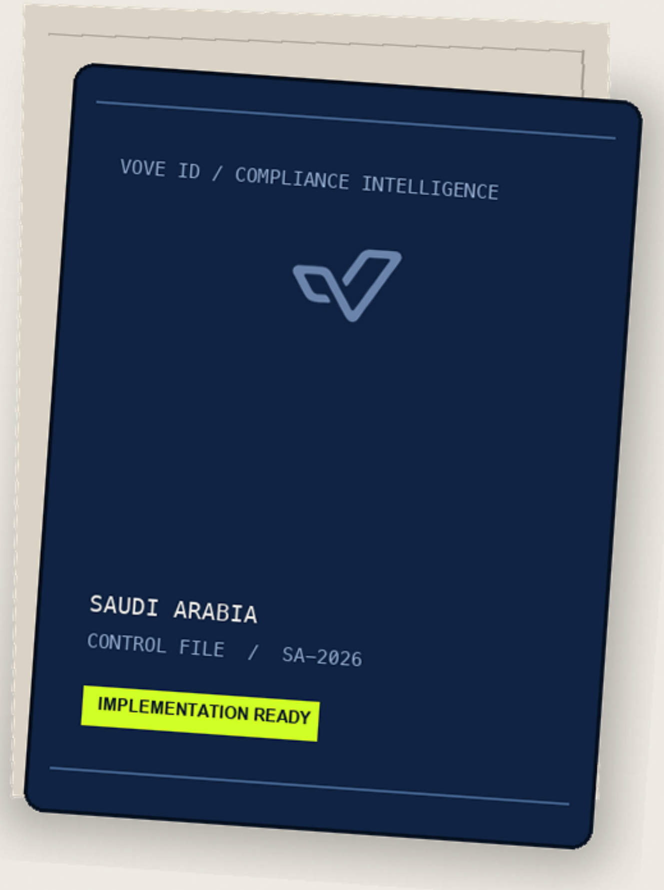
VOVE ID

VOVE COUNTRY CONTROL FILE
KYC / KYB / AML
2026 EDITION

SAUDI ARABIA

SAUDI ARABIA / SA



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Saudi Arabia KYC, KYB & AML Compliance Checklist

An implementation checklist for customer identity, corporate ownership, suspicious reporting, sanctions, payments and personal-data protection under Saudi Arabia's national and sector frameworks.

FIU	**Saudi Arabia Financial Intelligence Unit (SAFIU), under the Presidency of State Security**
Primary AML rule	**Anti-Money Laundering Law, Royal Decree M/20 dated 5/2/1439H, and Implementing Regulation**
Suspicion reporting	**Promptly and directly, including attempted transactions and regardless of amount**
Universal threshold	**No single universal CDD or transaction-reporting threshold is stated in the core AML Law**
AML retention	**At least 10 years; specified authorities may require longer retention**
Company BO test	**Resolution 99 applies 25% ownership, then control, then management fallback sequentially**
Privacy authority	**Saudi Data & AI Authority (SDAIA)**
FATF public lists	**Not listed at 19 June 2026**

Scope and legal framework

The Anti-Money Laundering Law issued by Royal Decree M/20 of 1439H and its Implementing Regulation are the core AML framework. The Law on Combating Terrorism Crimes and Financing, current supervisory rules, the 2025 Targeted Financial Sanctions Rules, Ministerial Resolution 99 of 1447H on beneficial ownership, and the Personal Data Protection Law and regulations apply according to entity, activity and data use.

FATF context

Saudi Arabia was not named on the FATF call-for-action or increased-monitoring lists dated 19 June 2026. Saudi Arabia is a FATF and MENAFATF member. Absence from a FATF public list is not a low-risk classification.

IMPORTANT	General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 16 September 2026. Confirm the controlling Arabic text, later amendments, sector circulars, SAFIU filing mechanics, sanctions-list procedures, Ministry of Commerce filing workflow and product-specific SAMA or CMA requirements with the competent authority and qualified Saudi 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.

Minimum review record

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

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

Scope, authorities, and licensing

Identify the reporting perimeter and every competent supervisor before onboarding or launch.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Classify each entity and activity under the national AML perimeter.	Determine whether the entity is a financial institution, designated non-financial business or profession, or nonprofit organisation and map its AML, CFT and CPF supervisor.	Entity map, activity analysis, licence inventory, supervisor confirmation and legal opinion.	Anti-Money Laundering Law, Articles 1, 24 and 25; Implementing Regulation, Article 1
Obtain required financial and payment permissions before operating.	Classify banking, finance, insurance, securities, payment, electronic-money and technical-support activity and secure the applicable SAMA, CMA or other licence, registration or non-objection.	Perimeter memorandum, application, licence, conditions, regulator correspondence and renewal calendar.	Law of Payments and Payment Services, Royal Decree M/26; Implementing Regulations, Articles 4-7
Do not treat a technical role as exempt without analysis.	Where the service supports e-commerce payments, document whether it is limited to linkage and technical support or enters regulated payment execution, custody, settlement or customer-funds activity.	Service diagram, funds-flow map, contracts, technical permit and regulatory analysis.	SAMA Rules for Dealing with E-Commerce Payment Service and Support Providers, Circular 46004436

Governance and risk assessment

Controls must be risk-based, senior-approved, independently tested and responsive to new risks.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented and current ML risk assessment.	Assess customer, country, product, service, transaction, delivery-channel and technology risks and provide the assessment to the supervisor on request.	Methodology, assessment, source inputs, approvals, residual-risk decisions and remediation plan.	Anti-Money Laundering Law, Article 5
Assess new products, practices and technologies before use.	Complete and approve a documented assessment before launching remote onboarding, biometrics, automation, new channels or materially changed products.	Pre-launch assessment, model or vendor validation, controls, approval and monitoring plan.	Anti-Money Laundering Law, Article 5; SAMA Circular 472039915
Maintain senior-approved AML policies and accountable management.	Cover CDD, reporting, sanctions, records, employee screening, training, group controls and an appropriately senior compliance officer.	Policy suite, board or senior approval, appointment, authority matrix and reporting packs.	Anti-Money Laundering Law, Article 14; Implementing Regulation, Articles 14/1-14/3
Independently test programme effectiveness.	Operate risk-based monitoring, ongoing training and an independent audit function; track findings to verified closure.	Training records, audit plan, samples, findings, owners and closure evidence.	Implementing Regulation, Article 14/1

Natural-person identification

Identify and verify customers, beneficial owners and representatives using reliable independent material.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply CDD at all core statutory triggers.	Perform CDD before a relationship, an occasional transaction, an occasional wire, whenever suspicion exists regardless of amount, and when prior identity information is doubtful; apply any supervisor-set threshold in addition.	Trigger matrix, aggregation logic, timestamps, customer file and exception log.	Implementing Regulation, Article 7/1
Verify the customer from authentic independent evidence.	Obtain and verify identity information proportionate to the customer and risk and prohibit anonymous, obviously fictitious-name or numbered accounts.	Identity copy, independent verification results, authenticity checks and discrepancy log.	Anti-Money Laundering Law, Articles 6-7; Implementing Regulation, Articles 7/2-7/3
Verify representatives and their authority.	Identify and verify anyone acting for the customer and establish the authenticity and scope of the authority before permitting instructions or access.	Representative KYC, power or mandate, verification result, limits and activity log.	Implementing Regulation, Article 7/2
Do not proceed when CDD cannot be completed.	Do not open the account, establish the relationship or execute the transaction; terminate an existing relationship as required and consider an STR. If CDD would tip off the customer, stop that step and report the reason.	Restriction, exit decision, suspicion assessment, approval and filing receipt.	Implementing Regulation, Articles 7/8-7/9

KYB, registries, and beneficial ownership

Verify legal existence, authority, ownership and actual control; keep AML verification and company filing duties distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal-person identity, purpose and authority.	Obtain current constitutional and commercial-register information, principal address, business purpose, directors or managers and binding authority from reliable independent sources.	Commercial-register extract, constitutional pack, licence, officer list, mandates and discrepancy log.	Implementing Regulation, Article 7/2
Identify and verify each AML beneficial owner.	Trace the natural person who ultimately owns or controls the customer and take reasonable measures to verify identity; for legal arrangements identify the relevant controlling natural persons.	Layered ownership chart, control analysis, source documents, verified identities and rationale.	Implementing Regulation, Article 7/3; SAMA AML/CTF Guide, section 3.17
Apply the current company-register beneficial-owner cascade.	Where Resolution 99 applies, identify natural persons owning directly or indirectly at least 25%; only if none, identify control by other means; only if still none, apply the manager, board-member or chairperson fallback.	Percentage calculations, control analysis, sequential fallback rationale and filing record.	Ministerial Resolution 99 dated 5/6/1447H; Ministry of Commerce announcement, 8 December 2025
Maintain and confirm the company beneficial-owner record.	Keep the prescribed identity, contact, qualification and nature-and-extent information accurate; disclose and annually confirm it through the current Ministry process and preserve the internal register.	BO register, reasonable-measures file, submission, annual confirmation and change log.	Ministerial Resolution 99 dated 5/6/1447H

PEPs, EDD, and reliance

Detect prominent public functions and strengthen controls where risk requires.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify customers and beneficial owners with prominent public functions.	Use risk systems, declarations and reliable sources to identify domestic or foreign prominent public functions and senior international-organisation roles, including relationships covered by the regulation.	Declaration, screening result, relationship map, rationale and refresh history.	Anti-Money Laundering Law, Article 8; Implementing Regulation, Article 8
Apply enhanced measures proportionate to higher risk.	Obtain required senior approval, establish source of wealth and source of funds where applicable, and increase ongoing monitoring for higher-risk customers and relationships.	Risk assessment, approval, source corroboration, monitoring plan and review record.	Anti-Money Laundering Law, Articles 7-8; Implementing Regulation, Articles 7/14 and 8
Retain responsibility when relying on a third party.	Obtain required CDD information immediately, ensure underlying documents are available without delay, confirm the relied party is regulated and supervised, assess country risk and keep ultimate responsibility.	Reliance assessment, agreement, information receipt, document test, supervision check and review.	Implementing Regulation, Articles 7/10-7/13

Monitoring and suspicious reporting

Suspicious funds and attempts are reported promptly and directly, regardless of amount.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor relationships and keep CDD current.	Scrutinise transactions against customer information, business activity, risk and source of funds where necessary; refresh higher-risk records more frequently.	Monitoring scenarios, alerts, investigations, refresh schedule and dispositions.	Anti-Money Laundering Law, Article 13; Implementing Regulation, Articles 7/6-7/7
Examine complex, unusually large or purposeless patterns.	Document the background and purpose of transactions or patterns with no clear economic or legal objective and escalate unresolved suspicion.	Alert, customer explanation, corroboration, analysis and disposition.	Anti-Money Laundering Law, Article 13
Report suspicion and attempted transactions promptly and directly.	When suspicion or reasonable grounds concern funds, proceeds or money laundering, regardless of amount, send SAFIU a detailed report with available information and respond promptly to follow-up requests.	Suspicion chronology, report, submission receipt, acknowledgement and supplemental responses.	Anti-Money Laundering Law, Articles 15 and 18
Prevent tipping off and preserve report confidentiality.	Restrict access and do not disclose that a report will be, is being or has been filed or that a criminal investigation is underway, except where lawfully permitted.	Need-to-know matrix, access logs, communication controls, training and incident review.	Anti-Money Laundering Law, Article 16

Payments, wires, thresholds, and agents

Payment permissions, wire data and agent oversight are product- and supervisor-specific.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Carry required originator and beneficiary information through the payment chain.	Obtain and retain prescribed originator and beneficiary data and do not execute a wire when required information cannot be obtained.	Field matrix, validation logic, sampled transfers, repair queue and rejection record.	Anti-Money Laundering Law, Article 10; Implementing Regulation, Article 10
Use the correct payment or electronic-money permission.	Map the product to regulated payment services and secure the SAMA licence, registration or other approval before offering, marketing or arranging it in the Kingdom.	Product classification, licence, conditions, terms, launch approval and renewal calendar.	Payments and Payment Services Implementing Regulations, Articles 4-7
Obtain SAMA non-objection before appointing payment agents.	Submit the prescribed business plan and agent information, verify required permissions and maintain annual performance and incident reporting.	Non-objection, due diligence, contract, agent register, annual report and monitoring.	Payments and Payment Services Implementing Regulations, Article 24
Obtain SAMA non-objection before material outsourcing.	Assess materiality, risks, audit and access rights, continuity and exit; obtain non-objection before contracting a material payment function.	Outsourcing assessment, regulator non-objection, contract, oversight and exit test.	Payments and Payment Services Implementing Regulations, Article 27

Targeted financial sanctions

Use the current national, UN and supervisory framework; procedures differ by supervised sector.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen relevant parties against current sanctions designations.	Screen customers, beneficial owners, controllers, representatives and transactions at onboarding, during the relationship and when applicable lists change.	List inventory, update logs, screening configuration, tests and dispositions.	SAMA Targeted Financial Sanctions Rules, Circular 472035766 dated 7 December 2025
Freeze covered property without delay when a confirmed designation applies.	Block covered funds or assets, prevent funds or services being made available and follow the current competent-authority reporting and release procedure without prior notice to the designated person.	Match analysis, freeze timestamp, ownership-control analysis, asset inventory, report and system blocks.	SAMA Targeted Financial Sanctions Rules, Circular 472035766; Law on Combating Terrorism Crimes and Financing
Scope proliferation-sanctions procedures to the relevant sector.	Apply SAMA's in-force rules to supervised financial institutions and the Ministry of Commerce guide to dealers in precious metals and stones; do not generalise a sector filing route without authority.	Sector analysis, applicable rule version, procedure map, training and test case.	SAMA Circular 472035766; Ministry of Commerce Guide for Dealers in Precious Metals and Stones, April 2026

9. RECORDS AND AUTHORITY ACCESS

Records and authority access

Records must reconstruct transactions and remain available for at least ten years.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain transaction and relationship records for at least ten years.	Keep domestic, international, commercial and monetary transaction records from transaction completion or account closure and CDD, account, correspondence and analysis material from the relevant statutory trigger.	Retention schedule, trigger calculations, archive sample, legal holds and deletion controls.	Anti-Money Laundering Law, Article 12
Extend retention when lawfully required.	Apply Public Prosecution extensions for criminal investigation or prosecution and preserve relevant material under controlled legal hold.	Authority request, validation, hold notice, affected records and release approval.	Anti-Money Laundering Law, Article 12(3)
Reconstruct and promptly produce records.	Organise records to reconstruct individual transactions, authenticate official requests and make responsive material readily available while protecting STR confidentiality.	Request register, authority validation, production index, delivery log and receipt.	Anti-Money Laundering Law, Articles 12(4), 18 and 25

Privacy, biometrics, and transfers

Identity and monitoring data must follow the PDPL, its Implementing Regulation and Transfer Regulation.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map scope, purpose and lawful basis for each processing activity.	Document the controller or processor role, purpose, statutory or consent basis, notice, source and recipient for identity, screening, monitoring and biometric data.	Data inventory, role and lawful-basis analysis, notices, consent records and exception register.	Personal Data Protection Law, Articles 2, 5-6 and 10-15
Minimise and secure personal and sensitive data.	Collect only necessary data, apply purpose limitation, accuracy, access, security and destruction controls, and give sensitive and biometric data heightened safeguards.	Field justification, security design, access reviews, retention configuration and tests.	PDPL; Implementing Regulation, Articles 8, 19 and 23
Govern processors and breaches.	Select processors providing sufficient guarantees, include required contract terms, control subprocessors and operate the applicable authority and data-subject breach-notification process.	Due diligence, contract, subprocessor register, incident assessment, notices and chronology.	PDPL Implementing Regulation, Articles 17 and 24
Use a lawful route for transfers outside the Kingdom.	Assess national and vital interests, necessity and minimisation; use adequacy, an approved appropriate safeguard or a permitted exception and complete a transfer risk assessment when required.	Transfer map, legal route, safeguard, risk assessment, approvals and monitoring.	PDPL, Article 29; Regulation on Personal Data Transfer Outside the Kingdom, Articles 2-8

Practical evidence packs

Evidence should reproduce onboarding, monitoring and launch decisions end to end.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a reconstructable onboarding pack.	Bundle identity, authority, KYB, beneficial ownership, PEP and sanctions screening, risk, approvals, privacy records and exceptions under stable identifiers.	Complete sampled onboarding pack and retrieval result.	Operational control supporting Anti-Money Laundering Law, Articles 7-8 and 12
Maintain a reconstructable reporting and sanctions pack.	Link transactions, alerts, analysis, timing, report, acknowledgement, supplements, freeze actions, authority communications and access logs.	Complete sampled case pack and controlled access log.	Operational control supporting Anti-Money Laundering Law, Articles 15-18 and applicable TFS rules
Maintain a regulator-scoped launch pack.	Record activity classification, licences, current legal sources, filing readiness, ownership duties, sanctions procedure, privacy analysis, vendor controls and validation before launch and material change.	Signed launch pack, source register, regulator map, uncertainty log, tests and approvals.	Official sources listed below

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.

Anti-Money Laundering Law and Implementing Regulation
Saudi Central Bank Rulebook · Primary legislation and official regulation
Open official source

Law on Combating Terrorism Crimes and Financing and Implementing Regulations
Saudi Central Bank Rulebook · Primary legislation and official regulation
Open official source

AML/CTF Guide for SAMA-supervised financial institutions
Saudi Central Bank Rulebook · Official supervisory guidance
Open official source

Guidance on assessing ML, TF and PF business risks
Saudi Central Bank Rulebook · Official in-force circular
Open official source

Targeted Financial Sanctions Rules, Circular 472035766
Saudi Central Bank Rulebook · Official in-force rules
Open official source

Targeted-financial-sanctions guide for dealers in precious metals and stones
Ministry of Commerce · Official sector guidance
Open official source

Beneficial Ownership Rules approved by Resolution 99
Ministry of Commerce · Official binding rules
Open official source

Ministry announcement of Resolution 99 and sequential BO criteria
Ministry of Commerce · Official explanatory announcement
Open official source

Ministry guidance on BO confirmation and register access
Ministry of Commerce · Official explanatory announcement
Open official source

Implementing Regulations of Payments and Payment Services Law
Saudi Central Bank Rulebook · Official in-force regulation
Open official source

Rules for e-commerce payment service and support providers
Saudi Central Bank Rulebook · Official in-force rules
Open official source

Personal Data Protection Law
Saudi Data & AI Authority · Primary legislation
Open official source

PDPL Implementing Regulation and Transfer Regulation
Saudi Data & AI Authority · Official regulations
Open official source

Saudi Arabia mutual evaluation
FATF · 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

United Nations Security Council consolidated sanctions list
United Nations · Authoritative sanctions list
Open official source

Document control

Version 1.0 / Published 16 September 2026 / Last reviewed 16 September 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 16 September 2026. Confirm the controlling Arabic text, later amendments, sector circulars, SAFIU filing mechanics, sanctions-list procedures, Ministry of Commerce filing workflow and product-specific SAMA or CMA requirements with the competent authority and qualified Saudi counsel before launch.