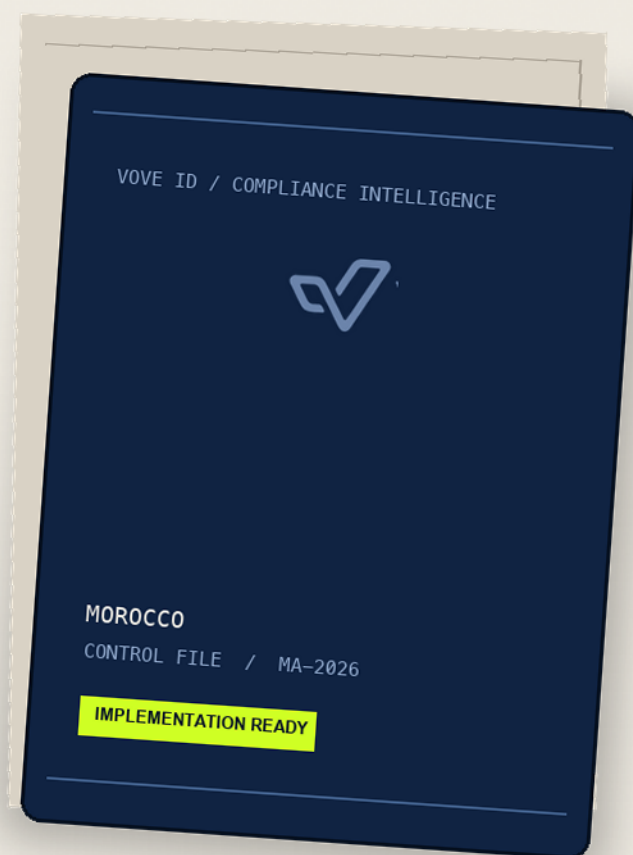


MOROCCO



MOROCCO / MA



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION



[READ THIS FIRST](#)

Morocco KYC, KYB & AML Compliance Checklist

A practical implementation checklist for regulated businesses operating in Morocco, with a focused overlay for banks, payment institutions and other entities supervised by Bank Al-Maghrib. It converts customer due diligence, beneficial ownership, remote onboarding, suspicious reporting, sanctions, monitoring, records and data-protection duties into operational controls and audit evidence.

Financial intelligence unit	Autorite Nationale du Renseignement Financier (ANRF)
Banking and payments supervisor	Bank Al-Maghrib
BAM beneficial-owner threshold	More than 25%, plus effective control
Suspicion reporting	Immediately once suspicion exists
Record retention	10 years under the AML framework
FATF public list	Not listed as of 19 June 2026

Scope and legal framework

Law No. 43-05 on combating money laundering, as amended and supplemented, including by Law No. 12-18; Decree No. 2-21-484 governing the national UN sanctions commission; Bank Al-Maghrib Circular No. 5/W/2017 on due diligence, as amended; Bank Al-Maghrib Directives No. 2/W/2019 and No. 3/W/2019; Bank Al-Maghrib Letter Circular No. 1/DSB/2020 on remote account opening; banking and sector-specific supervisory rules; Law No. 09-08 on personal-data processing and its implementing measures.

FATF context

Morocco was removed from FATF increased monitoring in February 2023 and was not named in FATF's jurisdictions under increased monitoring or jurisdictions subject to a call for action statements published on 19 June 2026. This is not a low-risk designation and does not replace documented customer, ownership, product, channel and geographic risk assessment.

IMPORTANT

This checklist is general compliance information, not legal advice. Law No. 43-05 provides the national baseline, while the Bank Al-Maghrib material used here applies specifically to credit institutions and assimilated bodies, including payment institutions. Capital-markets, insurance, real-estate, legal, accounting and other covered sectors must add the current AMMC, ACAPS or other competent-supervisor rules. Confirm amendments, forms, thresholds, reporting channels and CNASNU decisions against current official Arabic or French texts before implementation.

[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. APPLICABILITY AND GOVERNANCE

Applicability and governance

Map every regulated activity, assign accountable governance and operate an appropriately resourced AML/CFT control framework.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map the national and sector perimeter	Document every reporting entity and activity subject to Law No. 43-05. Map credit institutions, assimilated bodies and supervised financial conglomerates to Bank Al-Maghrib; currency-exchange companies to the Office des Changes; capital-market entities to AMMC; and insurance, reinsurance, insurance intermediaries, qualifying pension institutions and supervised financial conglomerates to ACAPS. Map lawyers, notaries and adouls to the governmental authority responsible for justice; offshore holding companies, chartered and accredited accountants to the governmental authority responsible for finance; casinos and gambling establishments jointly to the governmental authorities responsible for interior and finance; real-estate agents to the governmental authority responsible for housing; and dealers in precious metals, stones, antiquities and art to Customs and Indirect Tax Administration. ANRF supervises entities for which no other authority is designated. Apply Article 5's activity-specific DNFBP scope and its MAD 30,000 casino and MAD 150,000 cash-dealer thresholds.	Entity-perimeter memo, licence inventory, activity and threshold matrix, supervisor mapping and named obligations owner	Law 43-05, arts. 5 and 13.1, as amended by Law 12-18
Apply the correct Bank Al-Maghrib overlay	For a Bank Al-Maghrib-supervised institution, map Circular 5/W/2017, Directive 2/W/2019 on customer and beneficial-owner identification, Directive 3/W/2019 on the risk-based approach and applicable product, agent, outsourcing, control and reporting rules.	BAM obligations register, control mapping, legal-change process and implementation owners	BAM Circular 5/W/2017; Directives 2/W/2019 and 3/W/2019
Make governance responsible for effectiveness	Require the governing and executive bodies to approve the AML/CFT framework, risk appetite, customer-acceptance rules and material remediation; receive meaningful management information; and ensure the control function has sufficient authority, independence, people, systems and access.	Approved framework, committee terms, minutes, resource assessment, dashboards and remediation log	Law 43-05; BAM Circular 5/W/2017; BAM/ANRF AML/CFT Guide
Maintain an independent vigilance structure	For a Bank Al-Maghrib-supervised institution, maintain an independent structure with sufficient qualified resources to administer vigilance and internal monitoring. It must centralise agency reports, examine unusual or complex transactions within a reasonable period, maintain enhanced monitoring of suspicious and higher-risk relationships, keep executive management continuously informed, liaise with ANRF and have timely access to all required customer and transaction information. Communicate to ANRF the directors and employees authorised to liaise and submit reports, together with the required description of the internal vigilance framework.	Appointment, organisation chart, mandate, resources, access profile, ANRF liaison notifications, framework description and filing authority	Law 43-05, art. 9; BAM Circular 5/W/2017, arts. 7-8
Maintain current policies and procedures	Document customer acceptance, identification, beneficial ownership, customer risk, EDD, PEPs, sanctions, unusual activity, ANRF reporting, wires, agents, outsourcing, records, training, assurance and CNBP controls. Update them after legal, product, technology or risk change.	Policy suite, approvals, regulatory mapping, version history and staff attestations	Law 43-05; BAM Circular 5/W/2017

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Train, test and remediate	Provide continuous, role-appropriate AML/CFT training and regularly assess its effectiveness. For a Bank Al-Maghrib-supervised institution, perform the permanent and periodic controls required over the vigilance framework, policies, procedures, systems and staff implementation, and submit results and remediation plans to the audit committee. Apply independent assurance where required by the institution's control framework or another binding sector rule; otherwise treat independent testing as a recommended control rather than a universal statutory duty.	Training plan and effectiveness results, permanent and periodic control reports, audit-committee reporting, issue register and closure proof	BAM Circular 5/W/2017, arts. 9-11

2. KYC AND REMOTE ONBOARDING

KYC and remote onboarding

Identify customers and representatives from reliable sources, understand the relationship and make remote onboarding equivalent to physical presence.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify every relationship	Before establishing a relationship, identify and verify the customer, representative and persons acting on the customer's behalf using current, reliable and independent documents, data or information. Prohibit anonymous or manifestly fictitious accounts.	Identity record, document and database checks, representative authority, verification result and quality review	Law 43-05; BAM Circular 5/W/2017, arts. 14-15 and 25
Apply the occasional-customer rule	For a Bank Al-Maghrib-supervised institution, identify and verify an occasional customer and the beneficial owner of the transaction regardless of transaction amount, as required by the amended circular. Do not substitute an unsupported general threshold.	Occasional-customer workflow, identity and beneficial-owner checks, transaction record and exception report	BAM Circular 5/W/2017, art. 14, as amended
Understand purpose and expected activity	Record the purpose and intended nature of the relationship, occupation or business, products, expected volumes, channels, counterparties, geographies and source of funds where risk requires. Use the profile as the baseline for monitoring.	Customer profile, expected-activity fields, source evidence, risk rationale and review triggers	Law 43-05; BAM Circular 5/W/2017; Directive 2/W/2019
Stop and report failed CDD	When identification data are incomplete or manifestly fictitious, do not establish the relationship or execute the operation and immediately submit a suspicion report. If appropriate vigilance cannot be completed for an existing relationship, stop operations, terminate the relationship and immediately report to ANRF.	Rejected or restricted case, reason code, closure decision, ANRF report and non-tipping-off controls	BAM Circular 5/W/2017, art. 26
Make remote identification equivalent to presence	Before a bank or payment institution opens accounts remotely, deploy reliable and secure technology that provides risk-based equivalence to physical presence, verifies the authenticity of identity documents, mitigates impersonation and fraud and protects personal data.	Remote-onboarding design, document-authenticity result, biometric or equivalent control, fraud signals, security testing and privacy assessment	BAM Letter Circular 1/DSB/2020, arts. 1-3
Document remote-onboarding compliance	Maintain a formal demonstration that the remote-account-opening system complies with Law No. 43-05, Letter Circular 1/DSB/2020 and the relevant FATF new-technology and CDD principles. Reassess after material technology, vendor or fraud-pattern change.	Compliance assessment, control mapping, approval, test results, change review and vendor oversight	BAM Letter Circular 1/DSB/2020, art. 3

3. KYB AND BENEFICIAL OWNERSHIP

KYB and beneficial ownership

Verify legal existence, authority, ownership and effective control, and reconcile institution-held information with official records.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify the legal person and representatives	Verify legal name, form, registration, registered office, principal activity, tax identifiers, licences, constitutional documents, directors or managers, authorised representatives and each representative's authority using reliable independent sources, including OMPIC records where available.	Registry extract, constitutional records, tax and licence checks, representative authority and discrepancy log	Law 43-05; BAM Circular 5/W/2017, art. 15; OMPIC services
Identify natural-person beneficial owners	For a company under the Bank Al-Maghrib circular, identify and verify every natural person who directly or indirectly holds more than 25% of capital or voting rights, or exercises effective control by any other means over management, direction, administration or the general meeting. Identify the natural person for whose account an activity or transaction is conducted.	Ownership chart to natural persons, percentages, control analysis, identity verification and account-beneficiary assessment	BAM Circular 5/W/2017, art. 1, as amended
Apply ownership tests beyond companies	For another legal person or legal arrangement, identify the natural persons with rights over more than 25% of assets, those expected to acquire such rights under a legal instrument, and every person who ultimately controls the structure. Apply the trust or arrangement-party requirements relevant to the legal form.	Legal-form analysis, constitutional or trust instruments, asset-rights map, controllers and verification records	BAM Circular 5/W/2017, arts. 1 and 15
Use the beneficial-owner register as a source, not a substitute	Obtain available beneficial-owner information through the OMPIC-managed register and compare it with the customer's declaration and ownership evidence. Resolve missing, stale or inconsistent information before approval and do not treat registry access as replacing independent AML verification.	RBE request or result, customer declaration, reconciliation, supporting ownership documents and resolved discrepancy	Law 43-05 transparency framework; OMPIC Beneficial Owners Register
Verify the licensed business and operating reality	Confirm each required licence and compare the stated business to websites, premises, contracts, settlement accounts, customers, counterparties and transaction activity. Escalate shell characteristics, nominee control, unexplained ownership layers and inconsistent revenue or payment flows.	Regulator and licence check, operating-footprint evidence, website review, account match and escalation decision	Law 43-05; BAM Circular 5/W/2017; applicable sector licence
Keep corporate CDD current	Refresh registration, ownership, control, representative, licence and business-profile information periodically according to risk and immediately after a material trigger. Re-screen new owners and controllers and recalculate the risk rating.	Review calendar, registry-change alerts, updated chart, screening, risk decision and overdue restrictions	BAM Circular 5/W/2017; Directive 2/W/2019

4. RISK, PEPS AND TARGETED FINANCIAL SANCTIONS

Risk, PEPs and targeted financial sanctions

Operate documented institutional and customer risk assessment, enhanced PEP controls and immediate CNASNU sanctions implementation.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Assess institutional ML/TF risk	For a Bank Al-Maghrib-supervised institution, analyse and evaluate ML/TF risk at least annually across customer categories, countries and geographic areas, products, services, operations and distribution channels. Document results, present them to the governing body and implement proportionate limits and controls by product, service, period, transaction, channel and geography. Update sooner after a material risk, product, technology or business change.	Approved methodology, annual assessment, governing-body record, limits, residual-risk decisions, update log and remediation plan	BAM Circular 5/W/2017, art. 5; Directive 3/W/2019
Assign and explain customer risk	Classify every relationship using documented factors and defensible data. Ensure higher-risk ratings drive senior approval, deeper source checks, stronger monitoring and more frequent review; control and document overrides.	Scoring methodology, input data, risk rating, override record, approver and next review date	BAM Circular 5/W/2017; Directive 3/W/2019
Identify politically exposed persons	Screen customers, beneficial owners, representatives, family members and close associates to determine whether PEP risk applies under the current national and sector definitions. Repeat screening throughout the relationship and after ownership change.	PEP screening, relationship map, source data, alert decision and periodic rescreening	Law 43-05; BAM Circular 5/W/2017
Apply mandatory PEP measures	Before establishing or continuing a PEP relationship, obtain the required senior-management approval, take reasonable measures to establish source of wealth and source of funds and apply enhanced ongoing monitoring proportionate to risk.	Senior approval, source-of-wealth and source-of-funds corroboration, EDD file and monitoring plan	Law 43-05; BAM Circular 5/W/2017
Screen current CNASNU and UN lists	Register the institution and its permanent correspondents for the applicable CNASNU platform, list-update and notification services. Permanently and systematically screen prospective, existing and occasional customers, beneficial owners, controllers, representatives and every transaction party before onboarding, before executing a transaction and immediately after each CNASNU or UN list update.	CNASNU registration, correspondent appointments, authoritative-list inventory, update log, screening results, alert decisions and quality assurance	Law 43-05, art. 32; Decree 2-21-484; CNASNU Practical Guide
Freeze, prohibit and report without delay	For a confirmed or unresolved suspected match, act immediately and without prior notice. Freeze all funds, assets and economic resources owned or controlled directly or indirectly, wholly or jointly, including generated income and assets held through an entity owned or controlled by the designated person or by a person acting on that person's behalf or direction. Prohibit transfer, conversion, disposition, movement, access, establishment of a relationship and direct or indirect provision or availability of funds, assets, economic resources, financial services or related services. Notify CNASNU concomitantly through its prescribed platform of the analysis and measures; maintain them until CNASNU issues the applicable confirmation, exemption, delisting or unfreezing decision. Record attempted transactions and make any separate ANRF suspicion report required by the facts.	Match validation, freeze and prohibition record, attempted activity, concomitant CNASNU notification, asset-scope analysis, ANRF decision and release authority	Law 43-05, art. 32; Decree 2-21-484; CNASNU Practical Guide

5. ENHANCED DUE DILIGENCE

Enhanced due diligence

Apply proportionate additional measures to higher-risk customers, products, structures, geographies and counterparties.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply EDD to higher-risk relationships	Collect additional identity, ownership, business, purpose, source-of-funds and source-of-wealth information; obtain management approval; increase the frequency and depth of monitoring; and document why residual risk is acceptable.	EDD checklist, corroborating records, approval, monitoring plan and review date	Law 43-05 ; BAM Circular 5/W/2017, art. 40 ; Directive 3/W/2019
Control correspondent banking	Before opening a foreign correspondent relationship, understand the institution's activities, reputation, quality of supervision, ownership and AML controls; establish responsibilities; obtain required approval; and prohibit shell-bank relationships and uncontrolled payable-through access.	Correspondent questionnaire, public-source checks, control assessment, approval, agreement and periodic review	BAM Circular 5/W/2017, arts. 41-44
Control non-face-to-face and anonymity risk	Apply dedicated policies and additional safeguards to products, practices or technologies that do not involve physical presence or may facilitate anonymity. Tie control strength to documented impersonation, fraud, laundering and evasion risk.	Channel risk assessment, fraud and liveness controls, transaction limits, monitoring and exception review	BAM Circular 5/W/2017, art. 37 ; BAM Letter Circular 1/DSB/2020
Govern agents and outsourced providers	Perform pre-appointment due diligence; contract for AML, security, confidentiality, records, incident reporting and audit rights; include agents in the institution's AML/CFT system; monitor compliance; and retain accountability for outsourced controls.	Due diligence, contract, agent register, training, monitoring, audit results and termination process	BAM Circular 5/W/2017, as amended ; applicable outsourcing and agent rules
Investigate unusual or complex activity	Promptly examine complex, unusually large, linked or otherwise unusual transactions and patterns with no apparent lawful or economic purpose. Document the background and purpose, escalate to the responsible structure and immediately report when suspicion exists.	Alert, investigation chronology, customer explanation, independent corroboration, decision and ANRF receipt where filed	Law 43-05 ; BAM Circular 5/W/2017, art. 39

6. ONGOING MONITORING, PAYMENTS AND FINTECH CONTROLS

Ongoing monitoring, payments and fintech controls

Keep customer knowledge current, monitor behaviour and preserve complete payment information across the transaction chain.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor throughout the relationship	Monitor transactions against the customer's purpose, expected activity, business, risk and source-of-funds profile. Use scenarios suited to products and channels, link related activity and provide investigators with complete data and case context.	Monitoring coverage, data lineage, scenario inventory, alerts, tuning, quality assurance and management metrics	Law 43-05 ; BAM Circular 5/W/2017 ; BAM/ANRF AML/CFT Guide
Refresh on schedule and trigger	Update identity, beneficial ownership, business, expected activity, PEP, sanctions and risk information regularly according to risk and after a material trigger, including unusual behaviour, ownership change, new product use, adverse information or document expiry.	Risk-based review schedule, trigger feed, updated CDD, rescreening, risk decision and overdue dashboard	BAM Circular 5/W/2017 ; Directive 2/W/2019
Carry complete cross-border and domestic transfer information	For every cross-border wire or funds transfer sent or received in a relationship or for an occasional customer, regardless of amount, include the required names or legal names of the originator and beneficiary and, where applicable, the beneficial owner; account numbers or traceable unique reference; originator address, customer identifier or date and place of birth; and transaction purpose. Intermediaries must preserve all accompanying information and detect missing fields. Domestic transfers must carry the same information unless it can be made available to the beneficiary institution or competent authority by another method within three business days after request; at minimum carry the originator account or unique reference permitting retrieval.	Payment-message fields, validation rules, sample domestic and cross-border transfers, three-business-day retrieval test, batch traceability and exception report	BAM Circular 5/W/2017 , arts. 27-29, as amended
Control incomplete payment information	Beneficiary and intermediary institutions must apply risk-based procedures to transfers received without required information. Suspend and request repair within a reasonable period; reject where information is not received within the permitted period; and terminate a correspondent relationship where the originating institution cannot comply. Submit an immediate suspicion report when missing information or surrounding facts create suspicion.	Repair and reject rules, exception queue, counterparty escalation, termination decision, ANRF report and response-time logs	BAM Circular 5/W/2017 , arts. 28-29, as amended
Assess new products and technology before use	Before launch or material change, assess customer-identification, fraud, cyber, anonymity, sanctions, monitoring, outsourcing, privacy and record risks. Approve proportionate controls and test that compliance evidence is complete and retrievable.	Pre-launch risk assessment, control design, approval, test results, monitoring plan and post-launch review	Law 43-05 ; BAM Circular 5/W/2017 , art. 37; Directive 3/W/2019
Do not infer permission for virtual-asset activity	Do not treat draft Law No. 42.25 or announced reform as present authorisation. The 5 April 2022 joint warning by Bank Al-Maghrib, AMMC and the Office des Changes states that use of virtual currencies remains unauthorised in Morocco and may violate current foreign-exchange rules. Do not offer, facilitate or accept virtual-currency activity unless the competent authority confirms the proposed activity is lawful under an enacted and effective framework. Reassess immediately if Law No. 42.25 or another binding framework is enacted and published.	Current legal opinion, regulator confirmation, product restriction, regulatory-change trigger and monitoring rules	Joint Moroccan Financial Authorities Warning, 5 April 2022

7. REPORTING, RECORDS, PRIVACY AND ASSURANCE

Reporting, records, privacy and assurance

Report suspicion immediately, preserve reconstructable records and obtain the required CNDP clearance before processing personal data.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Report suspicion immediately	Submit a suspicion report to ANRF immediately when the institution knows, suspects or has reasonable grounds under the applicable rule, including linked or attempted activity where reportable. Do not wait for a monetary threshold or proof of predicate crime.	Case chronology, responsible-person decision time, ANRF report, submission receipt and escalation record	Law 43-05, arts. 9-11; BAM Circular 5/W/2017
Prevent tipping off and protect confidentiality	Restrict access to reporting information and prevent disclosure to the customer or third parties that a suspicion report or related information has been submitted or is being considered. Use controlled customer communications during holds, exits and information requests.	Access controls, confidentiality procedure, communication templates, audit log and training	Law 43-05, art. 29
Retain AML records for ten years	Keep customer and beneficial-owner identity records, transaction data, correspondence, analyses, reports, governance, training and control evidence for the applicable ten-year AML period, measured from the relationship end or transaction as required, and longer under a lawful hold.	Retention schedule, repository controls, sample retrieval, legal-hold process and deletion evidence	Law 43-05 recordkeeping provisions; BAM Circular 5/W/2017
Obtain CNDP processing and transfer clearance	Before implementing processing, submit the applicable CNDP prior declaration unless excluded, exempt or subject to prior authorisation. Obtain prior authorisation for sensitive data, change of purpose, offence or conviction data, use of the CIN number and interconnection of files having different purposes. Obtain the CNDP receipt or authorisation for the underlying processing before a foreign-transfer request. Before transferring or hosting data abroad, submit the required transfer filing and document the applicable route: an adequate destination, a specific Article 44 exception, an international agreement, or express reasoned CNDP authorisation supported by appropriate contractual or intra-group safeguards. Do not treat consent alone as a blanket solution for routine or systematic international KYC hosting.	Processing inventory, CNDP declaration, receipt or authorisation, CIN and sensitive-data assessment, transfer filing, legal route and safeguards	Law 09-08, arts. 12 and 43-44; CNDP Conditions and Notification Procedures
Apply purpose, proportionality and transparency	Give the required collection notice, specify legitimate purposes, collect only necessary and proportionate data, keep it accurate and current, define retention, support access, rectification and opposition rights and document any AML-law restriction on ordinary rights handling.	Privacy notices, lawful-purpose register, field minimisation, rights log, retention mapping and AML exception decision	Law 09-08; CNDP Conditions
Secure data and govern processors	Apply appropriate physical and logical security, confidentiality, access, audit and incident controls. Use contracts and audits to ensure processors and recipients comply with Law 09-08 and the approved purpose, security and transfer conditions.	Security assessment, access review, processor contract, audit, incident register and remediation	Law 09-08; CNDP Conditions

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain evidence-led regulatory assurance	For Bank Al-Maghrib-supervised institutions, operate the required permanent and periodic controls across onboarding, ownership, customer risk, PEPs, sanctions, remote verification, monitoring, wires, reporting, records, agents and outsourcing. Test CNDP status and privacy controls under the applicable governance framework. Report exceptions and remediation to the audit committee and verify closure; use independent assurance where separately required or adopted by the institution.	Control inventory, permanent and periodic test scripts, sampled files, metrics, audit-committee reporting and closure proof	BAM Circular 5/W/2017, arts. 9-11; Law 09-08

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.

Consolidated legislative and regulatory texts governing credit institutions, including Law 43-05 and Circular 5/W/2017

Bank Al-Maghrib · primary

[Open official source](#)
AML/CFT public guide, March 2025

Bank Al-Maghrib · primary

[Open official source](#)
Letter Circular No. 1/DSB/2020 on remote account opening

Bank Al-Maghrib · primary

[Open official source](#)
National Financial Intelligence Authority official page

Ministry of Economy and Finance · primary

[Open official source](#)
Beneficial Owners Register

OMPIC · primary

[Open official source](#)
Law No. 09-08 on personal-data processing

CNDP · primary

[Open official source](#)
Conditions for processing personal data

CNDP · primary

[Open official source](#)
Personal-data notification procedures

CNDP · primary

[Open official source](#)
Law No. 12-18 amending Law No. 43-05

CNASNU / Ministry of Justice · primary

[Open official source](#)
CNASNU reference texts

CNASNU · primary

[Open official source](#)
CNASNU Practical Implementation Guide

CNASNU · primary

[Open official source](#)
Joint warning against use of virtual currencies, 5 April 2022

Office des Changes · primary

[Open official source](#)
National Personal Data Protection Register

CNDP · primary

[Open official source](#)

Jurisdictions under Increased Monitoring, 19 June 2026

FATF · primary

[Open official source](#)**KYC Compliance in Morocco 2026**

VOVE ID · contextual

[Open contextual guide](#)**Navigating KYB in Morocco**

VOVE ID · contextual

[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 compliance information, not legal advice. Law No. 43-05 provides the national baseline, while the Bank Al-Maghrib material used here applies specifically to credit institutions and assimilated bodies, including payment institutions. Capital-markets, insurance, real-estate, legal, accounting and other covered sectors must add the current AMMC, ACAPS or other competent-supervisor rules. Confirm amendments, forms, thresholds, reporting channels and CNASNU decisions against current official Arabic or French texts before implementation.