VOVE ID

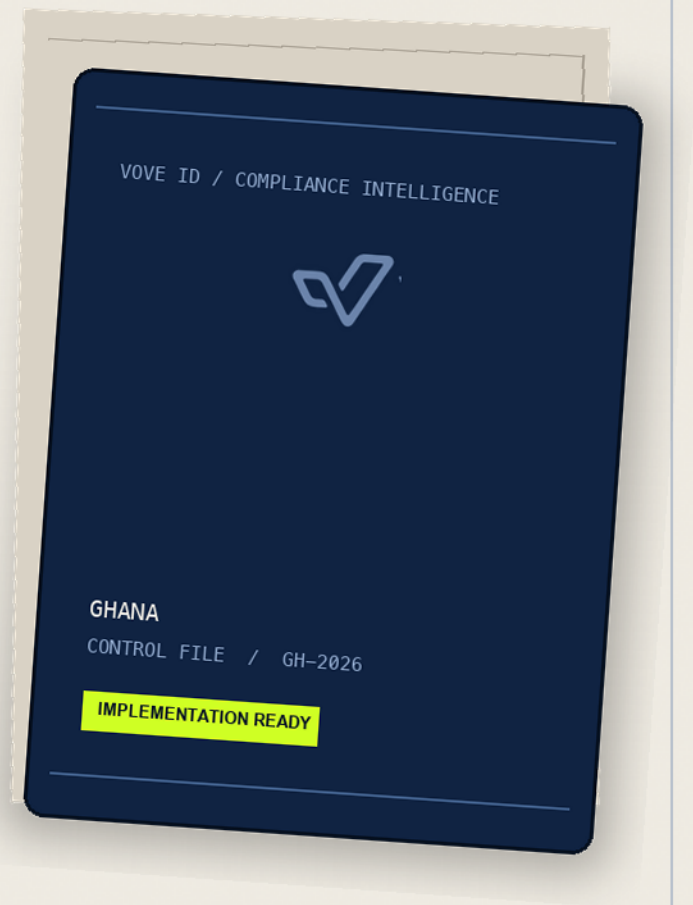
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

GHANA

GHANA / GH



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Ghana KYC, KYB & AML Compliance Checklist

A practical implementation checklist for accountable institutions operating in Ghana, with a focused overlay for Bank of Ghana-licensed institutions. It translates customer due diligence, beneficial ownership, Ghana Card, suspicious transaction reporting, sanctions, monitoring, records and data-protection duties into operational controls and reviewable evidence.

FINANCIAL INTELLIGENCE UNIT	**Financial Intelligence Centre (FIC Ghana)**
BoG AML BENEFICIAL OWNER TEST	**5% or more controlling interest, plus ultimate ownership or control**
STR DEADLINE	**Within 24 hours after suspicion or reasonable grounds arise**
RECORD RETENTION	**At least 5 years**
PRIMARY CITIZEN ID	**Ghana Card for Ghanaian citizens**
FATF PUBLIC LIST	**Not listed as of 19 June 2026**

Scope and legal framework

Anti-Money Laundering Act, 2020 (Act 1044); Anti-Money Laundering Regulations, 2011 (L.I. 1987), to the extent currently applicable; Anti-Terrorism Act, 2008 (Act 762), as amended, and Anti-Terrorism Regulations, 2012 (L.I. 2181); Bank of Ghana and Financial Intelligence Centre AML/CFT/CPF Guideline (September 2025); Companies Act, 2019 (Act 992) and Companies Regulations, 2023 (L.I. 2473); Data Protection Act, 2012 (Act 843).

FATF context

Ghana 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 the institution's documented customer, ownership, product, channel and geographic risk assessment.

IMPORTANT

This checklist is general compliance information, not legal advice. Act 1044 applies across accountable institutions, while the September 2025 BoG/FIC Guideline is the principal overlay used here for Bank of Ghana-licensed institutions. Securities, insurance, pensions, DNFBP and other regulated businesses must add their own supervisor's current rules. Confirm commencement, amendments, forms, thresholds and filing channels with the relevant Ghanaian authority 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.

01. SCOPE, ACCOUNTABILITY AND PROGRAMME GOVERNANCE

Scope, accountability and programme governance

Confirm the regulated perimeter, assign accountable governance and build a documented, independently tested AML/CFT/CPF programme.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map every regulated activity and supervisor	Document which group entities and services are accountable institutions under Act 1044. For every BoG licence, map the September 2025 BoG/FIC Guideline; add SEC, NIC, NPRA, Gaming Commission, professional-body or DNFBP rules where relevant.	Entity-perimeter register, licence inventory, legal applicability memo and named rule owner.	[1], [2], [3]
Make the board ultimately accountable	Have the board or highest governing authority approve the AML/CFT/CPF compliance programme, AML manual, risk framework and AMLRO appointment. Schedule at least quarterly review of the control environment and at least four AMLRO reports each year for BoG-licensed institutions.	Board charter, signed approvals, quarterly minutes, action log and AMLRO reports.	[2]
Appoint an empowered AMLRO	Obtain BoG approval for the AMLRO's appointment. Appoint the AMLRO at key managerial and at least senior-management grade, include the officer in the highest management decision-making body, preserve operational independence and provide direct reporting to the board or a board committee.	BoG approval, appointment letter, seniority and management-body record, reporting line, mandate and resourcing	BoG/FIC AML/CFT/CPF Guideline, sections 1.0 and 2.3.4
Maintain a board-approved AML manual	Translate Act 1044 and applicable supervisory rules into customer acceptance, CDD, EDD, PEP, sanctions, transaction-monitoring, reporting, records, training, audit and escalation procedures. For BoG-licensed institutions, submit the board-approved policy and manual to BoG within five working days.	Current manual, approval record, BoG submission receipt, change log and staff attestations.	[1], [2]
Train governance and staff on a documented cycle	For BoG-licensed institutions, train employees at least twice yearly and the board at least annually, with role-specific coverage for onboarding, operations, monitoring, investigations and reporting.	Annual plan, materials, attendance, assessment results, remedial training and board minutes.	[2]
Independently test the programme	Subject the AML/CFT/CPF programme to independent testing by appropriately experienced internal or external auditors. Submit the independent testing or review report to BoG and FIC no later than 15 January of each financial year. Promptly remediate identified weaknesses and update both authorities. Separately audit the transaction-monitoring system annually.	Auditor competence, independent-testing report, BoG and FIC submission receipts, remediation and annual monitoring-system audit	BoG/FIC AML/CFT/CPF Guideline, sections 2.3.6 and 2.8.6.1

02. CUSTOMER IDENTIFICATION AND GHANA CARD CONTROLS

Customer identification and Ghana Card controls

Identify natural-person customers using the prescribed credential and apply controlled remote-onboarding and failed-CDD outcomes.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify before providing unrestricted service	Identify the customer and verify identity using reliable, independent information before or during establishment of the relationship or occasional transaction. Permit deferred verification only within the narrow risk-based conditions allowed by the applicable rule, with limits, one-off use and documented rationale.	CDD standard, identity record, verification response, exception approval, transaction limits and completion log.	[1], [2]
Use the prescribed identity credential	Use the Ghana Card as the sole identity credential for Ghanaian citizens in BoG-regulated financial transactions. Apply the current non-citizen, refugee or asylum-seeker and diplomatic identification routes to eligible non-Ghanaian customers.	ID matrix, Ghana Card verification result, exception category evidence and staff guidance.	[2], [4]
Secure non-face-to-face onboarding	For remote onboarding under the BoG guideline, perform biometric liveness and match the customer against the Ghana Card record. Add device, behavioural, contact, fraud and multi-factor controls proportionate to risk.	Liveness result, biometric match, device and fraud signals, MFA log, exception queue and quality review.	[2]
Control financial-inclusion exceptions	Where an approved tiered or simplified route permits limited access before full documentation, impose the authorised limits and obtain a valid Ghana Card within 90 days. Suspend progression or access when the condition is not met.	Product approval, tier rules, expiry alerts, restriction logic and exception report.	[2]
Understand purpose and expected activity	Record the relationship purpose, occupation or business, source of funds where relevant, expected volumes, counterparties, channels and geographies so monitoring can test actual behaviour against a documented baseline.	Customer profile, expected-activity fields, source records, risk rationale and review triggers.	[1], [2]
Stop when CDD cannot be completed	If the institution cannot perform the CDD required by the BoG/FIC Guideline, do not open the account, commence the business relationship or perform the transaction. Submit an SAR or STR to FIC within 24 hours. For an existing relationship, restrict or discontinue activity in accordance with the approved closure procedure and maintain non-tipping-off controls.	Rejected or restricted case, closure decision, SAR or STR, filing receipt and non-tipping-off controls	BoG/FIC AML/CFT/CPF Guideline, section 2.4.6

03. KYB, OWNERSHIP AND CONTROL

KYB, ownership and control

Verify the legal person, trace natural-person ownership and control, and keep AML analysis distinct from ORC filing thresholds.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify the legal person and its authority chain	Obtain and independently verify incorporation, legal form, registered office, principal business, tax and licence information, directors, authorised signatories and the authority of each person acting for the entity. Use the Office of the Registrar of Companies entity-information service where available.	ORC extract, constitutional documents, tax and licence records, board authority, signatory verification and discrepancy log.	[1], [2], [5], [6]
Identify natural-person beneficial owners	For BoG-licensed institutions, identify and verify each natural person with 5% or more controlling interest and any natural person who ultimately owns, controls, directs or economically benefits from the customer. If ownership does not reveal the controller, follow the control and senior-managing-official cascade required by the applicable rule.	Ownership chart to natural persons, percentages, control rationale, identity verification and senior-official fallback record.	[2]
Separate ORC filing thresholds from AML CDD	Use the current ORC beneficial-ownership form and filing category for company-law submissions, while independently applying the AML test. The current BO1 form shows 5% for high-risk sectors and non-Ghanaian PEPs, any amount for Ghanaian PEPs, and 20% in other cases, plus control tests. ORC public materials are not fully consistent, so confirm the filing category directly with ORC.	Threshold decision note, current BO1 form, ORC confirmation where needed, filed return and separate AML ownership analysis.	[7], [8]
Keep registry ownership current	File beneficial-ownership changes within the applicable ORC deadline, currently described by ORC as 30 days, and include current ownership information in annual returns. Reconcile the registry record to the institution's CDD file.	Change alerts, filed forms, annual-return receipt, reconciliation and resolved discrepancies.	[8]
Reject bearer-share opacity	Apply the ORC public directive that no bearer shares may be issued and treat bearer-share structures, nominees or unexplained control layers as heightened-risk indicators requiring clarification and escalation.	Constitutional-document check, customer attestation, ownership evidence, escalation and remediation record.	[9]
Verify licences and merchant legitimacy	Confirm that the entity holds every required BoG or other sector licence and that its website, settlement account, directors, locations and stated activity align. Do not confuse a licensing ownership criterion, including a foreign-shareholder attestation threshold, with the AML beneficial-owner test.	Regulator check, licence copy, operating-footprint review, website and account match, and discrepancy decision.	[10]

04. RISK ASSESSMENT, PEPS AND TARGETED FINANCIAL SANCTIONS

Risk assessment, PEPs and targeted financial sanctions

Assess institutional and customer risk, control PEP relationships and implement binding targeted-financial-sanctions duties.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain an institution-wide risk assessment	Assess and document customer, country and geography, product, service, transaction and delivery-channel risks. For BoG-licensed institutions, obtain board or senior-management approval, review at least within a two-year cycle and refresh on trigger events, new risk information or a national risk assessment.	Risk methodology, data inputs, approved assessment, residual-risk decisions, trigger log and action plan.	[2], [11]
Assess new technology before launch	Identify, record and mitigate ML/TF/PF risks before launching a new product, delivery channel or technology. For BoG-licensed institutions, retain evidence of the required BoG approval before launch.	Pre-launch risk assessment, control design, model testing, approval pack and BoG correspondence.	[2]
Risk-rate each relationship	Assign a documented customer risk rating using ownership, PEP, sanctions, business, product, channel, transaction and geographic factors. Ensure overrides are reasoned, approved and monitored.	Scoring methodology, input data, rating, override log, approver and review date.	[1], [2]
Apply full PEP controls	Detect foreign and domestic PEPs, persons entrusted by international organisations, relevant traditional rulers, family members and close associates. Obtain senior-management approval before establishing or continuing the relationship, establish source of wealth and funds, and conduct enhanced ongoing monitoring.	PEP screening, relationship map, approval, source-of-wealth and source-of-funds substantiation, review and monitoring record.	[1], [2]
Meet BoG PEP reporting expectations	For BoG-licensed institutions, operationalise the current guideline's requirement to report PEP transactions to FIC and submit an STR within 24 hours when activity is abnormal or suspicious. Confirm the prescribed format and channel with FIC.	PEP transaction report, filing receipt, AMLRO review, STR where applicable and reporting procedure.	[2]
Screen sanctions comprehensively	Screen customers, beneficial owners, controllers, signatories, counterparties and payment parties against current binding FIC or competent-authority and UN designation lists. Apply other lists required by the current BoG guideline and the institution's risk policy, without representing every foreign list as independently binding Ghanaian law.	List inventory, update logs, screening results, fuzzy-match settings, alert decisions and quality assurance.	[1], [2]
Freeze and report confirmed designated-property exposure	When a binding designation or applicable targeted-financial-sanctions rule is confirmed, do not enter or continue the transaction, freeze or prevent dealing with the funds or property as required, and report immediately to FIC or the competent authority. Preserve controls for attempted transactions and false-positive resolution.	Match validation, freeze record, blocked transaction, immediate report, legal escalation and release authority where applicable.	[1], [2], [12]

05. ENHANCED DUE DILIGENCE AND HIGHER-RISK RELATIONSHIPS

Enhanced due diligence and higher-risk relationships

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply EDD to higher-risk cases	For higher-risk customers or activity, collect additional identity, ownership, business, purpose, source-of-funds and source-of-wealth information; obtain senior approval; increase monitoring; and shorten review intervals. Do not apply blanket de-risking solely because of geography or customer class.	EDD checklist, corroborating records, approval, monitoring plan and next-review date.	[1], [2]
Control correspondent relationships	Assess the respondent's ownership, management, reputation, regulation, AML controls and quality of supervision; understand each institution's responsibilities; obtain senior approval; and prohibit shell-bank exposure and unapproved payable-through access.	Correspondent questionnaire, public-source checks, approval, contract, control allocation and periodic review.	[1], [2]
Control third-party reliance	Rely on another institution only where the applicable conditions are met, required CDD information is immediately available and underlying documents can be obtained without delay. Retain ultimate responsibility and test the provider.	Reliance due diligence, agreement, sample retrieval test, oversight results and exit plan.	[1], [2]
Escalate opaque and cash-intensive structures	Apply EDD to unexplained ownership layers, nominee arrangements, cash-intensive merchants, rapid pass-through activity, high-risk countries, adverse information and structures inconsistent with the stated business model.	Risk triggers, adverse-media research, ownership clarification, site or activity evidence, decision and monitoring rules.	[1], [2], [11]
Investigate unusual activity	Examine complex, unusually large or unusual patterns with no apparent lawful or economic purpose, document the background and purpose, and preserve the result for supervisory review. File within 24 hours if suspicion or reasonable grounds arise.	Case narrative, transaction analysis, supporting documents, AMLRO decision and STR receipt where filed.	[1], [2], [13]

06. MONITORING, PAYMENTS AND FINTECH CONTROLS

Monitoring, payments and fintech controls

Keep customer profiles current and operate monitored, information-complete payment and fintech services.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Deploy automated transaction monitoring	For BoG-licensed institutions, develop or acquire an automated tool covering all transactions, products and channels in real time or close of day, with embedded sanctions screening. Calibrate scenarios to the institution's risk profile and audit the system yearly.	System inventory, data lineage, scenario library, thresholds, validation, alert metrics, tuning and annual audit.	[2]
Refresh CDD by risk and trigger	For BoG-licensed institutions, refresh high-risk customer files at least annually, medium-risk files at least every three years and low-risk files at least every five years, with earlier review after material ownership, profile, behaviour, sanctions, PEP or adverse-information changes.	Review calendar, trigger feed, completed refresh, overdue dashboard and restriction process.	[2]
Apply complete domestic and cross-border wire controls	For cross-border transfers of USD 1,000 equivalent or more, obtain, hold and transmit the prescribed originator and beneficiary information, including the transaction purpose and required identification data. Below USD 1,000, obtain and retain the minimum names and account numbers or traceable transaction references, and verify them when suspicious. For domestic transfers, ensure that originator and beneficiary information accompanies or remains traceable to the transfer. Establish procedures for executing, rejecting or suspending incomplete transfers and make traceability information available to the beneficiary institution or competent authority by close of day after receiving a request. Ordering, intermediary and beneficiary institutions must detect missing information, obtain and verify it where required, retain records and apply role-specific reject, suspend, reverse or monitoring controls. Where required information cannot be obtained, do not execute or accept the transfer and file an STR with FIC within 24 hours.	Payment-message fields, domestic traceability, role-based procedures, request log, reject or suspension queue, verification and STR receipt	BoG/FIC AML/CFT/CPF Guideline, sections 2.6.10.1-2.6.10.4
Scope electronic-transfer reporting correctly	Commercial banks should report inward and outward transfers above USD 1,000 to FIC within the prescribed 24-hour framework. Other institutions must apply only the thresholds and report types prescribed for their class; confirm the current FIC or supervisory instruction rather than copying the commercial-bank example.	Institution-class mapping, current threshold notice, report file, submission receipt and exception report.	[1], [2], [13]
Apply virtual-asset controls only where in scope	If the institution is authorised for or exposed to virtual-asset activity, assess wallet, counterparty, travel-rule, sanctions, source-of-funds and transaction risks under the current Ghanaian licensing and supervisory framework. Do not imply that a pending or evolving authorisation route permits unlicensed activity.	Legal-scope decision, licence or approval, wallet and counterparty controls, travel-rule data, monitoring and STR records.	[2], [10]
Control agents, merchants and outsourced operations	Risk-assess agents, merchants and outsourced providers before appointment; verify legal existence, ownership, location, settlement account and activity; contract for compliance and audit rights; monitor behaviour; and terminate prohibited or deceptive activity.	Due-diligence file, site or digital checks, contract, training, monitoring dashboard, complaints and termination log.	[2], [10]

07. REPORTING, RECORDS, PRIVACY AND REGULATORY ASSURANCE

Reporting, records, privacy and regulatory assurance

Meet FIC and BoG reporting clocks, preserve evidence, govern personal data and demonstrate effective assurance.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
File STRs within 24 hours	Submit an STR to FIC within 24 hours after suspicion or reasonable grounds arise, including attempted transactions and regardless of amount. Maintain strict non-tipping-off controls and use goAML or the current FIC-prescribed secure channel.	Case chronology, AMLRO decision time, STR, filing receipt, access log and customer-communication controls.	[1], [2], [13], [14]
Submit applicable threshold reports	Report an above-threshold cash transaction to FIC within 24 hours after it occurs. The current BoG/FIC Guideline operationalises this through daily prescribed-medium reporting and states thresholds of GHS 50,000 for banks and GHS 20,000 for specialised deposit-taking institutions, including the foreign-currency equivalent. Apply the threshold prescribed for the institution's actual sector and include linked transactions where the governing rule requires aggregation. FIC's public material separately gives GHS 50,000 as an example for banking and securities. Confirm the current Gazette threshold and filing instruction before implementation. ECTR reporting applies to commercial banks for inward and outward transfers exceeding USD 1,000, with reporting within 24 hours after transfer or receipt.	Sector threshold register, Gazette or authority confirmation, linked-transaction logic, daily report, ECTR, submission receipts and reconciliation	Act 1044, sections 40 and 42; FIC Report Types; BoG/FIC AML/CFT/CPF Guideline
Submit BoG compliance returns on time	For BoG-licensed institutions, prepare the applicable half-year and year-end AML/CFT/CPF compliance returns and supporting schedules for submission by 15 July and 15 January respectively, plus other prescribed SRAQ, PEP, CTR, ECTR, STR, training, audit and data returns.	Regulatory calendar, signed return, source-data reconciliation, approval and submission receipt.	[2]
Retain retrievable records for at least five years	Keep CDD, beneficial ownership, transaction, correspondence, investigation, reporting, training and audit records for at least five years after the relationship ends or the occasional transaction occurs, and longer where a lawful hold or sector rule requires.	Retention schedule, repository controls, sample retrieval, legal-hold log and deletion evidence.	[1], [2]
Register before processing personal data	Register the data controller or processor with the Data Protection Commission before processing personal data and renew on the current two-year cycle. For a newly commenced controller, also check the statutory commencement filing timing under Act 843.	DPC certificate, renewal diary, processing inventory and legal timing note.	[15], [16], [17]
Operate a privacy and security programme	Appoint and train a Data Protection Supervisor; publish a clear privacy notice; apply purpose limitation, minimisation, accuracy, retention and security; support data-subject rights; assess high-risk processing; govern processors and cross-border transfers; and maintain a breach-response procedure.	Appointment, training, privacy notice, processing records, DPIAs, contracts, rights log, security tests and incident register.	[15], [17], [18]
Maintain evidence-led regulatory assurance	Run periodic management testing across onboarding, ownership, PEP, sanctions, monitoring, STR timeliness, threshold reports, records, privacy and regulatory returns. Report exceptions to accountable executives and the board until verified closure.	Control inventory, test scripts, sampled files, metrics, issue register, board reporting and closure proof.	[2], [17]

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.

Bank of Ghana / Financial Intelligence Centre — AML/CFT/CPF Guideline, September 2025
Bank of Ghana / Financial Intelligence Centre · primary
Open official source

Revised Supervisory Guidance Note on the Use of the Ghana Card for Accountable Institutions, November 2025
Bank of Ghana · primary
Open official source

Office of the Registrar of Companies — Entity Information Search
Office of the Registrar of Companies · primary
Open official source

Office of the Registrar of Companies — Frequently Asked Questions
Office of the Registrar of Companies · primary
Open official source

Office of the Registrar of Companies — Public Directive on Non-Issuance of Bearer Shares
Office of the Registrar of Companies · primary
Open official source

Bank of Ghana — FinTech and Innovation Office Licence Requirements
Bank of Ghana · primary
Open official source

Ghana Financial Intelligence Centre — Targeted Financial Sanctions resources
Ghana Financial Intelligence Centre · primary
Open official source

Data Protection Commission Ghana — Data Protection Act, 2012 (Act 843)
Data Protection Commission Ghana · primary
Open official source

Data Protection Commission Ghana — Registration
Data Protection Commission Ghana · primary
Open official source

Data Protection Commission Ghana — Guidance for Organisations
Data Protection Commission Ghana · primary
Open official source

Data Protection Commission Ghana — Guidelines to Demonstrate Data Protection Compliance
Data Protection Commission Ghana · primary
Open official source

VOVE ID — Ghana Merchant Verification Guide 2026 (contextual implementation reference)
VOVE ID · contextual
Open contextual guide

Jurisdictions under Increased Monitoring and High-Risk Jurisdictions Subject to a Call for Action, 19 June 2026
FATF · primary
Open official source

Anti-Money Laundering Act, 2020 (Act 1044), current AML/CFT/CPF resources and reporting templates
Securities and Exchange Commission Ghana · primary
Open official source

National AML/CFT/CPF Risk Assessment for Ghana 2024
Bank of Ghana · primary
Open official source

Companies Act, 2019 (Act 992) and Companies Regulations, 2023
Office of the Registrar of Companies · primary
Open official source

Beneficial Ownership declaration forms
Office of the Registrar of Companies · primary
Open official source

Document control

Version 1.1 / Published 15 July 2026 / Last reviewed 15 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general compliance information, not legal advice. Act 1044 applies across accountable institutions, while the September 2025 BoG/FIC Guideline is the principal overlay used here for Bank of Ghana-licensed institutions. Securities, insurance, pensions, DNFBP and other regulated businesses must add their own supervisor's current rules. Confirm commencement, amendments, forms, thresholds and filing channels with the relevant Ghanaian authority before implementation.