. OPERATE PAYMENT-SERVICE CONTROLS

Operate payment-service controls

Payment products add Bank of Mauritius licensing, governance, security, safeguarding and reporting duties to the general FIAMLA baseline.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Obtain Bank authorisation or a pay ment-service-provider licence where required.	Classify system-operation, clearing, settlement and payment services under the National Payment Systems Act and the 2021 Regulations as amended in 2024. Submit the prescribed application and do not rely on a technology-provider label to conduct a regulated service without permission.	NPS legal classification; authorisation or licence; application file; conditions register.	National Payment Systems Act 2018; NPS (Authorisation and Licensing) Regulations 2021, as amended in 2024
Provide only the services and functions covered by the permission.	Map acquiring, payment-account, transfer, card, cash-in or cash-out, payment-initiation, aggregation and other functions to the licence and current Bank framework. Verify counterparties on the Bank's current licensee list.	Service-to-licence map; regulator-register check; partner due diligence; product approval.	NPS Act 2018; NPS licensing regulations; Bank of Mauritius payment licensee register
Apply the Bank AML/CFT/CPF Guideline to NPS licensees within scope.	Implement the Guideline's customer-risk, CDD, monitoring, wire-transfer, record, governance and sanctions expectations in addition to FIAMLA and the Regulations. Do not present the Bank Guideline as governing an FSC-only licensee outside the Bank's stated scope.	Bank-guideline gap analysis; control map; board approval; supervisory-return calendar.	Bank of Mauritius AML/CFT/CPF Guideline 2020, paras. 2.01-2.06
Maintain safe, secure, efficient and resilient payment operations.	Implement governance, access, fraud, cyber, continuity, reconciliation, incident and customer-protection controls required by the Act, licence conditions and current Bank directives or guidelines. Preserve complete transaction traceability for AML monitoring and authority requests.	Governance records; security architecture; reconciliations; continuity tests; incident reports.	National Payment Systems Act 2018, including ss. 17 and 24; applicable Bank directives and licence conditions
Apply the July 2026 Payment Aggregator Guideline only where the activity falls within its scope.	For an aggregator model, assess the current Bank Guideline for Payment Aggregators, licensing position, merchant due diligence, settlement, risk, security and consumer obligations. Record which provisions are binding through the Act, licence or direction and which are supervisory guidance.	Aggregator perimeter assessment; merchant-control framework; settlement map; Bank correspondence.	Bank of Mauritius Guidelines page; Guideline for Payment Aggregators, 10 July 2026

11. LAUNCH, OVERSEE AND EVIDENCE COMPLIANCE

Launch, oversee and evidence compliance

Publication-ready policies are not enough; every rule needs an owner, tested system implementation and retrievable evidence.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Run a documented pre-launch regulatory gate.	Confirm perimeter, licences, FIU and goAML registration, CDD and beneficial-owner rules, PEP and sanctions controls, monitoring, records, CBRD status, Data Protection Office registration and DPIA, payment permission, outsourcing and incident readiness before production.	Launch checklist; accountable approvals; unresolved-risk register; production decision.	FIAMLA; FIAML Regulations 2018; applicable Bank, FSC, CBRD, NSSEC and DPO instruments
Control reliance and outsourcing without transferring responsibility.	Use third-party CDD reliance only where the statutory conditions are met, obtain core CDD information immediately and ensure identification documents are available without delay. Assess processors and technology providers, contract security and audit rights and maintain the reporting person's responsibility.	Third-party assessment; reliance decision; contract; data-access test; exit plan.	FIAMLA, ss. 17D-17F; FIAML Regulations 2018, reg. 21; applicable Bank or FSC outsourcing guidance
Track legal and supervisory change from the primary authorities.	Monitor FIU, Bank, FSC, CBRD, National Sanctions Secretariat, Data Protection Office and FATF publications. Treat bills and consultation papers as horizon-scanning items until enacted or brought into force, and update controls only against verified legal status.	Legal inventory; alert subscriptions; impact assessments; implementation tickets.	Official FIU, Bank, FSC, CBRD, NSSEC, DPO and FATF publications
Test control effectiveness and remediate findings.	Use risk-based compliance monitoring and independent audit to test onboarding, beneficial ownership, PEPs, sanctions, payment, transaction monitoring, STR, privacy and recordkeeping controls. Report material deficiencies to senior management and the board and track them to evidence-based closure.	Monitoring plan; audit reports; issue register; governance reporting; closure evidence.	FIAML Regulations 2018, reg. 22; Bank AML/CFT/CPF Guideline 2020; FSC AML/CFT Handbook
Preserve a defensible control-to-law record.	For every material obligation, retain the primary source, interpretation, scope, configuration, test, owner, approval and effective date. Label Bank and FSC guidance as guidance and the VOVE article as contextual implementation material, not legal authority.	Obligations register; control-to-law map; source archive; approvals; release and test history.	FIAMLA, ss. 17 and 17A; applicable primary and sector sources

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.

Financial Intelligence and Anti-Money Laundering Act 2002, current Bank of Mauritius publication
Bank of Mauritius · Primary legislation
Open official source

FIAMLA consolidation updated as at 2024
Financial Intelligence Unit Mauritius · Primary legislation consolidation
Open official source

Financial Intelligence and Anti-Money Laundering Regulations 2018
Bank of Mauritius · Primary regulation
Open official source

Financial Intelligence and Anti-Money Laundering (Registration by Reporting Person) Regulations 2019
Bank of Mauritius · Primary regulation
Open official source

Financial Intelligence and Anti-Money Laundering (Administrative Penalties) Regulations 2025
Financial Intelligence Unit Mauritius · Primary regulation
Open official source

Report a Suspicious Transaction: 5-working-day deadline and electronic filing
Financial Intelligence Unit Mauritius · Official reporting procedure
Open official source

goAML production environment and registration resources
Financial Intelligence Unit Mauritius · Official reporting portal
Open official source

Guidance Note 4 on suspicious transaction reporting
Financial Intelligence Unit Mauritius · Official FIU guidance
Open official source

AML/CFT/CPF framework, 2025 national risk assessment and 2026-2029 strategy
Bank of Mauritius · Official AML portal
Open official source

Guideline on AML/CFT and Proliferation, January 2020
Bank of Mauritius · Sector supervisory guidance
Open official source

Current FSC AML/CFT Handbook landing page
Financial Services Commission Mauritius · Official sector guidance portal
Open official source

FSC AML/CFT Handbook, current published PDF
Financial Services Commission Mauritius · Sector supervisory guidance
Open official source

Companies Act 2001, amended through the Finance Act 2025
Corporate and Business Registration Department · Primary legislation
Open official source

AML/CFT/CPF (Miscellaneous Provisions) Act 2024, including company beneficial-ownership amendments
National Assembly of Mauritius · Primary amending legislation
Open official source

United Nations Sanctions Act 2019, current 2026 consolidation
National Sanctions Secretariat · Primary legislation
Open official source

National Sanctions Secretariat legislation and current list resources
National Sanctions Secretariat · Official sanctions portal
Open official source

Guidelines on implementation of targeted financial sanctions
Government of Mauritius · Official sanctions guidance
Open official source

Implementation of targeted sanctions and reporting expectations
Bank of Mauritius · Official supervisory procedure
Open official source

National Payment Systems Act 2018, current Bank of Mauritius publication
Bank of Mauritius · Primary legislation
Open official source

National Payment Systems (Authorisation and Licensing) Regulations 2021
Bank of Mauritius · Primary regulation
Open official source

National Payment Systems licensing and current licensee register
Bank of Mauritius · Official licensing portal
Open official source

Payment-system guidelines, including Guideline for Payment Aggregators dated 10 July 2026
Bank of Mauritius · Official sector guidance portal
Open official source

Data Protection Act 2017
Data Protection Office Mauritius · Primary legislation
Open official source

Registration and renewal of controllers and processors
Data Protection Office Mauritius · Official registration procedure
Open official source

Data Protection (Fees) Regulations 2020 and registration forms
Data Protection Office Mauritius · Primary regulation and official forms
Open official source

Jurisdictions under increased monitoring, 19 June 2026
FATF · Official FATF statement
Open official source

Mauritius removed from increased monitoring, October 2021
FATF · Official FATF statement
Open official source

AML Compliance in Mauritius 2026
VOVE ID · Contextual implementation guide; not legal authority
Open contextual guide

Document control

Version 1.0 / Published 15 July 2026 / Last reviewed 15 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general information, not legal advice. It reflects official materials available on 15 July 2026. Applicability depends on the entity, licence, product, customer and sector. Confirm current requirements, reporting formats, supervisory expectations, payment permissions, sanctions notices and privacy filings with FIU Mauritius, the Bank of Mauritius, the Financial Services Commission, the National Sanctions Secretariat, the Corporate and Business Registration Department, the Data Protection Office and qualified Mauritian counsel before launch.