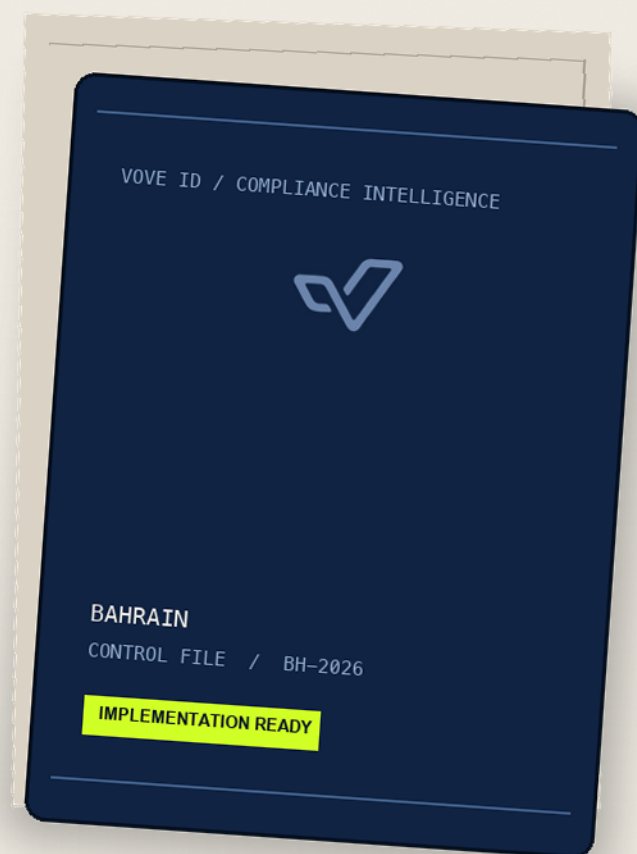


BAHRAIN



BAHRAIN / BH



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE



Bahrain KYC, KYB & AML Compliance Checklist

An implementation checklist for Bahrain customer due diligence, beneficial ownership, suspicious transaction reporting, sanctions, privacy, payments and crypto-asset controls.

Primary AML law	Legislative Decree No. 4 of 2001, as amended through 2025
FIU and reporting	National Financial Intelligence Centre; CBB licensees use the Online STR system under current rules
STR timing	Immediately upon suspicion, including attempted transactions, regardless of value
CBB occasional-transaction CDD	Above BHD 6,000, including linked transactions; wire transfers trigger CDD irrespective of amount in banking modules
AML retention	At least 5 years; the statutory start event depends on record class
Commercial-register UBO	10% ownership or voting control is one criterion; effective control and other influence tests also apply
Privacy	Law No. 30 of 2018 on Personal Data Protection and implementing decisions
FATF public lists	Not listed at 19 June 2026

Scope and legal framework

Legislative Decree No. 4 of 2001 on the Prohibition and Combating of Money Laundering and Terrorist Financing, as amended including by Legislative Decree No. 29 of 2020 and Legislative Decree No. 36 of 2025, establishes the national framework. CBB Rulebook Financial Crime modules and sector orders apply according to the regulated activity.

FATF context

Bahrain was absent from the FATF increased-monitoring and call-for-action lists dated 19 June 2026. Bahrain remains a MENAFATF member; its published 2022 third enhanced follow-up report records technical-compliance re-ratings and continued enhanced follow-up. Absence from a public list is not a low-risk classification.

IMPORTANT

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 30 September 2026. Confirm the regulated perimeter, current CBB volume and module, NFIC reporting specifications, sanctions designation, data-protection permissions and sector orders with the competent authority and qualified Bahrain counsel before launch.

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.

1. SCOPE, AUTHORITIES, AND LICENSING

Scope, authorities, and licensing

Classify the entity, activity and supervisory rulebook before assigning controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether each activity is an institution or otherwise subject to the AML law.	Map services, customers and Bahrain nexus to Legislative Decree No. 4 of 2001, current amendments, CBB licensing categories and the applicable DNFBP order.	Perimeter memo, service and funds-flow maps, legal analysis and authority confirmation.	Legislative Decree No. 4 of 2001, articles 1, 4 and 5; applicable competent-authority rules
Obtain each required CBB or sector licence before activity.	Classify banking, investment, insurance, payment, remittance, exchange, crypto-asset and other regulated services and secure approval before launch.	Licence matrix, applications, approvals, conditions register and renewal calendar.	CBB and Financial Institutions Law 2006; applicable CBB Rulebook volume
Apply the correct Financial Crime module and current version.	Identify the CBB volume for the licence category, track module amendments and document any sector-specific departures rather than copying controls across volumes.	Rulebook inventory, change log, compliance mapping and governance approval.	CBB Rulebook Financial Crime modules, current version

Governance and ML/TF/PF risk assessment

Governance must address money laundering, terrorist financing and proliferation-financing risk.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented enterprise risk assessment.	Assess customers, countries, products, delivery channels, transactions, technology, sanctions and emerging risks and update for material change and national findings.	Methodology, current assessment, data sources, approvals, residual-risk decisions and change log.	Legislative Decree No. 4 of 2001, articles 4-5; CBB FC risk-based approach requirements
Maintain proportionate AML/CFT/CPF policies and controls.	Document CDD, monitoring, reporting, recordkeeping, sanctions, employee screening, training, group controls, independent review and escalation.	Approved framework, control map, procedures, training and issue register.	Legislative Decree No. 4 of 2001, article 5; applicable CBB FC module
Appoint an approved and empowered MLRO.	Appoint a suitably senior Bahrain-resident MLRO and deputy where the rulebook requires; preserve independence, resources, unrestricted information access and direct board escalation.	CBB approval, appointment, fit-and-proper file, authority matrix and board reporting.	Applicable CBB FC module, MLRO chapter
Conduct independent compliance review and remediate findings.	Test design and operation at the required frequency using an independent and competent function; report results and verify closure.	Review plan, independence assessment, report, management response and closure testing.	Applicable CBB FC compliance-monitoring and audit requirements

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

CDD covers the customer, beneficial owner and each authorised representative.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply CDD before a relationship and when a statutory or rulebook trigger arises.	Identify and verify the customer before establishment, and refresh for material changes, doubts, suspicion, covered occasional transactions and transfers under the applicable module.	Trigger analysis, identity record, verification result, purpose and completion timestamp.	Legislative Decree No. 4 of 2001, articles 4-5; CBB FC-1
Apply the BHD 6,000 CBB occasional-trans action trigger in its proper scope.	For banking modules, apply CDD above BHD 6,000 and aggregate linked transactions; apply the exact current module for other licensees and do not treat the amount as a universal threshold report.	Aggregation logic, transaction samples, module mapping and CDD outcomes.	CBB FC-1.1.2 and corresponding current module provisions
Verify identity from reliable, independent evidence.	Obtain official identity attributes and validate authenticity, expiry, address where required and person-to-document linkage using risk-sensitive methods.	Identity attributes, source provenance, validation result, fraud checks and exceptions.	CBB FC-1 customer identification and verification requirements
Identify representatives and validate authority.	Identify and verify persons acting for the customer and confirm their legal mandate before accepting instructions.	Representative KYC, mandate, authority checks and instruction limits.	CBB FC-1; applicable sector order
Do not proceed when required CDD cannot be completed.	Decline or terminate as the applicable rule requires, restrict activity and consider an STR without tipping off.	CDD failure record, restriction or exit decision, STR assessment and communications review.	CBB FC-1 and suspicious-reporting provisions

4. KYB, REGISTRY, AND BENEFICIAL OWNERSHIP

KYB, registry, and beneficial ownership

Registry disclosure and AML beneficial-ownership analysis are related but distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify the legal person or arrangement and its powers.	Collect current legal name, form, commercial registration, address, governing documents, directors, partners or trustees and validate against SIJILAT or other reliable sources.	Registry extract, constitutional documents, officer list and discrepancy resolution.	CBB FC-1; Commercial Companies Law; MOIC registry guidance
Identify natural persons with ultimate ownership or effective control.	Trace layered, nominee and legal-arrangement structures to natural persons who ultimately own, control or benefit and to persons on whose behalf activity occurs.	Ownership chart, control analysis, declarations, source documents and verified identities.	CBB Rulebook definition of beneficial owner, amended June 2025
Identify trust and legal-arrangement parties.	Identify settlors, trustees, protectors, beneficiaries or classes and any other natural person exercising ultimate effective control; look through legal-person trustees.	Trust deed, party schedule, powers analysis, ownership look-through and verification.	CBB Rulebook beneficial-owner definition, June 2025
Apply the MOIC UBO disclosure criteria without reducing them to one percentage.	Treat direct or indirect ownership or voting control of at least 10% as one criterion and assess effective control, decision influence, financing, family or contractual relationships and management powers.	UBO analysis, calculation, control evidence, filing and update receipts.	Ministerial Order No. 83 of 2020, article 3
Keep commercial-register UBO information current.	File required UBO information at registration and update changes through the current MOIC/SIJILAT process; retain evidence of submissions and discrepancy resolution.	UBO register, SIJILAT filings, change log, notices and remediation.	Ministerial Order No. 83 of 2020; MOIC business-services guidance

PEPs, EDD, and remote onboarding

Enhanced measures attach to specified and higher-risk circumstances.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify PEPs, family members and close associates.	Screen customers and beneficial owners for domestic, foreign and international-organisation PEP exposure and apply senior approval, source-of-wealth, source-of-funds and enhanced monitoring controls.	Screening, relationship map, approval, source corroboration and review history.	Applicable CBB FC enhanced-CDD and PEP provisions
Apply enhanced due diligence to higher-risk relationships.	Obtain additional information on customer, ownership, purpose, source of wealth and funds; increase monitoring and document acceptance or continuation decisions.	Risk trigger, additional CDD, source evidence, approval and monitoring plan.	CBB FC-1 enhanced CDD; FATF high-risk-country measures
Control non-face-to-face and technology risk.	Validate document authenticity and liveness, detect impersonation, test vendors, preserve manual fallback and apply stronger measures when residual risk is elevated.	Method assessment, vendor diligence, testing, exceptions and fraud cases.	CBB FC non-face-to-face and new-technology provisions

Monitoring and suspicious transaction reporting

Ongoing scrutiny and immediate escalation support reporting to the NFIC.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Keep CDD current and monitor activity on a risk basis.	Examine transactions against purpose, profile, expected behaviour and risk; investigate significant, abnormal or unexplained activity and document source-of-funds work.	Monitoring scenarios, alerts, case decisions, refresh records and quality testing.	CBB FC-2 ongoing CDD and transaction monitoring
Escalate suspicion without waiting for proof or transaction completion.	Assess completed, attempted and proposed activity promptly and record the facts, grounds and timestamp at which suspicion was formed.	Alert chronology, information reviewed, suspicion decision and decision-maker.	Legislative Decree No. 4 of 2001, articles 4-5, as amended in 2020
Report suspicious transactions immediately, regardless of value.	The MLRO must submit complete reports through the current Online STR system to the NFIC and follow any parallel CBB notification required by the applicable module.	Suspicion timestamp, STR, system receipt, CBB notice and correction record.	Legislative Decree No. 4 of 2001, article 5(c); CBB FC external-reporting provisions
Prevent tipping off and protect STR information.	Restrict report knowledge, control customer and third-party communications and disclose only where legally permitted.	Access controls, disclosure register, legal review, training and incident log.	AML law and applicable CBB FC confidentiality provisions

Payments, wires, thresholds, and crypto-assets

Payment and crypto services require activity-specific CBB licensing and transfer controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Carry and validate required wire-transfer information.	Collect, transmit and retain prescribed originator and beneficiary information and establish risk-based procedures for missing, incomplete or suspect fields.	Field matrix, message samples, validation rules, repair queue and dispositions.	Applicable CBB FC wire-transfer provisions
Apply CDD to wire transfers under the applicable module.	For banking modules, apply CDD irrespective of amount; where a specialised-licensee simplified rule refers to transfers below US\$1,000, treat it only as a conditional simplification and never where suspicion or higher risk exists.	Module mapping, transfer samples, risk decisions and CDD result.	CBB FC-1 and FC-3, applicable Rulebook volume
Obtain payment-service approval before launch.	Classify domestic and cross-border transfer, merchant acquisition, e-money, payment initiation, account information, money changing and crypto-based payment services under the February 2026 PSP Module.	Product memo, CBB licence, conditions, safeguarding records and tests.	CBB Rulebook Volume 5, PSP Module, February 2026
Obtain the correct crypto-asset service licence.	Map exchange, brokerage, custody, portfolio, advisory and crypto-based payment features to the CBB CRA and PSP modules; meet category, governance, custody, cybersecurity, market-conduct and AML controls.	Service and wallet-flow map, CBB licence, category analysis, custody design and monitoring tests.	CBB Rulebook Volume 6, CRA Module; Volume 5 PSP Module

8. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Sanctions controls operate independently of an STR decision.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen UN and Bahrain designations and ownership or control.	Screen customers, beneficial owners, controllers, representatives and transactions at onboarding and upon list updates; test aliases and controlled entities rather than exact names only.	List versions, update logs, configuration tests, match analysis and dispositions.	Applicable Bahrain targeted-financial-sanctions framework and CBB FC requirements
Freeze or restrain without delay when a true designation match exists.	Stop dealings, prevent direct or indirect availability of assets and notify through the current competent route without waiting for an STR decision or customer notice.	Match analysis, restriction timestamp, notification, authority correspondence and release approval.	Applicable UN implementation orders; CBB FC sanctions provisions
Use licences, exemptions or releases only under written authority.	Identify the governing regime, obtain permission before activity, implement conditions and document expiry and release decisions.	Regime analysis, licence or permission, controls, reporting and release record.	Applicable designation and competent-authority procedure

Records and regulator access

Five years is the baseline, with distinct start events by record class.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain customer and relationship records for at least five years.	Keep identity and business-relationship records for at least five years after the relationship ceases, subject to longer legal holds or authority directions.	Retention schedule, relationship-end date, archive sample, retrieval test and deletion approval.	Legislative Decree No. 4 of 2001, article 5(a); CBB FC recordkeeping
Retain transaction and attempted-transaction records for at least five years.	Keep records sufficient to reconstruct each transaction or attempt for at least five years after completion or attempt.	Transaction sample, trigger calculation, legal hold and deletion log.	Legislative Decree No. 4 of 2001, article 5(b); CBB FC-7 or corresponding chapter
Preserve STR, monitoring, training and compliance evidence.	Keep internal and external reports, dispositions, annual review and training records for the required period and make them promptly accessible to authorised authorities.	Record-class matrix, access controls, retrieval tests and production log.	Applicable CBB FC recordkeeping requirements

Privacy, biometrics, breaches, and transfers

AML processing must also comply with Bahrain's personal-data framework.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Process personal data on a lawful basis and transparently.	Map each KYC data element to a lawful basis and specific purpose, provide required notices, minimise collection, maintain accuracy and support data-subject rights.	Data inventory, lawful-basis map, notices, request log and accuracy controls.	Law No. 30 of 2018 on Personal Data Protection
Apply special controls to sensitive and biometric data.	Classify biometric and other sensitive data, identify the applicable statutory condition or permission, document necessity and proportionality and apply heightened access and deletion controls.	Classification, legal assessment, privacy impact assessment, permissions and deletion tests.	Law No. 30 of 2018 and implementing decisions
Manage processors and personal-data breaches.	Contract for instructions, confidentiality, security, incident escalation, return and deletion; investigate and notify the Authority or affected people where current law and decisions require.	Processor contract, security review, incident chronology, notifications and remediation.	Law No. 30 of 2018; Personal Data Protection Authority executive decisions
Control transfers outside Bahrain.	Determine whether the destination is adequate or another statutory route, authority permission or safeguard is required before transfer or remote access.	Transfer map, adequacy analysis, permission or safeguard, contract and monitoring.	Law No. 30 of 2018, articles 12-13; Order No. 42 of 2022

Practical evidence packs

Evidence should reconstruct onboarding, reporting and launch decisions end to end.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a reconstructable onboarding pack.	Bundle identity, authority, KYB, beneficial ownership, PEP, sanctions, purpose, risk, privacy, approvals and exceptions under stable identifiers.	Complete sampled onboarding pack and retrieval result.	Operational control supporting AML law and CBB FC-1
Maintain a reconstructable NFIC and sanctions case pack.	Link activity, alert, suspicion chronology, STR, receipt, CBB notice, confidentiality, asset restrictions and authority communications.	Complete sampled case pack, timeline and controlled-access record.	Operational control supporting AML law articles 4-5 and CBB FC reporting rules
Maintain a launch and change pack.	Record perimeter, licences, approved programme, reporting connectivity, sanctions, privacy, vendors, tests and controlled uncertainties before launch or material change.	Signed launch pack, source register, tests, approvals and uncertainty log.	Official sources listed below

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.

Legislative Decree No. 4 of 2001 - AML/CFT framework

Legislation and Legal Opinion Commission · Primary legislation

[Open official source](#)

Legislative Decree No. 29 of 2020 - AML/CFT amendments

Legislation and Legal Opinion Commission · Primary amending legislation

[Open official source](#)

Legislative Decree No. 36 of 2025 - AML/CFT amendments

Legislation and Legal Opinion Commission · Primary amending legislation

[Open official source](#)

CBB Rulebook Volume 1 Financial Crime module

Central Bank of Bahrain · Official supervisor rules

[Open official source](#)

CBB Rulebook Volume 5 Financial Crime module

Central Bank of Bahrain · Official supervisor rules

[Open official source](#)

CBB Online STR system and authority contacts

Central Bank of Bahrain · Official reporting rules

[Open official source](#)

CBB recordkeeping requirements

Central Bank of Bahrain · Official supervisor rules

[Open official source](#)

CBB beneficial-owner definition

Central Bank of Bahrain · Official supervisor rules

[Open official source](#)

CBB Rulebook Volume 6 Crypto-asset module

Central Bank of Bahrain · Official licensing rules

[Open official source](#)

CBB Rulebook Volume 5 Payment Service Provider module, February 2026

Central Bank of Bahrain · Official licensing rules

[Open official source](#)

National Financial Intelligence Centre

Ministry of Interior · Official FIU information

[Open official source](#)

NFIC suspicious-activity indicators

National Financial Intelligence Centre · Official FIU guidance

[Open official source](#)

Ministerial Order No. 83 of 2020 on UBO disclosure

Ministry of Industry and Commerce · Primary registry order

[Open official source](#)

Business services and Ultimate Beneficial Owner

Ministry of Industry and Commerce · Official registry guidance

[Open official source](#)

Law No. 30 of 2018 on Personal Data Protection

Personal Data Protection Authority · Primary legislation

[Open official source](#)

Personal-data executive decisions and breach/transfer requirements

Personal Data Protection Authority · Official privacy guidance

[Open official source](#)

MENAFATF third enhanced follow-up report for Bahrain

MENAFATF · Authoritative assessment

[Open official source](#)

FATF jurisdictions under increased monitoring - 19 June 2026

FATF · Authoritative current status

[Open official source](#)

FATF high-risk jurisdictions subject to a call for action - 19 June 2026

FATF · Authoritative current status

[Open official source](#)

Document control

Version 1.0 / Published 30 September 2026 / Last reviewed 30 September 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 30 September 2026. Confirm the regulated perimeter, current CBB volume and module, NFIC reporting specifications, sanctions designation, data-protection permissions and sector orders with the competent authority and qualified Bahrain counsel before launch.