POLICY & PROCEDURES MANUAL

Anti-Money Laundering Counter-Terrorist Financing

and Counter-Proliferation Financing

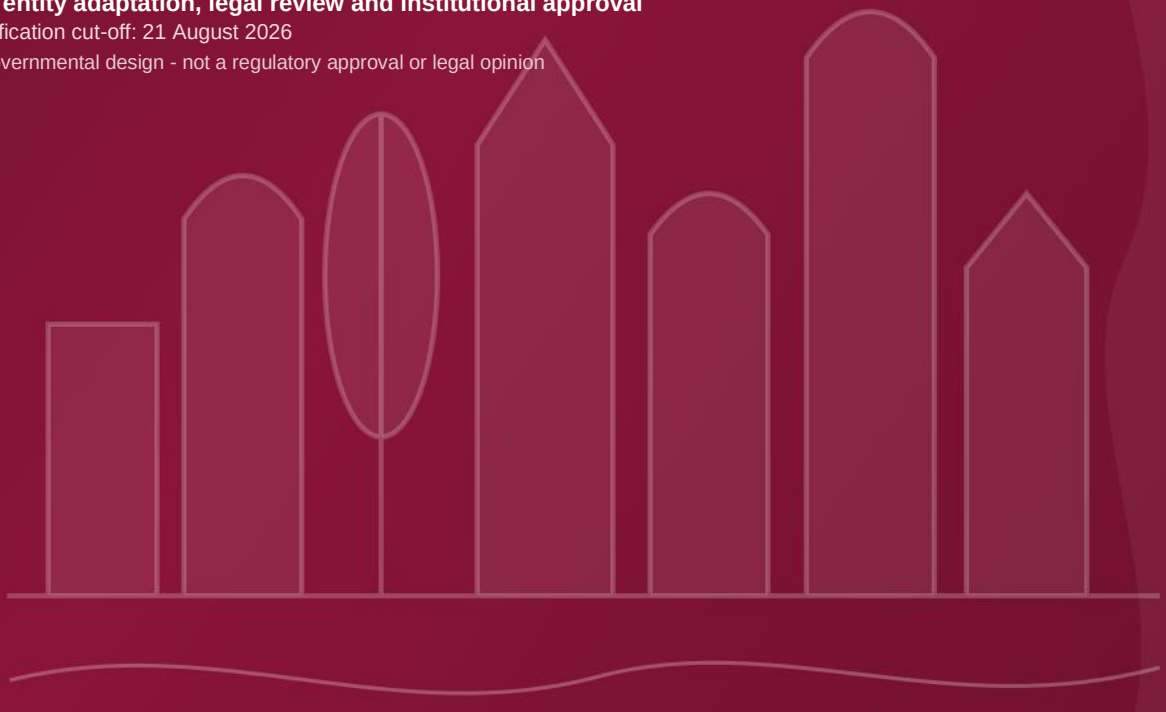
Sector edition: insurance, fintech and payment services supervised by Qatar Central Bank

Built on Qatar's national framework and the official sector sources identified in this edition. The authoritative Arabic legal text and current regulator instruments must be verified before approval.

Sector draft for entity adaptation, legal review and institutional approval

Version 1.0 | Verification cut-off: 21 August 2026

Professional non-governmental design - not a regulatory approval or legal opinion



Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Legal status and limitations of use

Status	A combined sector edition requiring the entity to select only the chapters applicable to its QCB licence: insurance, payment service, e-money/wallet, merchant acquiring, fintech or another supervised activity.

This edition addresses the overlapping AML/CFT controls of insurance, payment and technology-enabled financial services while maintaining product-specific overlays. The entity must define whether the customer is the policyholder, insured, beneficiary, claimant, merchant, wallet holder, payer, payee, agent or another party and apply CDD and monitoring at the legally relevant points.

Insurance and payments are not interchangeable. Life or investment-linked insurance, general insurance, wallets, merchant acquiring and technology platforms present different value flows and supervisory rules. The institution shall delete irrelevant material and verify all product definitions, thresholds, safeguarding and reporting requirements against the current QCB instrument.

The content distinguishes: (1) a fact or requirement supported by an official source, (2) a professional control design proposed to make the requirement operable and testable, and (3) an internal decision that the entity must complete. This manual does not replace qualified Qatari legal advice or the current instructions, forms and decisions of the competent authority.

Sector-edition control card

Target sector	Insurance, fintech and payment service activities supervised by Qatar Central Bank
Regulator / competent authority	Qatar Central Bank (QCB)
Applicability status	A combined sector edition requiring the entity to select only the chapters applicable to its QCB licence: insurance, payment service, e-money/wallet, merchant acquiring, fintech or another supervised activity.
Version	1.0
Document status	Sector draft for entity adaptation, legal review and institutional approval
Verification cut-off	21 August 2026
Prepared by	Ahmad Abumanei
Information classification	Internal - Controlled; STR and sanctions files are more restricted

Entity information - intentionally blank

Instruction	The response cells below are intentionally blank. The document owner shall complete them from the commercial registration, licence, organisation structure, systems and approved governance records before institutional approval.

Legal name of entity	
Commercial / trading name	
Legal form	
Commercial registration number	

Licence number and category	
Registered office	
Branches and subsidiaries	
Licensed products and services	
Delivery channels	
Markets / geographic footprint	
Financial year	
MLRO / Compliance Officer	
Deputy MLRO	
Official contact details	
Document owner	
Entity approval date for this edition	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Review and approval gate

Role	Name	Decision	Date	Signature / minutes reference
MLRO / Compliance				
Legal				
Risk				
Senior Management				
Governing Body / Committee				

Revision history

Version	Date	Description	Reason / source	Approved by
1.0	21 August 2026	Initial English sector edition	Requested sector translation and adaptation	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

How to use this manual and the evidence key

Use the manual in the following order: confirm legal and sector applicability; complete the entity information; approve governance and risk appetite; adapt the policies, controls, procedures and forms; configure systems and data; train personnel; perform independent testing; close material gaps; and obtain formal approval. A form or control shall not be used in isolation from its governing policy, trigger, owner and evidence.

Classification	Meaning and treatment
Regulatory requirement	An obligation expressly stated, or directly derived, from an applicable Qatari law, regulation, decision, rule or binding supervisory instruction. The cited source must be verified before institutional approval.
Professional control design	A proposed process, segregation of duties, record, system rule or management information measure that converts a requirement into a control capable of operation and testing. It requires entity approval.
Internal decision required	A parameter that the entity must determine, such as authority limits, review frequency, risk appetite, system configuration, staffing level or escalation threshold.
Conditional sector requirement	A requirement that applies only after the licensed activity, regulator, product and customer scope are confirmed. It must not be applied automatically to every entity.
Governing rule	Blank fields and decision tables are deliberate. A conditional sector requirement must be verified from the official source before it is represented as applicable to the entity.

Table of contents

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Executive summary

This edition provides a complete operating framework for managing money-laundering, terrorist-financing and proliferation-financing risk in the identified Qatar sector. It combines national legal foundations, sector applicability, governance, risk assessment, customer due diligence, beneficial ownership, PEP and EDD controls, sanctions and TFS, monitoring, STR reporting, records, training, assurance, professional forms and editable process flows.

19 policy chapters	**77** defined controls	**13** detailed procedures	**20** editable forms	**10** editable flowcharts

Control-design principles

- Risk before activity: inherent and residual risk shall determine due diligence, monitoring, staffing and assurance.
- Accountability remains with the entity: reliance, introduction and outsourcing do not transfer ultimate responsibility.
- Suspicion remains independent: the MLRO's STR decision is protected from commercial veto and tipping-off.
- Data is evidence: a control is not effective when the entity cannot prove population completeness or reconstruct the decision.
- Sanctions are a separate legal track: potential matches are adjudicated and confirmed legal triggers are frozen and reported without delay.
- Closure requires operation: policies, findings and changes close only when design, implementation and operating evidence meet acceptance criteria.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

National and sector legal-reference register

Verification cut-off	Sources were checked for this professional draft up to 21 August 2026. The entity shall repeat the official-source check when approving or reviewing the manual because laws, decisions, rules, guidance, forms and links may change.

National and international framework

Instrument / source	Status	Relevance	Official link
Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing	Primary national AML/CFT law, read with subsequent amendments. The Arabic text is authoritative; available English translations are unofficial.	Risk assessment, preventive measures, CDD, beneficial ownership, PEPs, reporting, confidentiality, supervision and sanctions.	Open official source
Council of Ministers Decision No. (41) of 2019 issuing the Implementing Regulations	National implementing regulations, read with later amendments including Decision No. (14) of 2021 and Decision No. (8) of 2026.	Operational detail for risk-based controls, customer due diligence, beneficial ownership and implementation duties.	Open official source
Decree-Law No. (19) of 2021	Amends provisions of Law No. (20) of 2019.	Must be read with the consolidated national framework during final legal verification.	Open official source
Decree-Law No. (18) of 2025	Amends provisions of Law No. (20) of 2019, including national governance provisions.	Updates the national AML/CFT institutional framework and must be reflected in the legal-change register.	Open official source
Public Prosecutor Decision No. (1) of 2020 and Decision No. (59) of 2020	Qatar targeted financial sanctions implementation instruments and operational guidance.	List monitoring, match validation, freezing without delay, prohibition on making funds available, reporting and record retention.	Open official source
Law No. (27) of 2019 on Combating Terrorism	National counter-terrorism law relevant to terrorist financing and targeted financial sanctions.	Terrorist financing offences, designations and sanctions-related obligations.	Open official source
FATF Recommendations and Qatar Mutual Evaluation Report 2023	International standard and effectiveness assessment; neither replaces Qatari law.	Risk-based approach, preventive measures, beneficial ownership, reporting, supervision, targeted financial sanctions and proliferation financing.	Open official source
Sector rules, instructions, circulars, forms and guidance	The entity must identify the current instruments issued by its actual supervisor and applicable to its licence.	Sector scope, thresholds, forms, reporting channels, review cycles, governance expectations and product-specific controls.	Open official source

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Sector and common official sources

Instrument / source	Status	Relevance	Official link
Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing	National legal source	National AML/CFT framework. English translations available through QFCRA are expressly identified as unofficial; the Arabic text is authoritative.	Open official source
Implementing Regulations issued by Council of Ministers Decision No. (41) of 2019, as amended	National legal source	Operational detail for preventive measures and institutional programmes, including later amendments listed by QFCRA.	Open official source
FATF Recommendations and Qatar Mutual Evaluation Report 2023	International reference	International design and effectiveness benchmark; not a substitute for applicable Qatari law or sector rules.	Open official source
Qatar Central Bank - Financial Crimes Enforcement Management	Official sector source	Official QCB supervisory source for financial-crime risk-based oversight.	Open official source
Qatar Central Bank - Supervision Sector	Official sector source	Official source used to confirm the licence category and supervisory perimeter.	Open official source
Qatar Central Bank official instructions pages	Official sector source	The entity must identify and retain the current instructions specifically applicable to insurance, payments, fintech or the licensed service.	Open official source
Translation status	QFCRA expressly states that English translations of Qatar State laws on its AML/CFT legislation page are unofficial and that the official laws are in Arabic. Legally significant decisions require verification against the authoritative text and qualified advice.		

Glossary

Term	Working definition for this manual
Money laundering (ML)	Conduct falling within the definition and offences established by the applicable Qatari legislation, including dealing with criminal proceeds with the legally required knowledge or intent.
Terrorist financing (TF)	The collection, provision, movement or management of funds or resources for terrorist purposes or designated persons or entities. The funds may originate from legitimate sources.
Proliferation financing (PF)	Financing or financial services associated with the proliferation of weapons of mass destruction, including exposure to designated parties, controlled goods, opaque trade routes and sanctions evasion.
Customer due diligence (CDD)	Measures to identify and verify the customer, representative and beneficial owner, understand the purpose and intended nature of the relationship, and conduct ongoing scrutiny.
Enhanced due diligence (EDD)	Additional and more intensive measures applied to higher-risk relationships, transactions or situations required by law, rule or risk assessment.
Simplified due diligence (SDD)	Reduced extent or timing of CDD permitted only where lower risk is evidenced and the applicable framework allows it; it is not zero due diligence.
Beneficial owner (BO)	The natural person who ultimately owns or controls a customer, or on whose behalf a transaction is conducted, determined under the applicable Qatari criteria.
Politically exposed person (PEP)	A person entrusted with a prominent public function, together with relevant family members and close associates under the applicable framework.
Money Laundering Reporting Officer (MLRO)	The appointed officer with sufficient authority, independence, access and resources to receive internal disclosures, assess suspicion and communicate with competent authorities.
Qatar Financial Information Unit (QFIU)	The national central unit responsible for receiving and analysing suspicious transaction reports and related information under Qatari law.
Suspicious transaction report (STR)	A report submitted to the QFIU when suspicion or reasonable grounds to suspect arise, using the prescribed channel and current form.
Tipping-off	Prohibited disclosure that may inform a customer or unauthorised person that an STR, analysis or related investigation exists or may occur.
Targeted financial sanctions (TFS)	Freezing and prohibition measures applied without delay to funds or economic resources of designated persons and entities under applicable lists and decisions.
Potential match	A screening similarity requiring analysis; it does not, by itself, establish that the screened party is designated.
True match	A match supported by sufficient identifiers that triggers the applicable legal action and escalation.
Inherent risk	The level of ML/TF/PF risk before considering the effect of controls.
Control effectiveness	The extent to which a control is appropriately designed, implemented and operating consistently, supported by evidence.
Residual risk	The risk remaining after considering the assessed effectiveness of relevant controls.
Source of funds (SoF)	The direct origin of the money used in a particular transaction or relationship.
Source of wealth (SoW)	How the customer or beneficial owner accumulated overall wealth over time.
Trigger event	A change or occurrence that requires risk reassessment or file review before the next scheduled review.
Ongoing monitoring	Review of transactions, behaviour and customer information throughout the relationship against the known profile and expected activity.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Term	Working definition for this manual
Designated non-financial businesses and professions (DNFBPs)	Non-financial activities and professions brought within AML/CFT obligations when the statutory scope or specified transaction conditions are met.
Risk-based approach (RBA)	The allocation of due diligence, monitoring, resources and management attention in proportion to identified and assessed risk.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Sector applicability and control overlay - QCB Insurance, FinTech & Payments

Applicability	A combined sector edition requiring the entity to select only the chapters applicable to its QCB licence: insurance, payment service, e-money/wallet, merchant acquiring, fintech or another supervised activity.

This edition addresses the overlapping AML/CFT controls of insurance, payment and technology-enabled financial services while maintaining product-specific overlays. The entity must define whether the customer is the policyholder, insured, beneficiary, claimant, merchant, wallet holder, payer, payee, agent or another party and apply CDD and monitoring at the legally relevant points.

Insurance and payments are not interchangeable. Life or investment-linked insurance, general insurance, wallets, merchant acquiring and technology platforms present different value flows and supervisory rules. The institution shall delete irrelevant material and verify all product definitions, thresholds, safeguarding and reporting requirements against the current QCB instrument.

Verified sector facts

- QCB is the competent supervisor for the in-scope licensed activity; the exact licence and instruction set determine the binding product requirements.
- Remote onboarding, agents, merchants and outsourced platforms increase channel and third-party risk but do not transfer the licensed entity's accountability.
- Policy premiums, refunds, claims, wallet loading, merchant settlement and rapid payment flows require different expected-activity baselines and monitoring scenarios.

Sector risk dimensions

Risk dimension	Exposure / misuse mechanism	Required response
Policyholder, beneficiary and claimant changes	Insurance value may be redirected through third-party premium payments, beneficiary changes, early surrender, refunds or claims.	Identify all legally relevant parties, verify change authority and monitor unusual value redirection.
Merchant and agent networks	Agents and merchants can introduce customers, accept value or transmit data outside direct control.	Risk-based onboarding, contractual duties, transaction oversight, site/quality review and prompt termination rights.
Wallets, prepaid value and rapid movement	Digital value can be loaded, transferred and cashed out quickly across multiple parties and devices.	Customer/merchant limits, device and network analytics, linked-account monitoring and real-time screening where required.
Non-face-to-face onboarding	Remote identity fraud, synthetic identity, account takeover and mule use can undermine CDD.	Layered electronic verification, liveness/device controls, first-payment checks and trigger review.
Refunds, claims and settlement	Value returned to a different payer, claimant, bank account or merchant may disguise laundering or fraud.	Return-to-source controls, authority verification, supporting documents and anomaly monitoring.
Platform, API and outsourcing dependency	Control failures may arise from incomplete API fields, provider outages, model changes or inaccessible records.	Data contracts, reconciliations, control testing, incident fallback, audit rights and model/change governance.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Sector control catalogue

Each control states who performs it, how, when and with what evidence. The cited basis identifies the risk or source used for design and does not replace clause-level legal mapping.

IFT-01 - Relevant-party identification

Owner	Onboarding / Policy / Merchant Operations
How the control operates	Identify and screen policyholder, insured, beneficiary, claimant, payer, merchant, owner/controller and agent as applicable.
Trigger / frequency	At onboarding, change, claim/settlement and trigger
Evidence	Party-role map and screening evidence
Basis	Product-specific CDD
Classification	Preventive / Semi-automated

IFT-02 - Third-party funding and refund rule

Owner	Operations
How the control operates	Detect third-party funding and require justified, verified return-to-source or approved beneficiary treatment.
Trigger / frequency	For each premium, load, refund, surrender or payout
Evidence	Funding/payout evidence and exception approval
Basis	Expected-activity and misuse control
Classification	Preventive / Automated

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

IFT-03 - Remote identity assurance

Owner	Digital Onboarding / Fraud / KYC
How the control operates	Apply approved electronic identity, liveness, device, duplicate-identity and first-payment controls.
Trigger / frequency	Before activation and on device/profile trigger
Evidence	Verification and device-risk record
Basis	Channel-risk mitigation
Classification	Preventive / Automated

IFT-04 - Merchant/agent risk oversight

Owner	Distribution / Acquiring / Compliance
How the control operates	Assess ownership, business, location, products and expected flows; monitor settlement and agent conduct.
Trigger / frequency	Before appointment and risk-based periodic/trigger review
Evidence	Due diligence, contract and monitoring report
Basis	Third-party and channel control
Classification	Preventive / Manual

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

IFT-05 - Rapid-value movement monitoring

Owner	Transaction Monitoring
How the control operates	Link wallet, device, payer, payee, merchant and cash-out activity and compare velocity with tier and profile.
Trigger / frequency	Near-real-time/daily as approved
Evidence	Alerts, cases and population reconciliation
Basis	Digital payments risk
Classification	Detective / Automated

IFT-06 - Insurance event anomaly review

Owner	Claims / Policy Servicing with Compliance
How the control operates	Review early surrender, overpayment/refund, beneficiary change, claim pattern and third-party settlement anomalies.
Trigger / frequency	At event before payout where applicable
Evidence	Event checklist and escalation
Basis	Insurance value-transfer risk
Classification	Preventive / Semi-automated

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

IFT-07 - API and data reconciliation

Owner	Technology / Data
How the control operates	Reconcile customers, parties, transactions, screening and monitoring events across source and platform interfaces.
Trigger / frequency	Each processing cycle
Evidence	Reconciliation and error reprocessing
Basis	Control completeness
Classification	Detective / Automated

IFT-08 - Model and limit governance

Owner	Product Risk / Compliance
How the control operates	Validate customer/merchant limits, fraud/AML models, rules, overrides and change impact.
Trigger / frequency	Before change and periodically
Evidence	Validation, tuning and approval
Basis	Professional control design
Classification	Detective / Manual

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Sector CDD and evidence baseline

The following evidence is a sector starting point. The entity shall add current legally required fields and product documents and remove items that do not apply to the licensed activity.

- Identity and independent digital or documentary verification
- Party-role mapping for policy/payment lifecycle
- Beneficial ownership and merchant/business evidence
- Authority of beneficiary/claimant/representative changes
- Purpose and expected loading, premium, claims or settlement profile
- Funding and payout bank-account evidence
- Agent/merchant due diligence and contract
- Device, channel and jurisdictional risk evidence

Sector monitoring scenarios

IFT-S01 - Rapid load-transfer-cash-out

Scenario logic	Stored value is loaded and quickly transferred or withdrawn through multiple accounts or devices inconsistent with purpose.
Minimum data	Wallet, device, payer/payee, timestamps, cash-out
Escalation objective	Assess mule, fraud and pass-through typologies.

IFT-S02 - Linked wallet or device network

Scenario logic	Multiple customers share device, credentials, funding source, IP, address or beneficiary without legitimate relationship.
Minimum data	Device/IP, identity, account, funding and beneficiary links
Escalation objective	Investigate network ownership, mule or synthetic identity.

IFT-S03 - Insurance early surrender/refund

Scenario logic	Policy is funded and cancelled or surrendered early, or overpayment is refunded to a different party.
Minimum data	Policy events, premium payer, refund account, timing
Escalation objective	Review economic rationale, payer identity and source/recipient.

IFT-S04 - Beneficiary or claimant change before payout

Scenario logic	Material change is made shortly before claim, maturity or payout.
Minimum data	Change history, authority, claimant, bank account
Escalation objective	Reverify authority and consider fraud/ML escalation.

IFT-S05 - Merchant settlement mismatch

Scenario logic	Merchant settlements, chargebacks or transaction mix are inconsistent with stated business and peer profile.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Minimum data	Merchant MCC/business, transactions, refunds, chargebacks, settlements
Escalation objective	Assess laundering through merchant processing and collusion.

IFT-S06 - Agent concentration and structuring

Scenario logic	Agent-originated customers or transactions show clustered sub-threshold, common-beneficiary or high-risk corridor patterns.
Minimum data	Agent, customer, value, corridor, beneficiary
Escalation objective	Review agent conduct, linked customers and control circumvention.

Sector red flags

A red flag is an investigation trigger, not a conclusion. The analyst shall compare it with the expected profile, reconstruct the relevant facts and document whether suspicion forms.

- Premium, wallet load or merchant funds paid by unexplained third parties
- Repeated refunds or payouts to accounts different from the original source
- Early surrender or cancellation without economic rationale
- Beneficiary or claimant changed shortly before payout
- Multiple customers linked to one device, funding source or beneficiary
- Rapid load-transfer-cash-out with minimal retained value
- Merchant volumes or transaction types inconsistent with business
- Agent portfolio with abnormal sub-threshold or common-beneficiary patterns
- Identity data repeatedly changed after remote activation
- Provider or platform cannot produce complete transaction and screening records

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Sector operating procedures

S-01 Digital customer or wallet activation

1. Capture identity and purpose
2. Perform electronic verification and device checks
3. Screen customer and relevant parties
4. Calculate risk and limits
5. Complete EDD where triggered
6. Activate only after system gate
7. Monitor device and transaction triggers

Required evidence	The process owner shall retain the source documents, screening or system result, risk decision, approval, exception and final disposition for each case.

S-02 Insurance payout or refund review

1. Identify payer, policyholder, beneficiary and claimant
2. Verify authority and event documents
3. Compare payout destination with original source
4. Screen relevant parties
5. Assess event and funding anomalies
6. Approve, hold or escalate
7. Retain decision evidence

Required evidence	The process owner shall retain the source documents, screening or system result, risk decision, approval, exception and final disposition for each case.

S-03 Merchant/agent appointment and oversight

1. Identify entity, BO and controllers
2. Verify licence/business and expected flows
3. Screen and risk-rate
4. Set contract controls and limits
5. Monitor transactions and service quality
6. Review on trigger
7. Remediate, suspend or terminate

Required evidence	The process owner shall retain the source documents, screening or system result, risk decision, approval, exception and final disposition for each case.

Sector RACI

Code	Role
GOV	Governing Body / Senior Management
BUS	Business / Relationship Owner
AML	MLRO / Compliance

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

OPS	KYC / Operations
TECH	Technology / Data
L/R	Legal / Risk
IA	Internal Audit

Activity	GOV	BUS	AML	OPS	TECH	L/R	IA
Approve product-specific customer standard	A	C	R	R	C	C	I
Operate digital identity controls	I	C	C	R	R	C	I
Approve merchant/agent	A	R	R	C	I	C	I
Review payout/refund anomaly	I	R	A	R	C	C	I
Monitor rapid payment patterns	I	C	A	R	R	C	I
Validate model and limits	I	C	C	C	R	A	I
Manage platform outage	I	C	A	R	R	C	I
Assure sector controls	I	I	C	I	I	C	A/R

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Blank sector adaptation form

Instruction	All response cells are deliberately blank. Complete the form from the entity's approved licence, risk assessment, system design and authorities; attach evidence and legal sign-off.

Sector adaptation field	Entity response
Licence and product type	
Relevant customer/party roles	
Remote channel and verification method	
Funding and payout flow	
Agent/merchant/provider details	
Expected volume, value and velocity	
Device and jurisdictional exposure	
Risk rating and EDD	
Limits and restrictions	
Monitoring scenarios	
Conditions and evidence	
Approvals and review date	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 1: Purpose, scope and governing principles

Legal / framework basis	Law No. 20 of 2019, Articles 6 and 7; FATF Recommendation 1

Objective	Define the purpose, boundaries and interpretation of the manual and prevent a generic template from being treated as evidence of compliance before sector and entity adaptation.

Policy statement

The entity shall maintain a documented, risk-based AML/CFT/CPF programme covering all relevant legal entities, business units, products, customers, channels, employees and outsourced activities. This manual becomes operative only after the entity information, regulatory applicability, risk appetite, systems, authorities and sector requirements are completed and formally approved.

Detailed requirements

1.1 Hierarchy of requirements

The manual shall be read with the authoritative Arabic text of Qatari law, the implementing regulations, national decisions, targeted financial sanctions instruments and the current rules, instructions, circulars and forms issued by the competent supervisor. Where requirements conflict, the higher or more specific legal requirement prevails and the issue is referred to Legal and the MLRO before an operational decision is made.

No general statement in this manual may reduce an express obligation. Silence in the manual is not permission, and an unofficial English translation may assist understanding but shall not be the sole basis for a legally significant decision on reporting, freezing, customer refusal, retention or disclosure.

1.2 Persons and lifecycle covered

The programme applies to the governing body, senior management, permanent and temporary employees, secondees, agents, contractors and service providers whose work can affect customer acceptance, transaction execution, screening, monitoring, investigation, reporting, information security or record retention. Relevant duties shall be reflected in contracts, role descriptions, access rights, training and supervision.

Coverage extends across the complete relationship lifecycle: pre-acceptance, identification and verification, risk classification, approval, occasional transactions where applicable, ongoing monitoring, periodic and trigger reviews, investigation, reporting, sanctions action, exit and record retention.

1.3 Proportionality and evidence

The risk-based approach increases the depth, frequency, seniority and resources of controls as risk increases. Lower risk never removes the statutory minimum, and simplified measures are prohibited where suspicion, a higher-risk factor, a sanctions concern or a sector restriction exists.

Every material judgement shall distinguish verified fact, documented assumption, professional assessment and internal decision. The file shall contain sufficient evidence for an independent reviewer to reconstruct the decision, identify who made it and confirm the applicable approval.

1.4 Adaptation and approval gate

Before issue, the entity shall complete its legal name, registration and licence, products, delivery channels, geographic reach, customer segments, regulator, systems, delegated authorities, escalation routes, record locations and review cycles. The MLRO and Legal shall complete a clause-by-clause applicability review.

The governing body or authorised committee shall approve the final controlled version after material gaps are identified, owners and deadlines are assigned, critical controls are tested and any residual risk above appetite is explicitly decided. An uncontrolled draft shall not be represented to a customer, auditor or regulator as an approved policy.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Defined controls

GOV-01 - Legal and sector applicability review

Control owner	Legal and MLRO
Trigger / frequency	Before approval and after a relevant regulatory change
How performed	Map each applicable requirement to the process, owner, control and evidence; record exclusions with a supported legal rationale.
Required evidence	Signed applicability matrix and decision log
Classification	Preventive / Manual

GOV-02 - Controlled approval and distribution

Control owner	Governing body / authorised committee
Trigger / frequency	At initial issue and each material revision
How performed	Approve a uniquely numbered version, publish it through a controlled repository and withdraw superseded copies.
Required evidence	Approval minutes, version register and distribution record
Classification	Preventive / Manual

GOV-03 - Acknowledgement of responsibility

Control owner	Human Resources and MLRO
Trigger / frequency	On appointment and after material revision
How performed	Issue role-specific notice and obtain traceable acknowledgement from all in-scope personnel.
Required evidence	Acknowledgement register
Classification	Preventive / Semi-automated

GOV-04 - Annual completeness challenge

Control owner	Compliance Quality Assurance
Trigger / frequency	At least annually
How performed	Compare actual licences, products, channels and outsourced activities with the approved scope and investigate omissions.
Required evidence	Annual scope attestation and exception report
Classification	Detective / Manual

Records and evidence

- Applicability matrix
- Approval minutes

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Controlled-copy register
- Acknowledgements
- Exception log
- Annual scope attestation

Management information and effectiveness indicators

- Percentage of in-scope units mapped
- Acknowledgement completion rate
- Number of uncontrolled copies identified
- Age of open applicability decisions

Escalation rule	Any material uncertainty, uncovered activity or conflict affecting customer acceptance, reporting, freezing or disclosure shall be escalated to the MLRO and Legal. No exception may override an applicable legal obligation.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 2: Regulatory obligations and legal-change management

Legal / framework basis	Law No. 20 of 2019 and amendments; Implementing Regulations and amendments; applicable sector instruments

Objective	Maintain a complete, current and traceable obligations register and convert regulatory change into implemented and tested operational change.

Policy statement

The entity shall maintain a central obligations register identifying the source, effective date, requirement, applicability, accountable owner, process, control, evidence and implementation status. A change is not closed merely because a policy document was amended; closure requires evidence that affected procedures, systems, forms, training and operating controls were updated and tested.

Detailed requirements

2.1 Source hierarchy and ownership

The register shall include national legislation and amendments, implementing regulations, targeted financial sanctions decisions and guidance, sector rules, supervisory instructions and circulars, official forms and relevant FATF standards used as control-design references. Each source shall have an owner, official link, verification date, effective date and authoritative-language status.

Legal owns interpretation of material statutory questions; Compliance owns regulatory inventory and implementation coordination; process owners own operational change; Technology owns system configuration; and independent quality assurance or Internal Audit tests closure without assuming management responsibility.

2.2 Regulatory horizon scanning

Compliance shall review official regulator and government sources at a frequency approved according to risk and shall record a result even when no change is identified. Reliance on memory, informal messaging or undated local copies is not an acceptable horizon-scanning control.

The scan shall also consider licence changes, new products, enforcement notices, national risk assessments, FATF statements, typologies and findings from inspections or independent audits when those sources could change the entity's risk or control obligations.

2.3 Impact assessment and implementation

For each relevant change, the impact assessment shall state the verified legal fact, management interpretation, affected entities and processes, required decisions, system and data impact, customer or transaction impact, implementation deadline, interim risk and compensating controls. Uncertainty shall be made visible rather than concealed in a generic action.

The implementation plan shall identify a single accountable executive, individual actions, dependencies, due dates and acceptance evidence. Changes affecting STRs, TFS, customer identification, record retention or regulatory disclosure receive heightened priority and legal review.

2.4 Closure and post-implementation review

Closure shall require evidence proportionate to the change: revised policy and procedure, approved system requirement, configuration test, updated form, communication and training, migrated data validation and a sample of actual transactions or cases demonstrating operation.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Material changes shall be subject to a post-implementation review after sufficient live operation. Any design defect, inconsistent operation or unintended customer impact shall be reopened, risk-rated and reported through the governance process.

Defined controls

REG-01 - Documented regulatory scan

Control owner	Regulatory Compliance
Trigger / frequency	Approved cycle and upon official notification
How performed	Review named official sources and record the result, source link, reviewer and date.
Required evidence	Regulatory scan log
Classification	Detective / Manual

REG-02 - Legal impact assessment

Control owner	MLRO and Legal
Trigger / frequency	For every relevant change
How performed	Perform clause-level assessment and link the change to products, processes, controls, owners, forms, data and systems.
Required evidence	Approved impact memorandum and implementation plan
Classification	Preventive / Manual

REG-03 - Implementation readiness gate

Control owner	Accountable executive
Trigger / frequency	Before the effective date
How performed	Confirm completion of dependencies, training, technology, data, communication and interim controls.
Required evidence	Readiness checklist and approval
Classification	Preventive / Manual

REG-04 - Independent closure test

Control owner	Compliance QA or Internal Audit
Trigger / frequency	Before final closure or during post-implementation review
How performed	Test design, implementation and an appropriate operating sample independent of the change owner.
Required evidence	Closure test workpaper and evidence
Classification	Detective / Manual

Records and evidence

- Source register
- Obligations register
- Scan log
- Impact memoranda
- Implementation plans
- Test evidence
- Status reports

Management information and effectiveness indicators

- Open changes by risk rating
- Percentage implemented before effective date
- Average impact-assessment time
- Overdue actions
- Reopened closure rate

Escalation rule	A change affecting STR, TFS, prohibited relationships, identity data, beneficial ownership, record retention or regulator access is presumed high impact until assessed otherwise and shall be reported promptly to the MLRO, Legal and accountable executive.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 3: Governance, accountability, independence and resources

Legal / framework basis	Law No. 20 of 2019, Article 7; Implementing Regulations; FATF Recommendation 18

Objective	Establish accountable governance, effective Three Lines separation, an independent MLRO decision path and resources proportionate to the entity's exposure.

Policy statement

The governing body retains ultimate accountability for the adequacy and effectiveness of the AML/CFT/CPF programme. Senior management shall implement the approved framework and provide resources. Business units own and manage the financial-crime risks created by their customers and activities. The MLRO shall have authority, independence, unrestricted access and a direct escalation path, while Internal Audit provides independent assurance and does not operate the controls it tests.

Detailed requirements

3.1 Governing body and committee

The governing body shall approve the risk appetite, policy, enterprise-wide risk assessment, material remediation, MLRO appointment and sufficient people, technology and data resources. Reporting shall present both compliance and effectiveness, including risk above appetite, overdue cases, screening and monitoring limitations, STR themes, control failures and regulator matters.

Committee terms of reference shall define membership, quorum, meeting frequency, reserved decisions, confidentiality, information barriers, minute retention and action tracking. STR subject details shall be restricted to what is lawful and necessary; governance does not justify unnecessary access to protected reports.

3.2 Senior management and first line

Senior management shall translate policy into operating processes, remove conflicts between revenue and compliance, maintain service capacity, enforce risk acceptance conditions and hold managers accountable for data quality and timely escalation. Performance measures shall not reward volume or speed at the expense of control quality.

The first line shall obtain reliable customer information, understand the relationship, apply required restrictions, monitor behaviour, raise internal concerns promptly and remediate deficiencies. Referral to Compliance does not transfer ownership of incomplete CDD, poor data or unexplained activity.

3.3 MLRO, deputy and compliance function

The MLRO shall have direct access to the governing body, staff, systems and records; sufficient seniority and competence; protected authority to challenge and escalate; and adequate time and budget. A competent deputy shall maintain continuity during absence without diluting responsibility or creating unacceptable case backlogs.

No commercial officer may veto an STR decision or delay a confirmed TFS action. The MLRO's decisions shall be documented, access-restricted and based on relevant facts, legal obligations and professional judgement. Material attempts to interfere shall be reported through an independent route.

3.4 Segregation, conflicts and assurance

RACI matrices and access roles shall prevent a person from initiating and finally approving a sensitive onboarding, alert closure, sanctions discount or exception without an approved compensating control. Conflicts shall be declared, reviewed and, where necessary, the file reassigned.

Internal Audit or another sufficiently independent assurance provider shall assess both design and operating effectiveness. Assurance shall have access to evidence but protect STR and sanctions information, and shall not design the controls whose effectiveness it is expected to conclude upon.

Defined controls

GOV-10 - Annual governance and resource adequacy review

Control owner	Governing body / committee
Trigger / frequency	At least annually and upon material change
How performed	Assess workload, competence, vacancy, systems, data quality, budget, assurance findings and forecast exposure.
Required evidence	Minutes and approved resource decision
Classification	Preventive / Manual

GOV-11 - Independent STR decision

Control owner	MLRO
Trigger / frequency	For every internal suspicion disclosure
How performed	Evaluate and record the report-or-not decision without commercial veto and with need-to-know access.
Required evidence	Restricted MLRO decision record
Classification	Preventive / Manual

GOV-12 - Conflict and access review

Control owner	Compliance and Information Security
Trigger / frequency	On appointment, role change, termination and periodically
How performed	Compare job responsibilities, declared conflicts and system permissions with segregation requirements.
Required evidence	Conflict declaration and access review report
Classification	Preventive / Semi-automated

GOV-13 - MLRO continuity test

Control owner	Senior Management
Trigger / frequency	At least annually and on prolonged absence
How performed	Confirm deputy authority, access, competence, filing channel and escalation contacts through a documented scenario test.
Required evidence	Continuity test record
Classification	Preventive / Manual

Records and evidence

- Committee charters
- Appointment decisions
- Role descriptions
- RACI matrices
- Conflict declarations
- Access reviews
- Resource assessments
- Board reports

Management information and effectiveness indicators

- Critical vacancy rate
- Case backlog and ageing
- Decision implementation rate
- Segregation overrides
- High-risk escalation response time
- Training and competence gaps

Escalation rule	Any attempt to influence an STR decision, conceal information, delay freezing, bypass a prohibition or disclose protected information shall be escalated immediately to the MLRO and the chair of the appropriate governing body committee through an independent route.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 4: Enterprise-wide ML/TF/PF risk assessment and risk appetite

Legal / framework basis	Law No. 20 of 2019, Articles 6 and 7; FATF Recommendation 1 and relevant sector guidance

Objective	Identify, assess and document the entity's inherent risk, control effectiveness and residual risk, and use the results to allocate resources and define risk acceptance.

Policy statement

The entity shall maintain an enterprise-wide risk assessment (EWRA) covering customer, product/service/transaction, delivery-channel and geographic risk, together with legal entities, branches, intermediaries, technology, data and outsourced activities. ML, TF and PF shall be considered distinctly. The approved results shall drive risk appetite, CDD intensity, monitoring, screening, training, staffing, product governance and independent assurance.

Detailed requirements

4.1 Scope, data and evidence

The assessment shall use reconciled quantitative data, including customer counts by segment and risk, volumes and values, cash and cross-border activity, jurisdictions, products, channels, alerts, cases, STRs, sanctions results and backlogs. Qualitative sources shall include the national and sector risk assessments, regulator findings, internal cases, audit results and credible typologies.

A data dictionary shall identify the period, source, owner, extraction logic, completeness, reconciliation and limitation for each input. Missing or unreliable data shall be reported as a limitation with a conservative treatment and remediation action, not replaced by an undisclosed estimate.

4.2 Method and scoring integrity

The method shall separately rate inherent exposure, control effectiveness and residual risk using defined scales and documented weights. Control effectiveness shall consider design, implementation and operating evidence; a written policy alone does not justify a risk reduction.

Sensitivity and concentration analysis shall test whether aggregation hides a material product, branch, channel, customer segment or jurisdiction. Overrides and expert judgements shall identify the decision-maker, evidence and impact on the final rating.

4.3 Distinct TF and PF assessment

TF risk shall not be inferred from transaction value alone because small, legitimate-source funds may be collected or directed to a prohibited purpose. The assessment shall consider NPO exposure, conflict and terrorism-linked geographies, collection-and-disbursement patterns, agents and beneficiaries.

PF risk shall consider designated parties and ownership, dual-use goods, trade intermediaries, shipping and trans-shipment routes, front companies, payment chains and evasion indicators. TFS controls may mitigate PF risk but do not replace a documented PF assessment.

4.4 Appetite, action and reassessment

The governing body shall state prohibited exposure, exposure permitted only with enhanced controls and tolerance for residual risk by material segment. Residual risk above appetite shall result in a time-bound treatment, restriction, exit or explicit temporary acceptance by the proper authority where legally permissible.

The EWRA shall be refreshed on the approved cycle and on trigger, including a new product or market, acquisition, material technology change, regulatory amendment, FATF list change, significant STR pattern,

sanctions event, control failure or assurance finding. The change between assessments shall be explained, not merely re-scored.

Defined controls

RISK-01 - EWRA data reconciliation

Control owner	Risk Analytics and Finance/Data Owners
Trigger / frequency	Each assessment cycle
How performed	Reconcile source populations and material totals to controlled systems and investigate unexplained differences.
Required evidence	Signed data pack and reconciliation
Classification	Detective / Semi-automated

RISK-02 - Methodology and challenge

Control owner	MLRO and Enterprise Risk
Trigger / frequency	Before scoring and approval
How performed	Approve scope, factor definitions, weights, thresholds, control-rating criteria and sensitivity tests.
Required evidence	Methodology paper and challenge minutes
Classification	Preventive / Manual

RISK-03 - Residual-risk approval

Control owner	Governing body / committee
Trigger / frequency	At each assessment and material trigger
How performed	Review residual risk against appetite and approve treatments, owners, dates and interim controls.
Required evidence	Approved EWRA and treatment plan
Classification	Preventive / Manual

RISK-04 - Trigger monitoring

Control owner	AML Risk Function
Trigger / frequency	Continuous monitoring with periodic review
How performed	Monitor defined internal and external events and document whether reassessment is required.
Required evidence	Trigger register and reassessment decisions
Classification	Detective / Semi-automated

Records and evidence

- EWRA methodology

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Data dictionary
- Source extracts
- Reconciliations
- Scoring workbook
- Challenge minutes
- Risk appetite
- Treatment plan
- Trigger register

Management information and effectiveness indicators

- Residual risk by factor family
- Exposure above appetite
- Overdue treatments
- Unreconciled data rate
- High-risk customer/product concentration
- EWRA trigger response time

Escalation rule	A critical exposure, unreliable material dataset, residual risk above appetite or control failure affecting sanctions or reporting shall be escalated immediately to the MLRO, Chief Risk Officer and governing body committee with interim restrictions.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 5: Customer acceptance, prohibited relationships and risk ownership

Legal / framework basis	Law No. 20 of 2019; Implementing Regulations; FATF Recommendations 10, 13 and 19

Objective	Ensure that no relationship or occasional transaction begins before required due diligence, risk classification, screening and approval are complete, and define exposures the entity will not accept.

Policy statement

The entity shall operate a documented customer acceptance framework aligned with its licence and risk appetite. Required CDD, beneficial ownership identification, sanctions and PEP screening, expected-activity profile, risk rating and approvals shall be completed before activation unless the applicable framework expressly permits a controlled exception. Prohibited relationships shall not be opened or continued.

Detailed requirements

5.1 Acceptance criteria and ownership

Acceptance criteria shall distinguish customers, beneficial owners, controllers, authorised persons, connected parties and transaction beneficiaries. The business sponsor remains responsible for the commercial purpose, completeness and plausibility of the relationship and may not delegate that responsibility to Compliance.

The acceptance file shall identify the requested products, expected values and volumes, funding sources, counterparties, jurisdictions, delivery channel and reason for the relationship. The profile shall be sufficiently specific to establish what normal activity should look like for later monitoring.

5.2 Prohibited or restricted exposure

The prohibited list shall include designated persons and entities, shell banks and relationships that permit shell-bank use, customers refusing required identification or beneficial ownership, false or materially inconsistent information and any activity prohibited by law, licence or binding supervisory instruction.

The entity may designate additional restricted or prohibited exposure through risk appetite, such as certain anonymous products, unverified virtual-asset exposure, unacceptable high-risk jurisdictions or structures without legitimate purpose. Internal restrictions shall identify the rationale, authority and review cycle and must not be presented as a statutory prohibition unless verified.

5.3 Conditional and high-risk approval

Higher-risk relationships require EDD, a documented rationale and approval at the seniority defined by law and policy. Conditions may include product limits, first payment from a verified account, additional documents, more frequent review or enhanced monitoring; every condition shall have an owner and evidence of activation.

An approval remains invalid if a mandatory condition is incomplete. The system shall prevent activation or use of restricted products until the condition is satisfied, and any manual override shall be exceptional, time-bound and independently reviewed.

5.4 Refusal, exit and tipping-off

Where CDD cannot be completed, the relationship or transaction shall not proceed and consideration shall be given to an STR in accordance with the applicable standard. Refusal and exit decisions shall be

coordinated with Legal and the MLRO where suspicion, a freeze, law-enforcement contact or customer rights could be affected.

Communications shall use neutral, approved wording and shall never disclose that an STR has been or may be filed. The operational reason provided to the customer shall be accurate, lawful and limited to what may be disclosed.

Defined controls

ONB-01 - Pre-activation completion gate

Control owner	Onboarding Operations
Trigger / frequency	Before activation or execution of an occasional transaction
How performed	Systematically verify required CDD, screening, risk rating, approvals and conditions; block incomplete files.
Required evidence	Workflow record and activation checklist
Classification	Preventive / Automated

ONB-02 - High-risk acceptance approval

Control owner	Senior Management and MLRO
Trigger / frequency	Before accepting or continuing a high-risk relationship
How performed	Review the complete EDD file, risks, SoW/SoF, conditions and monitoring plan.
Required evidence	Signed high-risk approval
Classification	Preventive / Manual

ONB-03 - Prohibited-party and product rule

Control owner	Compliance and Technology
Trigger / frequency	At onboarding and whenever rules or lists change
How performed	Maintain system rules that prevent prohibited relationships and products and log attempted overrides.
Required evidence	Rule configuration and override log
Classification	Preventive / Automated

ONB-04 - Post-onboarding quality review

Control owner	KYC Quality Assurance
Trigger / frequency	Risk-based sample after activation
How performed	Reperform key identity, beneficial ownership, risk-rating, screening and approval checks.
Required evidence	QA workpaper and defect log
Classification	Detective / Manual

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Records and evidence

- Acceptance standard
- CDD file
- Screening results
- Risk assessment
- Approval record
- Condition tracker
- Refusal/exit record
- QA results

Management information and effectiveness indicators

- Pre-activation exception rate
- High-risk approval turnaround
- Incomplete-file defect rate
- Manual override volume
- Conditions overdue
- Refusal and exit ageing

Escalation rule	A potential sanctions match, refusal to disclose beneficial ownership, materially false information, unexplained high-risk structure or pressure to bypass the activation gate shall be escalated immediately to the MLRO and relevant control owner.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 6: Customer identification, verification and ongoing CDD

Legal / framework basis	Law No. 20 of 2019; Implementing Regulations; FATF Recommendations 10 and 11

Objective	Establish who the customer and authorised representatives are, verify identity from reliable independent sources, understand the relationship and maintain current information throughout its life.

Policy statement

No customer or representative shall be treated as identified merely because information was collected. Identity shall be verified using reliable, independent documents, data or information; the purpose and intended nature of the relationship shall be understood; an expected-activity profile shall be established; and ongoing due diligence shall keep the file accurate and transactions consistent with the entity's knowledge.

Detailed requirements

6.1 Natural persons and representatives

For a natural person, the file shall record the legal name, date and place of birth, nationality, identification number and validity, residential address and any other information required by the applicable sector rules. Verification shall use a valid reliable source and record the document or data source, date, reviewer and result.

A representative or authorised signatory shall be identified and verified to the same appropriate standard, and the authority to act shall be confirmed from an authentic mandate, corporate resolution, power of attorney or other valid evidence. The entity shall assess whether the authority is plausible and remains in force.

6.2 Legal persons and legal arrangements

The file shall establish legal existence, form, registration, registered and operating address, governing documents, business purpose, licence where applicable, directors or equivalent controllers, authorised persons and ownership and control structure. Registry information shall be corroborated with reliable documents or official data.

For a trust or similar arrangement, the entity shall identify the settlor, trustee, protector where relevant, beneficiaries or class of beneficiaries and any other person exercising ultimate control. The legal and practical powers of each party shall be understood, not merely listed.

6.3 Purpose and expected activity

The business rationale shall explain why the customer needs the relationship and selected products, the expected source and destination of funds, anticipated values and volumes, counterparties, jurisdictions, frequency, channels and cash use. Generic statements such as 'business purposes' are insufficient where they do not create a monitorable baseline.

The first line shall compare the stated profile with occupation, business model, financial capacity, ownership, public information and requested products. Material inconsistency shall be resolved with evidence before approval or escalated for EDD and possible suspicion review.

6.4 Ongoing maintenance and trigger review

CDD shall be refreshed according to the customer risk tier and on trigger, including ownership or control change, expired identification, new product, new jurisdiction, adverse media, PEP status, unusual activity, material change in expected behaviour, legal change or a request from a competent authority.

A review shall not be closed by changing the review date alone. The reviewer shall compare current data with prior data, resolve inconsistencies, reperform required screening and risk rating, document changes and confirm that monitoring scenarios remain appropriate.

Defined controls

CDD-01 - Independent identity verification

Control owner	KYC Operations
Trigger / frequency	At onboarding and when identity evidence changes or expires
How performed	Verify required data against approved reliable sources and capture the source, date, result and reviewer.
Required evidence	Verification record and source evidence
Classification	Preventive / Semi-automated

CDD-02 - Authority-to-act validation

Control owner	KYC Operations and Legal where required
Trigger / frequency	Before granting access or accepting instructions
How performed	Validate the representative's identity, mandate, scope, expiry and revocation status.
Required evidence	Mandate and validation checklist
Classification	Preventive / Manual

CDD-03 - Expected-activity reasonableness review

Control owner	Business Owner
Trigger / frequency	Before acceptance and at material profile change
How performed	Compare the proposed profile with customer capacity, purpose, products, counterparties and jurisdictions and resolve inconsistencies.
Required evidence	Business rationale and supporting evidence
Classification	Preventive / Manual

CDD-04 - CDD ageing and trigger control

Control owner	KYC Management
Trigger / frequency	Daily system monitoring and periodic review
How performed	Identify due, overdue and trigger-affected files; restrict activity or escalate according to approved rules.
Required evidence	Ageing dashboard and restriction log
Classification	Preventive / Automated

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Records and evidence

- Identity evidence
- Verification records
- Authority documents
- Purpose and expected-activity profile
- Review record
- Trigger log
- Restriction record

Management information and effectiveness indicators

- Identity-verification exception rate
- Expired-document population
- CDD reviews overdue by risk tier
- Trigger-review completion time
- Files without quantified expected activity

Escalation rule	Identity doubt, suspected forgery, unexplained representative authority, material profile inconsistency or inability to complete CDD shall stop activation or the affected transaction and be escalated to the MLRO for risk and suspicion assessment.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 7: Beneficial ownership and control transparency

Legal / framework basis	Law No. 20 of 2019; applicable beneficial-ownership legislation and sector rules; FATF Recommendations 24 and 25

Objective	Identify and reasonably verify the natural persons who ultimately own or control customers and prevent legal entities or arrangements from obscuring accountability.

Policy statement

The entity shall understand the complete ownership and control structure of each legal person or legal arrangement and identify the natural person or persons who ultimately own or control it under the applicable Qatari criteria. The entity shall not stop at an intermediate corporate layer, nominee, trustee or authorised representative and shall document the reasoning used to determine the beneficial owner.

Detailed requirements

7.1 Ownership and control pathway

The reviewer shall obtain an ownership chart supported by current registers, constitutional documents and reliable registry data. Direct and indirect holdings shall be calculated through each layer, and control through voting, appointment rights, contractual influence or other means shall be considered separately from ownership percentage.

The applicable ownership threshold must be taken from the law or sector rule governing the entity and customer. A commonly used international threshold shall not be substituted for a different Qatari threshold. Where no qualifying owner is identified, the control-by-other-means and senior-managing-official tests shall be applied as legally required.

7.2 Complex structures and nominees

Layered companies, trusts, foundations, nominee shareholders or directors, bearer-like arrangements and multiple jurisdictions require an explanation of legitimate purpose and additional corroboration. Complexity is not automatically prohibited, but unexplained complexity is a risk indicator requiring challenge.

The entity shall distinguish a nominee from the person for whom the nominee acts and identify the underlying natural person. Professional intermediaries shall provide evidence of authority and underlying ownership; confidentiality claims do not override applicable CDD duties.

7.3 Verification and discrepancy handling

Verification shall be proportionate to risk and use reliable independent data. The file shall show which ownership and control assertions were verified, the source used, limitations and the reviewer conclusion. Self-declaration alone is insufficient where independent corroboration is reasonably available or risk is elevated.

Discrepancies between customer declarations, company registers, licences, public sources and transaction behaviour shall be recorded, investigated and resolved. Material unresolved discrepancies may require refusal, restriction, regulator notification where applicable and consideration of an STR.

7.4 Maintenance and connected parties

Beneficial ownership shall be refreshed on the customer review cycle and immediately upon changes to capital, shareholders, voting rights, directors, trustees, beneficiaries, control agreements, mergers, restructurings or credible adverse information.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Beneficial owners, controllers and relevant connected parties shall be included in sanctions, PEP and adverse-media screening and in the customer risk assessment. A change shall trigger reassessment of EDD, approval, expected activity and monitoring coverage.

Defined controls

BO-01 - Ownership and control reconstruction

Control owner	KYC Analyst
Trigger / frequency	At onboarding and each ownership/control change
How performed	Calculate direct and indirect ownership, identify control rights and document the path to natural persons.
Required evidence	Signed ownership chart and calculation
Classification	Preventive / Manual

BO-02 - Independent beneficial-owner verification

Control owner	KYC Operations
Trigger / frequency	Before activation and on risk-based refresh
How performed	Corroborate identity and ownership/control through approved registry data and supporting documents.
Required evidence	Verification evidence and conclusion
Classification	Preventive / Manual

BO-03 - Complex-structure challenge

Control owner	MLRO / EDD Team
Trigger / frequency	When complexity, nominee arrangements or high-risk jurisdictions are present
How performed	Assess legitimate purpose, intermediaries, control, tax/legal rationale and source of wealth; approve or reject with conditions.
Required evidence	EDD memorandum and approval
Classification	Preventive / Manual

BO-04 - Ownership-change surveillance

Control owner	Customer Management and Company Secretarial Data Owner
Trigger / frequency	Continuous notification and periodic comparison
How performed	Detect changes from customer notifications, registry data and internal events and route them for review.
Required evidence	Change alert and completed review
Classification	Detective / Semi-automated

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Records and evidence

- Ownership chart
- Registers and constitutional documents
- Ownership calculation
- Control analysis
- Beneficial-owner declarations
- Verification evidence
- Discrepancy log

Management information and effectiveness indicators

- Files without verified BO
- Average ownership layers
- Unresolved discrepancy ageing
- Nominee-structure population
- Ownership-change review timeliness

Escalation rule	Refusal to disclose ownership, suspected nominee concealment, an unresolved material discrepancy or a designated/PEP beneficial owner shall be escalated to the MLRO before activation or continuation.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 8: Customer risk rating, simplified measures and enhanced due diligence

Legal / framework basis	Law No. 20 of 2019; Implementing Regulations; FATF Recommendations 1, 10, 12 and 19
Objective	Operate a transparent customer risk-rating model that changes due-diligence intensity, approval, monitoring and review frequency in proportion to risk.

Policy statement

Every customer shall be assigned a documented risk rating using approved customer, product/service/transaction, delivery-channel and geographic factors. The model shall include mandatory overrides and prohibited outcomes. Higher risk shall trigger EDD, senior approval, enhanced monitoring and shorter review cycles; simplified measures may be used only when lower risk is evidenced and legally permitted.

Detailed requirements

8.1 Model design and governance

The methodology shall define each factor, input source, score, weight, threshold, override, prohibited criterion and treatment. It shall be calibrated to the entity's EWRA and actual portfolio; copying generic weights without evidence is not an acceptable design basis.

Changes to weights, thresholds, data sources or treatment mappings require documented impact analysis, validation, approval and controlled implementation. Model limitations and manual judgement shall be visible in management information.

8.2 Mandatory overrides and quality

Overrides shall address conditions that cannot be averaged away, including a true sanctions prohibition, foreign PEP status, unacceptable jurisdiction, inability to identify beneficial ownership, shell-bank exposure or another statutory or appetite-based condition. The file shall show whether the override changes the rating, treatment or acceptance decision.

Automated inputs shall be reconciled to source systems and manual inputs shall be evidenced. A reviewer shall not reduce a rating merely to avoid EDD or a shorter review; downward overrides require defined authority, objective rationale and independent review.

8.3 Simplified due diligence

SDD may reduce the extent or timing of specified measures only where lower risk is demonstrated, the applicable framework permits it and no suspicion or higher-risk factor exists. Customer identification, beneficial ownership and sanctions obligations are not eliminated.

The SDD rationale shall identify the evidence of lower risk, measures simplified, residual controls, approval and review trigger. The population shall be monitored to confirm that actual behaviour remains consistent with the lower-risk premise.

8.4 Enhanced due diligence

EDD shall obtain additional information and verification proportionate to the risk, establish and corroborate source of wealth and source of funds where required, secure senior approval, understand transaction purpose in greater depth and apply enhanced ongoing monitoring.

The EDD plan shall identify the risk, measure, owner, evidence, due date, approval and treatment. EDD is not complete because a generic checklist is signed; the additional information must address the specific risk that caused EDD.

Defined controls

CRR-01 - Customer risk-rating calculation

Control owner	KYC Risk Engine / Analyst
Trigger / frequency	At onboarding, periodic review and trigger
How performed	Calculate the approved factor scores and overrides from controlled data and retain the inputs and output.
Required evidence	Risk-rating record
Classification	Preventive / Automated

CRR-02 - Risk-model validation

Control owner	Independent Model Validation / Compliance QA
Trigger / frequency	Before implementation and periodically
How performed	Test conceptual soundness, data quality, discriminatory power, overrides, treatment mapping and change impact.
Required evidence	Validation report
Classification	Detective / Manual

CRR-03 - EDD completion and approval gate

Control owner	EDD Team and Senior Management
Trigger / frequency	Before accepting or continuing a high-risk relationship
How performed	Confirm that each risk-specific EDD measure is complete and approved before activation or continuation.
Required evidence	EDD checklist, evidence and approval
Classification	Preventive / Manual

CRR-04 - SDD population review

Control owner	Compliance Monitoring
Trigger / frequency	Periodic risk-based review
How performed	Sample lower-risk files and activity to confirm eligibility, minimum CDD and continued consistency with the premise.
Required evidence	SDD monitoring report
Classification	Detective / Manual

Records and evidence

- CRR methodology

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Factor data
- Rating and override record
- Validation report
- EDD plan
- SDD rationale
- Approvals
- Treatment configuration

Management information and effectiveness indicators

- Customer distribution by tier
- Manual override rate
- Downward-override defects
- High-risk files without current EDD
- SDD eligibility failures
- Rating changes after trigger

Escalation rule	A prohibited outcome, material data defect, unexplained downward override or high-risk relationship without complete EDD shall be restricted and escalated to the MLRO and accountable business executive.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 9: Politically exposed persons and source of wealth/funds

Legal / framework basis	Law No. 20 of 2019; Implementing Regulations; FATF Recommendation 12
Objective	Identify PEP exposure, apply proportionate enhanced measures and distinguish and corroborate source of wealth from source of funds.

Policy statement

The entity shall maintain risk-based controls to identify foreign, domestic and international-organisation PEPs, relevant family members and close associates. PEP status shall not automatically cause rejection, but the applicable enhanced measures, senior approval, SoW/SoF work and enhanced monitoring shall be completed. The entity shall distinguish the origin of a specific transaction from the manner in which overall wealth was accumulated.

Detailed requirements

9.1 Identification and classification

Screening shall use reliable data and consider name variants, nationality, date of birth, position, period in office, family members and close associates. Potential matches shall be adjudicated with identifiers; a list label alone does not replace a reasoned classification.

The file shall state the PEP category, role, jurisdiction, period, associated persons, risk drivers and basis for treatment. Former PEP status shall be managed according to continuing risk rather than an unsupported automatic expiry date.

9.2 Approval and enhanced measures

Before establishing or continuing the relevant relationship, the entity shall obtain the senior management approval required by the applicable framework and assess corruption exposure, public function, jurisdiction, products, counterparties, ownership, adverse information and expected activity.

Enhanced monitoring shall be tailored to the risk and may include shorter review intervals, lower or additional monitoring thresholds, closer review of public-sector counterparties, payments through intermediaries and significant changes in wealth or transaction pattern.

9.3 Source of wealth

SoW explains how overall net worth was accumulated, such as business ownership, career income, inheritance, investments or asset sales. The explanation shall be plausible relative to age, profession, public role, ownership and available financial information and shall be corroborated according to risk.

Evidence may include audited financial statements, reliable company ownership information, tax or income records where lawfully available, probate documents, sale agreements, investment statements or other independent information. Unverifiable self-declaration is not sufficient for a materially high-risk relationship.

9.4 Source of funds and ongoing review

SoF identifies the origin of the specific money entering the relationship or funding a transaction. Bank statements, sale contracts, dividend vouchers, salary records, loan agreements and remitter information shall be assessed for consistency with the transaction and customer profile.

Material changes in role, wealth, ownership, public exposure, adverse information or transaction pattern shall trigger reassessment, refreshed evidence, screening and senior approval where required. The review shall consider whether unexplained wealth or flows create suspicion.

Defined controls

PEP-01 - PEP screening and adjudication

Control owner	Screening Operations
Trigger / frequency	At onboarding, list/data update, transaction where relevant and periodic rescreening
How performed	Screen names and connected parties, compare identifiers and document false-positive or confirmed classification.
Required evidence	Screening alert and adjudication
Classification	Preventive / Semi-automated

PEP-02 - PEP risk assessment and approval

Control owner	MLRO and Senior Management
Trigger / frequency	Before acceptance/continuation and on material trigger
How performed	Assess category, corruption exposure, SoW/SoF, products, geography, connected parties and monitoring plan.
Required evidence	PEP memorandum and approval
Classification	Preventive / Manual

PEP-03 - SoW/SoF corroboration

Control owner	EDD Analyst
Trigger / frequency	At high-risk onboarding and significant funding or trigger
How performed	Obtain independent evidence, compare with known profile and record plausibility and limitations.
Required evidence	Source evidence and analyst conclusion
Classification	Preventive / Manual

PEP-04 - Enhanced PEP monitoring

Control owner	Transaction Monitoring
Trigger / frequency	Ongoing according to approved plan
How performed	Apply designated scenarios and periodic review and escalate deviations from the approved profile.
Required evidence	PEP monitoring report
Classification	Detective / Automated

Records and evidence

- PEP screening results
- PEP classification
- Approval

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- SoW evidence
- SoF evidence
- Enhanced monitoring plan
- Periodic review
- Adverse-media assessment

Management information and effectiveness indicators

- PEP population by category
- PEP files without current approval
- SoW/SoF evidence defects
- PEP trigger-review timeliness
- Enhanced-monitoring exceptions

Escalation rule	A confirmed PEP, credible corruption allegation, unexplained wealth, funding inconsistent with the profile or an attempt to bypass senior approval shall be escalated promptly to the MLRO for risk and suspicion assessment.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 10: Sanctions, targeted financial sanctions and proliferation financing

Legal / framework basis	Law No. 20 of 2019; Law No. 27 of 2019; Public Prosecutor Decisions No. 1 and 59 of 2020; FATF Recommendations 6 and 7

Objective	Screen relevant parties and transactions, distinguish potential from true matches, freeze without delay when legally required and manage PF risk separately from ordinary suspicion.

Policy statement

The entity shall maintain a documented TFS programme covering list governance, customer and transaction screening, beneficial owners and connected parties, match adjudication, freezing and prohibition without delay, reporting, confidentiality, release and record retention. A sanctions match and an STR are separate legal pathways; either or both may be triggered by the same facts.

Detailed requirements

10.1 List governance and population

The programme shall identify the UN and national lists that always apply and any additional lists required by currency, correspondent, contractual or geographic exposure. The source, update method, update time, version, quality checks, re-screening population and exception handling shall be documented.

Screening shall cover customers, beneficial owners, controllers, representatives, relevant counterparties and payment-message parties as required by the entity's activity. Ownership and control by designated persons shall be assessed and shall not be limited to an exact-name match.

10.2 Name and transaction screening

Configuration shall address Arabic and Latin transliteration, aliases, word order, dates of birth, nationality, identification numbers and other identifiers. Thresholds shall be risk-based, validated and tuned; a vendor default is not evidence of effectiveness.

Relevant transactions shall be screened before execution where required, with particular attention to cross-border parties, intermediary institutions, vessels, ports and trade information as applicable. System outages shall activate an approved contingency that prevents uncontrolled release.

10.3 Adjudication, freezing and reporting

Analysts shall distinguish a false positive from a potential or true match using sufficient identifiers and record the reasoning. Bulk closure without individual or validated rule-based evidence is prohibited. A potential match shall be escalated and affected activity held according to approved legal procedures.

When a true match triggers the applicable obligation, funds and economic resources shall be frozen and services prohibited without delay and without prior notice, and the required report or notification shall be made through the current competent channel. Release or access requires valid authority and documented verification.

10.4 PF risk and effectiveness testing

PF risk assessment shall consider designated ownership, front companies, dual-use goods, end users, shipping anomalies, trans-shipment, DPRK or Iran nexus, trade-document inconsistencies and complex payments. Screening is a key control but does not replace transaction and trade analysis.

Effectiveness testing shall include alert quality, timeliness, list-update-to-screen time, true-match simulations, false-negative or below-the-line testing, transliteration testing, ownership scenarios, outage response and independent review of discounted alerts.

Defined controls

TFS-01 - Authoritative list update and rescreen

Control owner	Sanctions Compliance and Technology
Trigger / frequency	Upon each list change
How performed	Load and validate the update, record timing, re-screen the defined population and investigate processing exceptions.
Required evidence	List log, validation and rescreen report
Classification	Preventive / Automated

TFS-02 - Pre-execution transaction screening

Control owner	Payments / Operations
Trigger / frequency	For each in-scope transaction
How performed	Screen required message fields and prevent release until alerts are resolved or legally authorised.
Required evidence	Screening decision and release log
Classification	Preventive / Automated

TFS-03 - Independent match adjudication

Control owner	Sanctions Analyst and Senior Reviewer
Trigger / frequency	For every potential match
How performed	Compare names and secondary identifiers, ownership/control and context; document discount or escalation with review.
Required evidence	Restricted adjudication record
Classification	Preventive / Manual

TFS-04 - Freeze-and-report response

Control owner	MLRO / Sanctions Officer
Trigger / frequency	Immediately upon confirmed legal trigger
How performed	Apply system and operational freeze, prohibit availability, notify the competent authority and protect confidentiality.
Required evidence	Freeze record, report receipt and access log
Classification	Preventive / Manual

TFS-05 - Screening effectiveness test

Control owner	Compliance QA / Independent Assurance

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Trigger / frequency	Periodic and after material change
How performed	Run scenario, transliteration, ownership, below-the-line and outage tests and track remediation.
Required evidence	Effectiveness test report
Classification	Detective / Manual

Records and evidence

- List inventory
- Update logs
- Screening configuration
- Alerts and adjudications
- Freeze records
- Competent-authority reports
- Release authority
- Effectiveness tests

Management information and effectiveness indicators

- List-update latency
- Unscreened population
- Alert ageing
- Discount QA error rate
- Freeze execution time
- Screening system availability
- Below-the-line miss rate

Escalation rule	A potential or true match, screening outage, missed population, delayed freeze or unauthorised release shall be escalated immediately to the MLRO, Sanctions Officer, Legal, Operations and the appropriate senior authority under the incident procedure.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 11: Transaction monitoring, alert investigation and typologies

Legal / framework basis	Law No. 20 of 2019; Implementing Regulations; FATF Recommendations 10 and 20

Objective	Detect activity inconsistent with the customer's known profile and relevant typologies, investigate alerts consistently and demonstrate monitoring coverage and effectiveness.

Policy statement

The entity shall monitor relevant transactions and behaviour throughout the relationship using risk-based automated and manual controls appropriate to its products, customers, channels and data. Monitoring shall compare actual activity with the expected profile, map scenarios to the EWRA and current typologies, produce traceable cases and support a timely suspicion decision.

Detailed requirements

11.1 Coverage and scenario inventory

The scenario inventory shall map each material EWRA risk to one or more preventive or detective controls and identify products, systems, customer segments, data fields and known limitations. Risks without monitoring coverage require an approved compensating control and remediation plan.

Scenario families shall be selected for the actual business and may include structuring, rapid movement, pass-through activity, unusual cash, unexpected cross-border flows, dormant-to-active behaviour, third-party funding, funnel patterns, trade anomalies, TF collection/disbursement and PF or sanctions-evasion indicators.

11.2 Data and segmentation

Monitoring inputs shall be complete, timely and reconciled from source systems, including customer identity and risk, beneficial owners, accounts or contracts, transactions, counterparties, geography, products, channel and expected activity. Critical data lineage and transformation shall be documented.

Thresholds and rules shall be segmented according to risk and customer behaviour. A single threshold applied to all customers is unlikely to be effective; higher-risk customers require tighter or additional scenarios and lower-risk segments still require coverage for suspicion independent of value.

11.3 Alert investigation and disposition

The analyst shall reconstruct relevant activity, compare it with the expected profile, review connected accounts or parties where lawful, identify the likely typology, seek a legitimate explanation and document both supporting and contradictory evidence. The record shall allow an independent reviewer to understand the conclusion without redoing undocumented work.

A closure shall explain why activity is reasonable and consistent, not merely state 'no suspicion'. If suspicion may exist, the case shall be escalated promptly through the internal reporting process; the analyst shall not contact the customer in a manner that could tip off.

11.4 Tuning, quality assurance and learning

Thresholds and logic shall be tuned using alert volumes, productivity, risk coverage, case outcomes and data quality, but alert reduction alone is not an objective. Below-the-line testing shall sample activity that did not alert to identify false negatives and confirm scenario sensitivity.

Quality assurance shall reperform a risk-based sample of closures and escalations and assess completeness, timeliness, typology logic and evidence. Findings, STR themes, regulator feedback and emerging typologies shall feed back into the EWRA, CDD baseline, scenario library and training.

Defined controls

TM-01 - Monitoring population reconciliation

Control owner	Monitoring Data Owner
Trigger / frequency	Each processing cycle
How performed	Reconcile expected accounts/contracts and transactions to those ingested and hold or investigate exceptions.
Required evidence	Population reconciliation and exception log
Classification	Detective / Automated

TM-02 - Risk-segmented scenario execution

Control owner	Transaction Monitoring
Trigger / frequency	Daily or other approved frequency
How performed	Run approved scenarios using current risk, profile and transaction data and generate traceable alerts.
Required evidence	Scenario run and alert log
Classification	Detective / Automated

TM-03 - Alert investigation and review

Control owner	Monitoring Analyst and Senior Reviewer
Trigger / frequency	For every alert
How performed	Compare with baseline, reconstruct activity, assess typology and record evidence and reasoned disposition.
Required evidence	Case file and review approval
Classification	Preventive / Manual

TM-04 - Below-the-line and tuning review

Control owner	Monitoring Governance / Compliance QA
Trigger / frequency	Periodic and after material change
How performed	Test non-alerted activity, analyse outcomes, approve tuning and confirm no material risk was removed.
Required evidence	Tuning paper and effectiveness test
Classification	Detective / Manual

Records and evidence

- Scenario inventory
- Risk-to-scenario map

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Data lineage
- Reconciliations
- Alerts
- Case files
- Tuning approvals
- QA results
- Typology updates

Management information and effectiveness indicators

- Unmonitored population
- Alert ageing
- Escalation rate
- Closure QA error rate
- Below-the-line miss rate
- Scenario productivity
- Data exceptions

Escalation rule	A missed material population, evidence of a false negative, alert backlog above tolerance, unexplained activity or potential sanctions nexus shall be escalated promptly to the MLRO and the relevant data, technology and operations owners.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 12: Internal suspicion reporting, STR decisions and tipping-off

Legal / framework basis	Law No. 20 of 2019; Implementing Regulations; FATF Recommendations 20 and 21

Objective	Provide a confidential, timely and defensible pathway from employee concern to independent MLRO decision and external reporting to the QFIU.

Policy statement

All personnel shall report facts giving rise to suspicion or reasonable grounds to suspect through the confidential internal channel without delay. The MLRO shall independently evaluate the full information, document the decision to report or not report and, where the reporting standard is met, file through the current QFIU channel and form. Tipping-off and unnecessary disclosure are prohibited.

Detailed requirements

12.1 Internal disclosure standard

Training and procedures shall explain that suspicion is more than unease and less than proof and may arise from a transaction, attempted transaction, pattern, relationship, ownership, behaviour or information. No monetary threshold limits the duty to raise a concern.

The internal report shall capture the subject, relationship, relevant dates and amounts, counterparties, jurisdictions, activity, deviation from expected behaviour, typology and available evidence. The reporter need not prove a predicate offence and shall not investigate beyond authorised access.

12.2 MLRO evaluation and decision

The MLRO shall consider CDD, beneficial ownership, history, expected activity, alerts, screening, related parties, open-source information and any lawful business explanation. The analysis shall distinguish verified fact, inference and unresolved limitation and shall evaluate the suspicion threshold, not the prospect of conviction.

Both report and no-report decisions shall be reasoned, dated and access-restricted. Commercial value, customer status or fear of inconvenience shall not influence the decision. Any request for additional information shall avoid tipping-off and unnecessary delay.

12.3 External filing and follow-up

When suspicion remains, the MLRO shall submit the STR to the QFIU using the prescribed channel, form and timeline current for the entity. The narrative shall state who, what, when, where, how, why suspicious, the amounts and the supporting evidence in a factual chronology.

The file shall retain filing confirmation, supporting documents, information requests, supplementary reports and decisions regarding continuation, restriction or exit. Filing does not automatically require account closure; subsequent actions shall comply with law and avoid tipping-off.

12.4 Confidentiality and information barriers

Knowledge of an internal report or STR shall be limited to persons with a lawful need to know. Access roles, logging, secure storage, controlled exports and communication protocols shall prevent accidental or deliberate disclosure.

Customer communications, delayed or declined transactions, information requests and exit letters shall use approved neutral wording. Suspected tipping-off, improper access or unauthorised disclosure is a serious incident requiring immediate containment and legal escalation.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Defined controls

STR-01 - Confidential internal reporting channel

Control owner	MLRO Office
Trigger / frequency	Continuous availability
How performed	Provide an accessible, secure route with receipt confirmation, restricted access and contingency arrangements.
Required evidence	Internal disclosure and receipt log
Classification	Preventive / Semi-automated

STR-02 - Independent MLRO decision

Control owner	MLRO
Trigger / frequency	For every internal report
How performed	Assess the complete record against the suspicion standard and document report/no-report reasoning without commercial veto.
Required evidence	Restricted decision memorandum
Classification	Preventive / Manual

STR-03 - External filing quality gate

Control owner	MLRO / Authorised Deputy
Trigger / frequency	Before submission
How performed	Validate subjects, chronology, amounts, typology, deviation, evidence, attachments and current QFIU submission requirements.
Required evidence	Filed STR and submission receipt
Classification	Preventive / Manual

STR-04 - Need-to-know access monitoring

Control owner	Information Security and MLRO
Trigger / frequency	Continuous logging and periodic review
How performed	Restrict and review access to internal reports, STRs and related investigations; investigate anomalies.
Required evidence	Access log and review report
Classification	Detective / Automated

Records and evidence

- Internal reports
- MLRO analyses

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Report/no-report decisions
- STRs and receipts
- QFIU correspondence
- Supplementary reports
- Access logs
- Tipping-off incidents

Management information and effectiveness indicators

- Internal-report-to-MLRO time
- Decision ageing
- Filing timeliness
- Narrative QA defects
- Supplementary-report timeliness
- Unauthorised-access alerts

Escalation rule	Any internal disclosure, risk of tipping-off, attempted interference, missed filing requirement or suspected unauthorised access shall be escalated immediately to the MLRO and Legal through the protected route.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 13: Payments, correspondent relationships and reliance on third parties

Legal / framework basis	Applicable sector rules; FATF Recommendations 13, 16 and 17

Objective	Control higher-risk payment chains, correspondent relationships, originator/beneficiary information and permitted reliance without transferring accountability.

Policy statement

This chapter applies only to the extent relevant to the entity's licence and products. Where applicable, the entity shall conduct enhanced due diligence on correspondent relationships, prevent shell-bank exposure, maintain required payment information and controls, and ensure that reliance on a third party does not transfer ultimate responsibility for CDD.

Detailed requirements

13.1 Applicability and payment transparency

The entity shall map payment types, message formats, intermediaries, clearing currencies and obligations for originator and beneficiary information. Missing, incomplete or inconsistent information shall trigger defined rejection, hold, repair or risk-based review rules before processing.

Data transformations across channels and systems shall preserve legally required information. Operations and Technology shall test truncation, character conversion, field mapping and exception queues, including non-Latin names and intermediary-bank information.

13.2 Correspondent due diligence

Before a cross-border correspondent relationship, the entity shall understand the respondent's ownership, business, licence, management, reputation, supervision, customer base, products, geography and AML/CFT controls and obtain senior management approval. The respective responsibilities shall be documented.

The entity shall prohibit shell banks and respondents that permit their accounts to be used by shell banks. Payable-through arrangements require confirmation that the respondent conducts appropriate CDD on customers with direct access and can provide relevant information on request.

13.3 Reliance on third parties

Reliance shall be distinguished from outsourcing and introductions. Before permitted reliance, the entity shall assess the third party's regulation, supervision, CDD standard, record retention, geographic risk and ability to provide underlying documents without delay.

The relying entity retains ultimate responsibility and shall obtain core CDD information immediately and underlying evidence promptly on request. Reliance shall be suspended if quality, access or regulatory conditions fail.

13.4 Ongoing monitoring and termination

Correspondent and reliance arrangements shall be reviewed on a risk-based cycle and on trigger, including enforcement, ownership or licence change, poor information response, sanctions exposure, adverse media, unexplained payment patterns or audit findings.

Material deficiencies shall result in remediation, restriction, enhanced monitoring, suspension or exit according to severity. Exit planning shall preserve reporting, freezing, record-retention and confidentiality obligations.

Defined controls

PAY-01 - Payment information completeness gate

Control owner	Payment Operations
Trigger / frequency	For each in-scope payment
How performed	Validate required originator, beneficiary and intermediary information and apply hold/reject/repair rules.
Required evidence	Message-validation and exception log
Classification	Preventive / Automated

PAY-02 - Correspondent acceptance due diligence

Control owner	Correspondent Banking and MLRO
Trigger / frequency	Before approval and on periodic/trigger review
How performed	Complete risk assessment, control questionnaire, reputation and supervision checks, responsibilities and senior approval.
Required evidence	Correspondent file and approval
Classification	Preventive / Manual

PAY-03 - Shell-bank prohibition

Control owner	Correspondent Banking and Sanctions Compliance
Trigger / frequency	At onboarding and periodic/trigger review
How performed	Verify physical presence and supervision and obtain confirmation that the respondent does not permit shell-bank use.
Required evidence	Verification and contractual representation
Classification	Preventive / Manual

PAY-04 - Reliance performance test

Control owner	KYC Quality Assurance
Trigger / frequency	Periodic risk-based sample
How performed	Request underlying CDD evidence, test timeliness and quality and suspend reliance when criteria fail.
Required evidence	Reliance test and remediation log
Classification	Detective / Manual

Records and evidence

- Payment data map
- Message exceptions

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Correspondent due-diligence files
- Questionnaires
- Approvals
- Reliance agreements
- Document requests
- Review and exit records

Management information and effectiveness indicators

- Payments with missing information
- Repair and rejection rate
- Correspondent reviews overdue
- Reliance document-response time
- Shell-bank attestations overdue
- High-risk payment alerts

Escalation rule	Missing payment data, suspected shell-bank exposure, refusal to provide underlying CDD, material correspondent-control weakness or sanctions concern shall be escalated immediately to the MLRO and relevant operations owner.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 14: New products, technology, digital channels and outsourcing

Legal / framework basis	Law No. 20 of 2019; applicable sector rules; FATF Recommendations 15, 17 and 18

Objective	Assess ML/TF/PF risk before launch or material change and maintain accountability for technology and outsourced controls.

Policy statement

No new or materially changed product, service, channel, technology, market, outsourcing arrangement or virtual-asset exposure shall be launched before documented AML/CFT/CPF risk assessment, control design, data and system testing, approval and readiness evidence are complete. Outsourcing does not transfer accountability.

Detailed requirements

14.1 Change identification and risk assessment

The product-governance process shall define what constitutes a new or material change and require early involvement of Compliance, MLRO, Legal, Risk, Technology, Information Security, Data, Operations and Internal Audit as an observer where appropriate.

The assessment shall cover target customers, anonymity, speed, value movement, cash or third-party funding, non-face-to-face identity, cross-border reach, agents, merchants, virtual assets, sanctions screening, monitoring, record reconstruction, data lineage and exit capability.

14.2 Control requirements and testing

The design shall specify CDD and risk-rating changes, screening points, monitoring scenarios, transaction limits, exceptions, approvals, access, audit trails, data retention, management information, training and contingency. Each control shall identify owner, frequency, evidence and acceptance criteria.

Testing shall include positive and negative scenarios, higher-risk cases, list updates, system failure, data reconciliation, manual fallback, override and reporting. Critical defects shall prevent launch; unresolved lower defects require explicit risk acceptance and a time-bound plan.

14.3 Outsourcing and service providers

Due diligence shall assess ownership, competence, regulatory status, financial resilience, information security, data location, subcontractors, business continuity, sanctions exposure, access to records, audit rights and termination support. The contract shall reflect measurable control and incident obligations.

The entity shall monitor service levels and control outcomes, not only contractual delivery. It shall retain the ability to obtain records promptly, test the service, direct remediation and continue critical AML processes during outage or termination.

14.4 Post-launch and model governance

A post-implementation review shall compare actual customers, volumes, alerts, losses, exceptions and data quality with the approved assumptions. Unexpected exposure shall trigger recalibration, restrictions or suspension.

Rules, models and algorithms affecting identity, risk rating, screening or monitoring shall have documented ownership, versions, change control, validation, explainability proportionate to impact, access restrictions and performance monitoring.

Defined controls

NPT-01 - AML risk assessment before launch

Control owner	Product Owner and MLRO
Trigger / frequency	At concept stage and before material change
How performed	Assess exposure and required controls using a documented cross-functional template.
Required evidence	Approved risk assessment
Classification	Preventive / Manual

NPT-02 - Launch readiness and defect gate

Control owner	Change Approval Committee
Trigger / frequency	Before production launch
How performed	Confirm test completion, critical defect closure, data readiness, monitoring, screening, training and contingency.
Required evidence	Readiness checklist and decision
Classification	Preventive / Manual

NPT-03 - Third-party due diligence and contract control

Control owner	Procurement, Legal and Compliance
Trigger / frequency	Before engagement and renewal
How performed	Assess provider risk and include access, audit, incident, data, subcontractor, continuity and exit obligations.
Required evidence	Due-diligence file and contract
Classification	Preventive / Manual

NPT-04 - Post-launch effectiveness review

Control owner	Product Risk and Compliance QA
Trigger / frequency	After an approved live-operation period
How performed	Compare actual exposure and control outcomes with assumptions and approve recalibration or remediation.
Required evidence	Post-launch review
Classification	Detective / Manual

Records and evidence

- Change inventory
- Product risk assessments

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Control requirements
- Test scripts and results
- Approvals
- Provider due diligence
- Contracts
- Post-launch reviews
- Model documentation

Management information and effectiveness indicators

- Changes launched without approval
- Open critical defects
- Post-launch variance
- Provider control breaches
- System outage time
- Model validation overdue

Escalation rule	A proposed launch without required controls, critical test failure, material data gap, sanctions-screening defect or provider denial of records shall stop the launch or affected service and be escalated to the MLRO and accountable executive.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 15: Records, data quality, confidentiality and regulatory access

Legal / framework basis	Law No. 20 of 2019; Implementing Regulations; FATF Recommendation 11; applicable data-protection and sector requirements

Objective	Retain complete and retrievable records for the legally required period, protect sensitive information and demonstrate transaction and decision reconstruction.

Policy statement

The entity shall maintain complete, accurate, secure and promptly retrievable records of CDD, beneficial ownership, transactions, screening, monitoring, internal reports, STR decisions, TFS actions, approvals, training and assurance for the period required by the applicable Qatari framework. The retention schedule shall use the longest applicable requirement and shall distinguish ordinary records from specially restricted STR and sanctions records.

Detailed requirements

15.1 Record inventory and retention schedule

The records inventory shall identify record class, legal basis, start event, minimum period, owner, system or location, format, access role, legal hold, destruction rule and regulator-production method. The entity shall verify the applicable national and sector period rather than assume an international minimum.

Where records are held by a third party, the entity remains responsible for accessibility, integrity and retention. Contracts and tests shall demonstrate that records can be obtained promptly in a usable form throughout and after the service relationship.

15.2 Reconstruction and data quality

Records shall be sufficient to reconstruct an individual transaction, customer decision, alert, sanctions action and STR analysis, including who acted, when, data considered, approval, system result and subsequent changes. Audit trails shall prevent undetected alteration.

Critical data elements shall have definitions, owners, validation rules, lineage and quality monitoring. Exceptions affecting screening, monitoring, risk rating or reporting shall be risk-assessed, corrected and, where appropriate, populations reprocessed.

15.3 Confidentiality and access

Access shall follow least privilege and need to know, with separate roles for restricted investigations, STRs and TFS. Access grants, changes, exports, printing and unusual activity shall be logged and reviewed; terminated or transferred users shall lose access promptly.

Information sharing inside a group, with a service provider or with an authority shall have a lawful basis, defined purpose, secure channel and minimum necessary content. Tipping-off and restrictions on STR disclosure remain controlling considerations.

15.4 Production, legal hold and destruction

A competent-authority request shall be authenticated, logged, interpreted by authorised personnel and fulfilled accurately within the required time. The response shall be quality-checked and transmission confirmed, without alerting the customer where prohibited.

Legal holds suspend ordinary destruction. At the end of the retention period and after hold clearance, destruction shall be authorised, secure and evidenced; system backups, third-party copies and exports shall be included in the disposal design.

Defined controls

REC-01 - Approved records and retention schedule

Control owner	Records Management and Legal
Trigger / frequency	At framework change and periodic review
How performed	Map each record class to legal basis, start event, period, system, access and destruction rule.
Required evidence	Approved schedule
Classification	Preventive / Manual

REC-02 - Record reconstruction test

Control owner	Compliance QA
Trigger / frequency	Periodic risk-based sample
How performed	Reconstruct selected customers, transactions, alerts and decisions from retained evidence and record defects.
Required evidence	Reconstruction workpaper
Classification	Detective / Manual

REC-03 - Restricted-access monitoring

Control owner	Information Security
Trigger / frequency	Continuous logging and periodic review
How performed	Monitor access, exports and role changes for sensitive AML records and investigate anomalies.
Required evidence	Access report and investigations
Classification	Detective / Automated

REC-04 - Authority-request response control

Control owner	MLRO / Legal / Records Owner
Trigger / frequency	For each authenticated request
How performed	Log scope and deadline, retrieve and quality-check the response, approve and transmit securely.
Required evidence	Request log, response copy and receipt
Classification	Preventive / Manual

Records and evidence

- Records inventory
- Retention schedule
- CDD and transaction records
- Audit trails

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Access logs
- Authority requests
- Legal holds
- Destruction certificates

Management information and effectiveness indicators

- Retrieval time
- Reconstruction failure rate
- Critical data-quality defects
- Unauthorised-access incidents
- Authority requests overdue
- Records destroyed under hold

Escalation rule	Missing or altered records, material data corruption, unauthorised access, potential tipping-off or inability to meet a competent-authority deadline shall be escalated immediately to the MLRO, Legal, Information Security and accountable record owner.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 16: Training, competence and financial-crime culture

Legal / framework basis	Law No. 20 of 2019; Implementing Regulations; FATF Recommendation 18

Objective	Ensure that personnel understand their role-specific obligations, recognise relevant risks and demonstrate competence through assessed learning and supervised performance.

Policy statement

The entity shall maintain a risk-based AML/CFT/CPF training programme covering the governing body, senior management, first line, MLRO and Compliance, operations, screening, monitoring, technology, data, procurement and assurance roles. Training shall be timely, role-specific, tested and updated for legal change, sector risks, control failures and actual typologies.

Detailed requirements

16.1 Training needs analysis

The annual needs analysis shall map roles to decisions, data access, products, customer contact, sanctions responsibilities, reporting duties and control failures. It shall identify required learning at induction, before system or product access, periodically and after a material change or incident.

Generic awareness may form a common foundation but shall not replace specialist training for KYC, EDD, PEP, sanctions, alert investigation, STR decision, payment operations, product governance, technology or independent assurance.

16.2 Content and practical application

Content shall cover applicable Qatar requirements, the entity's policy, confidentiality and tipping-off, current internal reporting channel, customer and beneficial-owner verification, PEPs, TFS and PF, monitoring, red flags, record keeping and consequences of non-compliance.

Examples shall reflect the sector and actual products and distinguish ML, TF, PF, fraud, sanctions and ordinary customer service. Exercises shall require a decision or escalation, not passive attendance only.

16.3 Assessment and competence

Completion shall require an approved assessment threshold and, for critical roles, practical observation, case simulation or supervisor sign-off. Failure shall trigger targeted remediation and restricted duties where the deficiency could create immediate risk.

The entity shall retain attendance, assessment, attempts, scores, remediation and competence evidence. Training effectiveness shall be compared with operating errors, internal reports, QA findings and near misses.

16.4 Governance and continuous improvement

The MLRO shall approve the curriculum and receive management information on coverage, overdue populations, assessment failures and high-risk roles. Business managers are responsible for releasing staff to complete learning and reinforcing expected behaviour.

Regulatory change, a new product, sanctions event, missed STR, data failure, enforcement outcome or emerging typology shall trigger content review. Lessons learned shall be incorporated without disclosing protected case information unnecessarily.

Defined controls

TRN-01 - Role-based training assignment

Control owner	Learning and Development with MLRO
Trigger / frequency	At appointment, role change, annual cycle and trigger
How performed	Map each role to required modules and automatically assign the approved curriculum.
Required evidence	Training matrix and assignment log
Classification	Preventive / Automated

TRN-02 - Competence assessment

Control owner	Line Manager and Training Owner
Trigger / frequency	After each required module and practical training
How performed	Apply knowledge and scenario assessment with a defined pass mark and remediate failures.
Required evidence	Assessment and remediation record
Classification	Preventive / Manual

TRN-03 - Access linked to completion

Control owner	Human Resources and Information Security
Trigger / frequency	Before access to critical AML functions
How performed	Prevent or restrict system permissions until required training and competence evidence are complete.
Required evidence	Access/training linkage report
Classification	Preventive / Semi-automated

TRN-04 - Training effectiveness review

Control owner	Compliance QA
Trigger / frequency	At least annually
How performed	Compare learning outcomes with control errors, audit findings, internal disclosures and operational quality.
Required evidence	Effectiveness review
Classification	Detective / Manual

Records and evidence

- Needs analysis
- Curriculum
- Training material
- Attendance

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Assessments
- Remediation
- Competence sign-offs
- Effectiveness review

Management information and effectiveness indicators

- Completion by role
- Overdue high-risk roles
- First-attempt pass rate
- Repeat failure rate
- Operational errors after training
- Time to update training after trigger

Escalation rule	Failure or refusal to complete mandatory training, repeated competence failure in a critical role or evidence that training content is materially inaccurate shall be escalated to the MLRO, Human Resources and the accountable manager for restriction and remediation.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 17: Management information, governance reporting and regulatory submissions

Legal / framework basis	Law No. 20 of 2019; applicable sector rules; FATF Recommendation 18

Objective	Provide accurate, balanced and decision-useful information on risk, control effectiveness, incidents and remediation to management, the governing body and regulators.

Policy statement

AML/CFT/CPF management information shall be reconciled, risk-based and sufficiently detailed to support action. Reports shall distinguish activity volume from control effectiveness, present trends and ageing, disclose material limitations and identify the decision, owner and deadline required. Regulatory submissions shall use the current form, scope, channel and approval.

Detailed requirements

17.1 Reporting architecture and definitions

A reporting catalogue shall define each report, audience, purpose, frequency, owner, source systems, data definitions, cut-off, reconciliation, review, approval, confidentiality and retention. The same metric shall use a consistent definition across committees unless a difference is clearly explained.

Management information shall cover the EWRA and appetite, customer risk, overdue CDD and EDD, PEPs, screening and TFS, monitoring alerts and cases, internal disclosures and STR themes, data and systems, training, incidents, regulatory change, audit findings and remediation.

17.2 Decision-oriented analysis

Reports shall explain the movement and cause, not present counts alone. A rise or fall in alerts or STRs shall be analysed for business growth, risk change, scenario tuning, data failure, staffing, quality and typology rather than labelled automatically as improvement or deterioration.

Material limitations, risk acceptance, overdue actions and uncertainty shall be explicit. The report shall identify decisions required from the audience and track prior decisions to closure.

17.3 Data quality and attestation

Source populations and key totals shall be reconciled, and manual adjustments shall be documented and approved. Report owners and data owners shall attest completeness and accuracy according to defined materiality and acceptance criteria.

Where a limitation could mislead the audience, the affected metric shall be qualified or withheld, the limitation and estimated impact explained, and a corrective action assigned. Unsupported precision shall not replace reliable evidence.

17.4 Regulatory and QFIU submissions

The entity shall maintain a calendar of sector questionnaires, returns, MLRO reports, notifications and other required submissions, including owner, approver, source, form, channel and deadline. The latest official form and instructions shall be verified before preparation.

Submissions shall be independently reviewed for scope, completeness, consistency and approval, transmitted securely and supported by evidence of receipt. Errors after submission shall be escalated and corrected transparently under the applicable process.

Defined controls

MI-01 - Controlled reporting catalogue

Control owner	MLRO Office
Trigger / frequency	At least annually and after reporting change
How performed	Maintain report definitions, ownership, data sources, frequency, approval and confidentiality.
Required evidence	Approved catalogue
Classification	Preventive / Manual

MI-02 - Data reconciliation and attestation

Control owner	Report Owner and Data Owners
Trigger / frequency	For each material report
How performed	Reconcile source populations and totals, document adjustments and attest completeness and accuracy.
Required evidence	Reconciliation and attestation
Classification	Detective / Manual

MI-03 - Committee challenge and action tracking

Control owner	Committee Chair / Secretariat
Trigger / frequency	At each meeting
How performed	Record challenge, decisions, owners and deadlines and follow actions to evidence-based closure.
Required evidence	Minutes and action tracker
Classification	Preventive / Manual

MI-04 - Regulatory submission quality gate

Control owner	Regulatory Compliance and Approver
Trigger / frequency	Before every submission
How performed	Verify current form, population, consistency, evidence, approval and secure transmission.
Required evidence	Submission checklist and receipt
Classification	Preventive / Manual

Records and evidence

- Reporting catalogue
- Data definitions
- Reconciliations
- Management reports

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Attestations
- Committee minutes
- Submission calendar
- Returns and receipts

Management information and effectiveness indicators

- Reports issued on time
- Metrics with unresolved limitation
- Reconciliation differences
- Actions overdue
- Regulatory submissions late
- Post-submission corrections

Escalation rule	A materially unreliable report, missed regulatory deadline, inconsistent submission, concealed limitation or critical action overdue shall be escalated to the MLRO, accountable executive and governing body committee.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 18: Independent assurance, control testing and remediation

Legal / framework basis	Law No. 20 of 2019; Implementing Regulations; FATF Recommendation 18; Global Internal Audit Standards 2024 where Internal Audit performs the work

Objective	Assess whether the AML/CFT/CPF programme is adequately designed and operating effectively and ensure deficiencies are corrected and sustainably closed.

Policy statement

The entity shall obtain independent, risk-based assurance over governance, EWRA, CDD and beneficial ownership, PEP and EDD, sanctions and TFS, monitoring, STR reporting, records, training, data, technology, outsourcing and prior remediation. The assurance provider shall be competent, sufficiently independent and unrestricted in access, while protecting confidential information.

Detailed requirements

18.1 Assurance universe and plan

The assurance plan shall be based on the EWRA, legal obligations, regulatory findings, control changes, incidents, data limitations, product exposure and prior results. High-risk processes and critical controls shall receive appropriate frequency and depth; coverage shall not be driven only by the time since the last review.

The engagement objective, scope, criteria, population, sampling method, acceptance criteria, evidence requirements, reliance and limitations shall be documented. Exclusions shall identify risk and approval and shall not silently remove critical processes.

18.2 Design and operating effectiveness

Design effectiveness asks whether the control, if performed as prescribed, would address the stated risk with clear owner, trigger, method, evidence and escalation. Operating effectiveness asks whether it was performed consistently, completely, accurately and on time over the selected period.

Testing shall use reliable populations, justified samples, reperformance, inspection, observation, inquiry corroborated by evidence and data analysis where appropriate. A single example does not prove consistent operation, and an absence of reported incidents does not prove effectiveness.

18.3 Findings and root cause

A finding shall state condition, criteria, root cause, consequence/risk, rating and actionable recommendation. The rating shall consider regulatory breach, customer and market harm, financial-crime exposure, duration, population, control dependency, detectability and management response.

Root cause shall go beyond the immediate error and examine governance, accountability, capacity, competence, process design, technology, data, incentives and change management. Recommendations shall address the root cause and identify priority, owner and target date.

18.4 Validation and sustainable closure

Management shall provide a corrective action, accountable owner, target date, interim control and target residual risk. Critical or high findings require timely senior and governing-body oversight and may require regulator notification according to the applicable framework.

Closure validation shall inspect and test the implemented solution and an adequate period of operation. A policy update or management statement alone is insufficient. Recurring findings shall trigger broader root-cause and accountability review.

Defined controls

AUD-01 - Risk-based assurance plan

Control owner	Chief Audit Executive / Independent Assurance Lead
Trigger / frequency	Annual and on material trigger
How performed	Prioritise the AML universe using risk, regulatory, incident, change and prior-finding information.
Required evidence	Approved assurance plan
Classification	Preventive / Manual

AUD-02 - Population and sample validation

Control owner	Engagement Lead
Trigger / frequency	Before detailed testing
How performed	Confirm population completeness, select a justified sample and define evidence and acceptance criteria.
Required evidence	Sampling memorandum and population reconciliation
Classification	Detective / Manual

AUD-03 - Independent quality review

Control owner	Audit Quality Reviewer
Trigger / frequency	Before report issue
How performed	Challenge criteria, evidence, conclusions, rating, root cause and recommendation and confirm confidentiality.
Required evidence	Quality review checklist
Classification	Preventive / Manual

AUD-04 - Evidence-based closure validation

Control owner	Internal Audit / Independent Validator
Trigger / frequency	When management requests closure
How performed	Inspect implementation, test operation and confirm that the root cause and risk are addressed.
Required evidence	Closure validation workpaper
Classification	Detective / Manual

Records and evidence

- Audit universe
- Risk assessment
- Engagement plan

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- RCM
- Population and sample
- Workpapers
- Findings
- Management actions
- Closure validation
- Quality review

Management information and effectiveness indicators

- High-risk assurance coverage
- Findings by rating
- Repeat finding rate
- Actions overdue
- Closure rejection rate
- Time to validate critical actions

Escalation rule	A critical control failure, limitation imposed on assurance, evidence of management interference, repeated high-risk finding or unremediated regulatory breach shall be escalated to the audit committee and MLRO without delay.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Chapter 19: Breaches, exceptions, disciplinary action and policy review

Legal / framework basis	Law No. 20 of 2019; applicable sector rules and employment/governance requirements
Objective	Identify and contain control breaches, prohibit unlawful exceptions, apply fair accountability and ensure the manual remains current and effective.

Policy statement

The entity shall record, assess, contain, investigate and remediate AML/CFT/CPF breaches and near misses. No internal exception may waive a legal prohibition, STR duty, TFS action, required CDD or regulator access. Permissible risk-based exceptions shall be narrowly defined, approved by proper authority, time-bound, monitored and independently reviewed.

Detailed requirements

19.1 Breach identification and triage

Personnel shall report control failures, missed or late reviews, screening or monitoring defects, unauthorised overrides, data loss, disclosure, delayed reporting and suspected misconduct through defined channels. The incident record shall distinguish event, affected population, legal obligation, immediate risk and known limitation.

Triage shall assess potential regulatory breach, sanctions or STR impact, customer and transaction exposure, duration, volume, recurrence and containment. Critical issues shall receive immediate senior, Legal, MLRO, Technology or Information Security involvement as appropriate.

19.2 Containment and look-back

Containment may include blocking onboarding or transactions, disabling a rule change, restricting access, implementing manual review, freezing affected processing, preserving evidence and notifying relevant control owners. Actions shall be lawful and avoid tipping-off.

The entity shall identify the full affected period and population and conduct a risk-based look-back. Re-screening, re-monitoring, customer review, STR reconsideration or regulatory notification shall be performed where the failure may have caused missed obligations.

19.3 Exception governance and accountability

Permissible exceptions shall state the requirement, rationale, risk, compensating control, owner, approver, start and expiry, affected population and monitoring. Automatic renewal is prohibited; expiry shall close the exception or trigger formal reassessment.

Accountability and disciplinary action shall be consistent with law, human-resources policy, intent, competence, prior instruction, impact and recurrence. Commercial seniority shall not shield misconduct, and good-faith internal reporting shall not attract retaliation.

19.4 Lessons learned and policy review

Root-cause analysis shall identify whether governance, capacity, competence, process, system, data, incentive, supplier or change-management failure contributed. Corrective actions shall update the relevant control, training, monitoring and assurance rather than only address the individual case.

The manual shall be reviewed on the approved cycle and on legal, regulatory, product, organisational, system, risk or incident triggers. The review shall document sources checked, changes made, decisions retained, consultation and approval.

Defined controls

INC-01 - Breach and near-miss reporting

Control owner	All Personnel / Incident Management
Trigger / frequency	Immediately upon awareness
How performed	Record the event through a protected channel and route it by severity and subject matter.
Required evidence	Incident record and receipt
Classification	Detective / Semi-automated

INC-02 - Containment and affected-population assessment

Control owner	MLRO and Incident Owner
Trigger / frequency	For each material event
How performed	Identify period and population, apply containment and decide look-back, reprocessing and notification.
Required evidence	Containment plan and population analysis
Classification	Preventive / Manual

INC-03 - Time-bound exception approval

Control owner	MLRO / Legal / Authorised Executive
Trigger / frequency	Before any permissible deviation
How performed	Document rationale, risk, compensating control, owner, expiry and monitoring; block unlawful exceptions.
Required evidence	Exception record and approval
Classification	Preventive / Manual

INC-04 - Root-cause and lessons-learned review

Control owner	Independent Incident Reviewer / Compliance QA
Trigger / frequency	After containment of material events
How performed	Determine systemic causes, verify corrective actions and feed learning into policy, systems, training and assurance.
Required evidence	Root-cause report and action tracker
Classification	Detective / Manual

Records and evidence

- Incident register
- Containment records
- Affected-population analysis

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

- Look-back results
- Exception register
- Disciplinary records
- Root-cause analysis
- Policy review log

Management information and effectiveness indicators

- Incidents by severity
- Time to contain
- Affected cases reprocessed
- Exceptions overdue
- Repeat incidents
- Actions overdue
- Policy review completed on time

Escalation rule	A suspected legal breach, missed TFS or STR obligation, tipping-off, deliberate override, material data failure or retaliation against a good-faith reporter shall be escalated immediately to the MLRO, Legal and the appropriate governing body authority.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Enterprise RACI matrix

The matrix establishes execution, accountability, consultation and information roles. It must be adapted to the approved organisation structure without assigning more than one accountable role to a decision unless governance documents expressly create joint accountability.

- R - Responsible - performs the activity and produces the evidence.
- A - Accountable - owns the outcome and approves or accepts the decision. One accountable role per activity.
- C - Consulted - provides required specialist input before the decision.
- I - Informed - receives the result or status after the decision.

	Role
	Governing Body / Committee
	Senior Management
	Business / First Line
	MLRO / Compliance
	Legal
	Risk
	KYC / Operations
	Technology / Data
	Internal Audit

	GB	SM	BUS	AML	LEG	RISK	OPS	TECH	IA
PF policy and risk appetite	A	R	C	R	C	C	I	I	I
obligations register	I	I	C	A/R	C	C	I	I	I
the EWRA	A	R	C	R	C	R	C	C	I
k-rating methodology	I	A	C	R	C	R	C	C	I
stomer information	I	I	A	C	C	I	R	C	I
eneficial owners	I	I	A	C	C	I	R	C	I
nd PEP relationships	I	A	C	R	C	C	R	I	I
sts and screening	I	I	I	A/R	C	I	C	R	I
sanctions matches	I	I	I	A/R	C	I	R	C	I
quired freeze and	I	I	I	A/R	C	I	R	R	I
monitoring	I	I	C	A	I	C	R	R	I
d escalate suspicion	I	I	C	A	I	I	R	C	I
n STR	I	I	I	A/R	C	I	C	I	I
ls and restricted access	I	A	C	C	C	I	R	R	I
s and technology	I	A	R	R	C	R	C	R	I
r outsourced AML services	I	A	R	R	C	C	C	R	I

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

aining	I	A	R	R	C	C	C	C	I
t and regulatory reports	I	A	C	R	C	C	R	R	I
t AML assurance	I	I	I	C	C	C	I	I	A/R
and close findings	I	A	R	C	C	C	R	R	R

eguard	The first and second lines design and operate controls; Internal Audit or another independent assurance provider evaluates them. Internal Audit shall not become responsible or accountable for controls it is expected to audit.

Detailed operating procedures

Each procedure defines the trigger, inputs, responsible role, decision point and evidence. The entity shall configure service standards and escalation timelines from current legal and supervisory requirements and its approved risk appetite.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-01 - Regulatory applicability and legal-change management

Procedure owner	Regulatory Compliance
Approver	MLRO and Legal
Trigger	Initial implementation; regulatory change; licence, product, entity or supervisory-scope change

Inputs

- Official source or notice
- Current obligations register
- Licence and product inventory
- Process and control inventory

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**Regulatory Compliance**	Capture the official source, effective date, authoritative language, affected provisions and verification date in the source register.	Is the source relevant to the entity or its activities?	Source-register entry
2	**Legal**	Confirm the legal fact and identify interpretation questions; distinguish binding requirement from guidance and unofficial translation.	Is external legal advice or regulator clarification required?	Legal analysis
3	**MLRO and Process Owners**	Map affected legal entities, products, customers, processes, systems, forms, data, training and reports.	Does the change affect STR, TFS, CDD, BO or retention?	Impact matrix
4	**Accountable Executive**	Risk-rate the change, set the implementation owner and deadline, and approve interim controls for any gap before the effective date.	Can the entity operate lawfully before full implementation?	Approved implementation plan
5	**Technology / Operations**	Implement controlled procedure, system, form, data and workflow changes and execute documented tests.	Have all critical acceptance criteria passed?	Implementation and test evidence
6	**Training Owner**	Communicate and train affected roles before they perform the changed activity.	Is competence evidence sufficient for critical roles?	Training record
7	**Compliance QA / Internal Audit**	Independently test design, implementation and an appropriate live-operation sample.	Is closure supported by operating evidence?	Closure-validation workpaper
8	**MLRO**	Update the obligations register, report status and residual risk, and authorise closure or reopening.	Does residual risk remain above appetite?	Closure decision and governance report

Outputs

- Updated obligations register
- Approved impact assessment
- Implemented change
- Independent closure evidence

Critical control points

- Official-source verification
- Legal interpretation sign-off
- Effective-date control
- Independent closure test

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Exception and escalation	An unresolved change affecting reporting, freezing, prohibited business or minimum CDD shall be escalated and the affected activity restricted until a lawful control is in place.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-02 - Enterprise-wide ML/TF/PF risk assessment

Procedure owner	AML Risk Function
Approver	Governing Body / Committee
Trigger	Approved cycle or trigger event

Inputs

- Prior EWRA
- NRA and sector risk information
- Customer/product/channel/geographic data
- Controls and assurance results
- Incidents and typologies

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**AML Risk Function**	Define the scope, entities, period, factor taxonomy, method, rating scale, weights, owners and timetable.	Is every material activity and risk family included?	Approved methodology and scope
2	**Data Owners**	Extract, reconcile and attest quantitative inputs; document data lineage, completeness and limitations.	Are material differences or missing data unresolved?	Data pack and reconciliations
3	**Business and Compliance**	Assess inherent customer, product/service/transaction, channel and geographic risks, with separate ML, TF and PF consideration.	Are concentrations hidden by aggregation?	Inherent-risk assessment
4	**Control Owners**	Assess design and operating effectiveness of controls using evidence rather than policy existence.	Does each risk reduction have an evidenced control?	Control-effectiveness assessment
5	**AML Risk Function**	Calculate residual risk, perform sensitivity and concentration analysis and document overrides and limitations.	Does residual risk exceed inherent risk logic or appetite?	Residual-risk results
6	**MLRO / Risk**	Challenge assumptions, scores, control ratings, data quality and the distinction between legal fact and professional judgement.	Are material challenges resolved or transparently recorded?	Challenge log
7	**Senior Management**	Define treatment actions, owners, dates, interim controls and target residual ratings.	Can above-appetite risk be temporarily accepted lawfully?	Risk treatment plan
8	**Governing Body**	Approve the EWRA, appetite implications, resources and actions and require periodic status reporting.	Is the risk response proportionate and funded?	Approval minutes

Outputs

- Approved EWRA
- Risk treatment plan
- Updated CRR and monitoring inputs
- Governance reporting

Critical control points

- Population reconciliation
- Four-factor-family completeness
- Control-effectiveness evidence
- Board approval

Exception and escalation	A critical risk, unreliable material data, unmitigated sanctions/reporting exposure or residual risk above appetite shall be reported immediately with interim restrictions.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-03 - New product, channel and technology approval

Procedure owner	Product Owner
Approver	Change Approval Committee
Trigger	Concept proposal or material change

Inputs

- Business case
- Product and process design
- Target market
- Data and system design
- Provider information

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**Product Owner**	Describe the product, customers, jurisdictions, transaction flows, channels, funding, intermediaries, volumes and launch plan.	Is the change material under the governance standard?	Change request
2	**MLRO / Risk**	Assess ML, TF, PF, fraud, sanctions and misuse scenarios and map them to the EWRA.	Is any exposure prohibited or above appetite?	Risk assessment
3	**KYC / Operations**	Specify onboarding, BO, CRR, EDD, approval, review and record requirements.	Can the required customer knowledge be obtained and verified?	CDD control design
4	**Sanctions / Monitoring**	Define screening points, monitoring scenarios, data fields, thresholds, alert ownership and outage fallback.	Is end-to-end coverage demonstrable?	Screening and monitoring requirements
5	**Technology / Data**	Build controlled rules, access, audit trails, reconciliations, retention and management information.	Are critical data elements complete and traceable?	Configured solution
6	**Cross-functional Test Team**	Execute positive, negative, high-risk, sanctions, data-failure, override and contingency tests.	Are critical acceptance criteria met?	Test results and defect log
7	**Change Approval Committee**	Review residual risk, critical defects, resources, training and contingency and approve, defer or reject launch.	Is any condition incomplete?	Formal launch decision
8	**Compliance QA**	Perform post-launch review using actual customers, transactions, alerts, data and incidents.	Do actual outcomes remain within approved assumptions?	Post-launch review

Outputs

- Approved or rejected change
- Configured controls
- Test evidence
- Post-launch assessment

Critical control points

- Early Compliance involvement
- Critical-defect gate
- Data-lineage verification
- Post-launch review

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Exception and escalation	A prohibited exposure, missing critical control or failed sanctions/reporting test stops launch until remediated and reapproved.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-04 - Customer onboarding and standard CDD

Procedure owner	KYC Operations
Approver	Business Owner
Trigger	New relationship or in-scope occasional transaction

Inputs

- Application
- Identity and authority evidence
- Legal and ownership documents
- Product request
- Expected activity

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**Business**	Record the relationship purpose, requested products, expected activity, counterparties, jurisdictions and commercial rationale.	Is the purpose legitimate and consistent with the entity's licence and appetite?	Business rationale
2	**KYC Operations**	Identify and verify the customer and representatives using approved reliable independent sources.	Are identity and authority complete and valid?	Verification record
3	**KYC Operations**	Reconstruct ownership and control to natural persons and verify beneficial owners proportionate to risk.	Is ownership transparent and supported?	Ownership chart and BO evidence
4	**Screening Operations**	Screen customer, BO, controllers, representatives and relevant connected parties for sanctions, PEP and adverse information.	Is there a potential match or higher-risk information?	Screening results
5	**KYC Risk Engine / Analyst**	Calculate the customer risk rating and apply mandatory overrides and prohibited criteria.	Does the customer require EDD or senior approval?	Risk-rating record
6	**KYC Reviewer**	Perform maker-checker review of completeness, consistency, verification, screening, risk rating and required evidence.	Are all defects resolved?	Review checklist
7	**Business Owner**	Approve standard-risk acceptance and activate approved products only after the system completion gate passes.	Are any conditions or restrictions outstanding?	Acceptance and activation record
8	**KYC QA**	Select risk-based post-onboarding samples and reperform critical checks.	Is a systemic defect indicated?	QA report and remediation

Outputs

- Approved or declined relationship
- Complete CDD file
- Risk rating
- Expected-activity baseline

Critical control points

- Independent verification
- Beneficial-owner completion
- Screening before activation
- Maker-checker review
- System activation gate

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Exception and escalation	Identity doubt, material inconsistency, opaque ownership, potential sanctions match or high risk moves the file to the appropriate escalation or EDD pathway before activation.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-05 - Beneficial owner, PEP and enhanced due diligence

Procedure owner	EDD Team
Approver	MLRO / Senior Management
Trigger	High customer rating, PEP, complex structure, high-risk geography, adverse information or other EDD trigger

Inputs

- Standard CDD file
- Ownership structure
- PEP and adverse-media results
- Risk drivers
- Proposed relationship

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**EDD Analyst**	State each EDD trigger and the risk-specific information and evidence required to address it.	Is the trigger statutory, model-driven or professional judgement?	EDD plan
2	**EDD Analyst**	Obtain additional identity, background, ownership, business, financial and relationship information.	Are independent sources sufficient for the assessed risk?	Additional evidence
3	**EDD Analyst**	Establish and corroborate source of wealth and the source of funds for material funding or transactions.	Are wealth and funds plausible and consistent?	SoW/SoF assessment
4	**Screening Specialist**	Resolve PEP category, sanctions potential matches, adverse media and connected-party exposure.	Does any result require prohibition, freeze or further investigation?	Adjudication record
5	**Business and Monitoring**	Define acceptance conditions, product limits, enhanced monitoring scenarios and review frequency.	Do the measures address the identified risks?	Risk treatment plan
6	**MLRO**	Challenge completeness, legitimacy, residual risk and any suspicion indicator.	Is an internal suspicion decision required?	MLRO review
7	**Senior Management**	Approve, reject or continue the relationship with documented conditions as required.	Is residual risk within appetite and legally acceptable?	Senior approval
8	**KYC Operations**	Implement conditions and confirm system restrictions, monitoring and review dates before activation or continuation.	Are all mandatory conditions evidenced?	Condition activation record

Outputs

- EDD conclusion
- Senior approval or rejection
- SoW/SoF evidence
- Enhanced monitoring plan

Critical control points

- Trigger-specific measures
- Independent corroboration
- MLRO challenge
- Senior approval

- Condition implementation

Exception and escalation	A designated party, unexplained wealth/funds, false information, unresolved ownership or formed suspicion is handled through the sanctions or STR pathway and is not cured by additional documents alone.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-06 - Sanctions potential match, freezing and reporting

Procedure owner	Sanctions Compliance
Approver	MLRO / Sanctions Officer
Trigger	Customer, connected-party or transaction screening alert

Inputs

- Alert and screened data
- Current list record
- Customer and transaction identifiers
- Ownership/control information

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**System / Operations**	Place the affected relationship or transaction in the approved hold state and preserve the screening evidence.	Was the alert generated before release?	Hold and alert log
2	**Sanctions Analyst**	Compare name, aliases, date of birth, nationality, identification, address and other identifiers.	Can the alert be confidently discounted?	Identifier comparison
3	**Sanctions Analyst**	Assess ownership, control, representation and indirect benefit involving a designated party.	Could the designation apply through ownership or control?	Ownership/control analysis
4	**Senior Sanctions Reviewer**	Independently review the evidence and classify the result as false positive, unresolved potential match or true match.	Is additional competent-authority guidance required?	Reviewed adjudication
5	**MLRO / Legal**	Determine the applicable legal action, competent reporting channel and any parallel suspicion assessment.	Does the legal trigger require freezing without delay?	Legal action decision
6	**Operations / Technology**	Execute the freeze and prohibition across all relevant systems and prevent unauthorised release or service.	Is the full funds/economic-resources population controlled?	Freeze evidence
7	**MLRO / Sanctions Officer**	Submit the required notification or report securely and retain acknowledgement.	Has the current official channel and form been verified?	Report and receipt
8	**Information Security / Compliance**	Restrict access, monitor leakage and perform incident and population look-back where needed.	Was any activity released or information disclosed improperly?	Access review and look-back

Outputs

- Documented discount or confirmed match
- Freeze and prohibition evidence
- Competent-authority report
- Incident/look-back result

Critical control points

- Pre-release hold
- Independent adjudication
- Ownership/control test
- Freeze without delay
- Restricted access

Exception and escalation	A system outage, incomplete identifier set, unresolved potential match or evidence of prior release is escalated immediately and controlled under the contingency and incident procedures.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-07 - Transaction-monitoring alert investigation

Procedure owner	Transaction Monitoring
Approver	Monitoring Team Leader
Trigger	Monitoring alert or manual referral

Inputs

- Alert parameters
- Customer profile and risk rating
- Transaction history
- Counterparty and screening data
- Prior cases

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**Monitoring Analyst**	Confirm alert population, scenario, data completeness and processing time; correct or escalate data defects.	Is the alert reliable enough to investigate?	Alert validation
2	**Monitoring Analyst**	Compare the activity with expected values, volumes, counterparties, geography, products and channel.	What specific deviation caused the alert?	Baseline comparison
3	**Monitoring Analyst**	Reconstruct the relevant flow chronologically, including source, destination, linked activity and remaining gaps.	Does the pattern match a known typology?	Transaction chronology
4	**Monitoring Analyst**	Review CDD, BO, PEP, sanctions, adverse media, prior alerts and lawful connected-party information.	Do combined facts heighten or reduce concern?	Context review
5	**Business / Customer Team**	Provide authorised factual information or documents using neutral wording that avoids tipping-off.	Is the explanation supported and plausible?	Business information
6	**Monitoring Analyst**	Document facts, analysis, typology, contradictory evidence, limitations and recommended closure or escalation.	Are reasonable grounds for suspicion present?	Investigation narrative
7	**Senior Reviewer**	Reperform critical steps and approve closure or internal suspicion escalation.	Is the evidence sufficient and conclusion consistent?	Review decision
8	**Monitoring Governance**	Feed material themes, data issues and false-negative concerns into tuning, EWRA and training.	Is systemic remediation required?	Feedback and action record

Outputs

- Closed alert with rationale or internal suspicion report
- Identified data/control issues
- Typology feedback

Critical control points

- Expected-profile comparison
- Chronological reconstruction
- Reasoned closure
- Independent review
- Tipping-off control

Exception and escalation	A sanctions indicator follows the sanctions process immediately; possible suspicion follows the protected internal-reporting route without waiting for proof.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-08 - Internal suspicion assessment and STR filing

Procedure owner	MLRO Office
Approver	MLRO
Trigger	Internal disclosure, escalated case or other information indicating possible suspicion

Inputs

- Internal report
- CDD and BO file
- Transaction and alert history
- Screening data
- Supporting evidence

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**MLRO Office**	Acknowledge receipt, assign a restricted case reference and protect the reporter and information.	Is urgent transaction, sanctions or safety action required?	Restricted case record
2	**MLRO / Investigator**	Assess completeness and obtain authorised additional internal information without unnecessary delay or tipping-off.	Is the evidence sufficient to evaluate suspicion?	Information plan
3	**MLRO / Investigator**	Reconstruct subjects, relationship, activity, counterparties, dates, amounts, jurisdictions and channels.	What is verified fact and what remains inference?	Factual chronology
4	**MLRO**	Assess deviation, typology, legitimate explanation, predicate indicators and the applicable suspicion standard.	Does suspicion or reasonable ground to suspect remain?	Decision analysis
5	**MLRO**	Document the report or no-report decision, rationale, date and any ongoing monitoring or customer treatment.	Is external reporting required now?	MLRO decision
6	**Authorised Preparer**	Prepare the STR narrative and attachments using the current QFIU requirements and factual neutral language.	Are all subjects, transactions and evidence complete?	Draft STR
7	**MLRO**	Quality-review and submit through the prescribed secure channel and retain receipt.	Was submission accepted and on time?	Filed STR and receipt
8	**MLRO / Operations**	Implement lawful follow-up, continued monitoring or restriction without tipping-off and respond to QFIU requests.	Is supplementary reporting required?	Follow-up log

Outputs

- Reasoned report/no-report decision
- STR and receipt where applicable
- Ongoing action and supplemental reporting record

Critical control points

- Independent MLRO authority
- Suspicion standard
- Narrative quality
- Current QFIU channel
- Need-to-know access

Exception and escalation	Urgent sanctions, law-enforcement, customer-safety or dissipation risk is escalated immediately under the applicable legal procedure and does not remove the STR duty.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-09 - Periodic and trigger-based customer review

Procedure owner	KYC Review Team
Approver	KYC Manager / MLRO for high risk
Trigger	Scheduled review date or trigger event

Inputs

- Current CDD file
- Review trigger
- Transactions and expected profile
- Screening and risk data
- Open conditions and findings

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**KYC Review Team**	Confirm the review reason, scope, customer risk tier and applicable due date.	Is a higher-priority trigger present?	Review initiation
2	**KYC Review Team**	Obtain current identity, registration, licence, authority, ownership and control information and verify changes.	Are documents current and independently verified?	Updated CDD evidence
3	**Screening Operations**	Re-screen all required parties and resolve potential sanctions, PEP and adverse-media results.	Does any result require escalation or EDD?	Screening result
4	**KYC Review Team**	Compare actual activity, products, counterparties, geography and funding with the prior expected profile.	Is activity materially inconsistent or unexplained?	Activity comparison
5	**Risk Engine / Analyst**	Recalculate the customer risk rating and apply current overrides and criteria.	Has the treatment tier changed?	Updated risk rating
6	**EDD Team**	Refresh risk-specific EDD, SoW/SoF, PEP approval and monitoring conditions where required.	Are all high-risk measures complete?	Updated EDD
7	**Approver**	Approve continuation, restriction, remediation or exit and assign outstanding actions.	Is residual risk acceptable and lawful?	Review decision
8	**KYC Operations**	Update systems, review date, conditions and monitoring and retain the complete audit trail.	Were all downstream systems updated?	Completion record

Outputs

- Updated customer file
- Current risk rating
- Continuation/restriction/exit decision
- Updated monitoring and review cycle

Critical control points

- Trigger prioritisation
- Ownership refresh
- Activity-to-profile comparison
- Current screening
- Downstream system update

Exception and escalation	A sanctions concern, inability to complete CDD, unexplained activity or formed suspicion follows the relevant escalation process before the review is closed.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-10 - Record retrieval, authority request and secure disclosure

Procedure owner	Records Owner
Approver	MLRO / Legal
Trigger	Authenticated request from a competent authority or approved internal need

Inputs

- Request and authority
- Scope and deadline
- Records inventory
- Legal hold and confidentiality rules

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**Receiving Officer**	Authenticate the requester, record receipt, scope, legal basis, deadline and secure contact details.	Is the request valid and within authority?	Request log
2	**MLRO / Legal**	Interpret scope, resolve ambiguity and identify confidentiality, tipping-off, privilege and preservation requirements.	Is clarification required from the authority?	Scope decision
3	**Records Owner**	Identify systems, custodians, date ranges and record classes and apply or confirm legal hold where needed.	Could ordinary deletion affect responsive records?	Retrieval plan
4	**Data / Operations**	Extract records through controlled methods and preserve integrity, source and chain of custody.	Is the population complete and readable?	Extract and audit trail
5	**Independent Reviewer**	Reconcile the population and review relevance, completeness, duplicates, confidentiality and redaction authority.	Does the response match the approved scope?	Quality review
6	**MLRO / Legal**	Approve the final response and method of secure transmission.	Are all legal and confidentiality conditions met?	Approval
7	**Authorised Sender**	Transmit securely, obtain receipt and log any rejected files or follow-up questions.	Was receipt confirmed before the deadline?	Transmission receipt
8	**Records Owner**	Retain the request, decision, response and receipt and close or continue the legal hold as authorised.	Is further preservation or supplemental response required?	Closed request file

Outputs

- Complete and timely response
- Transmission receipt
- Preserved request file
- Updated legal hold

Critical control points

- Requester authentication
- Scope approval
- Population reconciliation
- Secure transmission
- Tipping-off control

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Exception and escalation	An unauthenticated request, impossible deadline, missing records, suspected alteration or disclosure risk is escalated immediately to the MLRO, Legal and Information Security.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-11 - Role-based training and competence management

Procedure owner	Learning and Development
Approver	MLRO
Trigger	Appointment, role change, annual cycle, legal change, product launch or incident

Inputs

- Role inventory
- Training needs analysis
- Legal and policy changes
- QA and audit findings
- Typologies and incidents

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**MLRO / Training Owner**	Map roles to required knowledge, decisions, system access and training frequency.	Are all high-risk roles identified?	Training matrix
2	**Subject-Matter Owners**	Update content for current Qatar requirements, entity controls, sector risks, reporting channels and lessons learned.	Has Legal/MLRO verified material regulatory content?	Approved curriculum
3	**Learning and Development**	Assign induction, periodic and trigger modules with completion deadlines.	Must access be restricted pending completion?	Assignment record
4	**Employee**	Complete training and scenario-based assessment without unauthorised assistance.	Has the required pass mark been achieved?	Assessment result
5	**Line Manager**	Observe practical competence for critical roles and document supervised sign-off or remediation.	Can the employee perform the control independently?	Competence sign-off
6	**Learning and Development**	Reassign targeted learning, coaching or reassessment for failures and notify managers of overdue status.	Is duty restriction required?	Remediation record
7	**Compliance QA**	Compare training outcomes with control defects, incidents and internal-reporting behaviour.	Is content or delivery ineffective?	Effectiveness review
8	**MLRO**	Report material gaps and approve programme improvements.	Are high-risk gaps within tolerance?	Governance report

Outputs

- Completed training
- Competence evidence
- Remediated failures
- Effectiveness assessment

Critical control points

- Role-based mapping
- Assessment threshold
- Critical-role competence
- Access restriction
- Effectiveness review

Exception and escalation	A critical-role employee who has not demonstrated competence shall not independently operate the affected control until remediation and approval are complete.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-12 - AML outsourcing and third-party oversight

Procedure owner	Service Owner
Approver	Senior Management
Trigger	New provider, material change, renewal, incident or termination

Inputs

- Service specification
- Provider due diligence
- Risk assessment
- Contract
- Service and control data

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**Service Owner**	Define the activity, data, legal obligations, control outcomes, locations, subcontractors and business criticality.	Is outsourcing permitted and within appetite?	Service-risk profile
2	**Procurement / Compliance**	Assess ownership, competence, regulation, sanctions, financial resilience, control environment and reputation.	Does the provider meet minimum eligibility?	Due-diligence file
3	**Information Security / Data**	Assess access, encryption, data location, retention, incident response, continuity and exit migration.	Are critical data and access risks controlled?	Security and data assessment
4	**Legal**	Include service standards, control duties, audit and access rights, regulator access, incident notice, subcontractor, continuity, records and termination clauses.	Can the entity obtain evidence and intervene promptly?	Approved contract
5	**Technology / Operations**	Test integration, data completeness, screening/monitoring outcomes, fallback and record retrieval before go-live.	Have critical acceptance tests passed?	Test evidence
6	**Service Owner / Compliance**	Monitor service, control outcomes, incidents, data, backlog, quality and remediation using defined indicators.	Is performance outside tolerance?	Oversight report
7	**Compliance QA / Internal Audit**	Exercise audit rights and test a risk-based sample of provider operations and records.	Are controls demonstrably effective?	Assurance result
8	**Senior Management**	Approve remediation, restriction, suspension, renewal or exit based on risk and evidence.	Can the service continue lawfully and safely?	Provider decision

Outputs

- Approved provider
- Controlled service
- Oversight and assurance evidence
- Renewal or exit decision

Critical control points

- Pre-contract due diligence
- Regulator and audit access
- Pre-go-live testing
- Outcome monitoring
- Exit readiness

Exception and escalation	A provider that denies access, loses critical data, fails sanctions/reporting controls or cannot maintain service continuity is subject to immediate containment and executive escalation.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

P-13 - Independent assurance and remediation closure

Procedure owner	Internal Audit / Independent Assurance
Approver	Audit Committee
Trigger	Approved audit plan, regulatory request, incident or management trigger

Inputs

- EWRA
- Obligations and controls
- Prior findings
- Populations and data
- Policies, procedures and evidence

Procedure steps

No.	Role	Action	Decision / question	Evidence
1	**Engagement Lead**	Define objective, scope, criteria, risks, processes, period, exclusions, confidentiality and reporting route.	Does the scope cover material regulatory and residual risks?	Engagement planning memorandum
2	**Data Analyst / Auditor**	Obtain and reconcile complete populations and define a justified sample and acceptance criteria.	Is the population reliable for testing?	Population and sampling memorandum
3	**Auditor**	Evaluate design by linking risk, owner, trigger, method, evidence, segregation and escalation.	Would the control address the risk if performed?	Design assessment
4	**Auditor**	Test operating effectiveness through inspection, reperformance, observation and corroborated inquiry over the selected period.	Was the control complete, accurate and timely?	Operating test workpaper
5	**Engagement Lead**	Develop findings using condition, criteria, root cause, consequence, rating and actionable recommendation.	Is the conclusion fully supported and fairly rated?	Draft finding
6	**Independent Quality Reviewer**	Challenge evidence, criteria, sampling, legal accuracy, rating, recommendation and confidentiality.	Are all review points resolved?	Quality-review record
7	**Management**	Agree actions with owner, date, interim control and target outcome; formally record any disagreement.	Does the action address the root cause?	Management action plan
8	**Independent Validator**	Inspect implemented change and test an adequate period of operation before closure.	Is sustainable closure evidenced?	Closure-validation workpaper

Outputs

- Independent assurance conclusion
- Rated findings
- Management action plan
- Validated closure or reopened issue

Critical control points

- Scope tied to risk
- Population reconciliation
- Design vs operating distinction
- Independent quality review
- Evidence-based closure

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Exception and escalation	A scope limitation, critical failure, management interference, repeated high-risk issue or unsupported closure request is escalated to the Audit Committee and MLRO.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

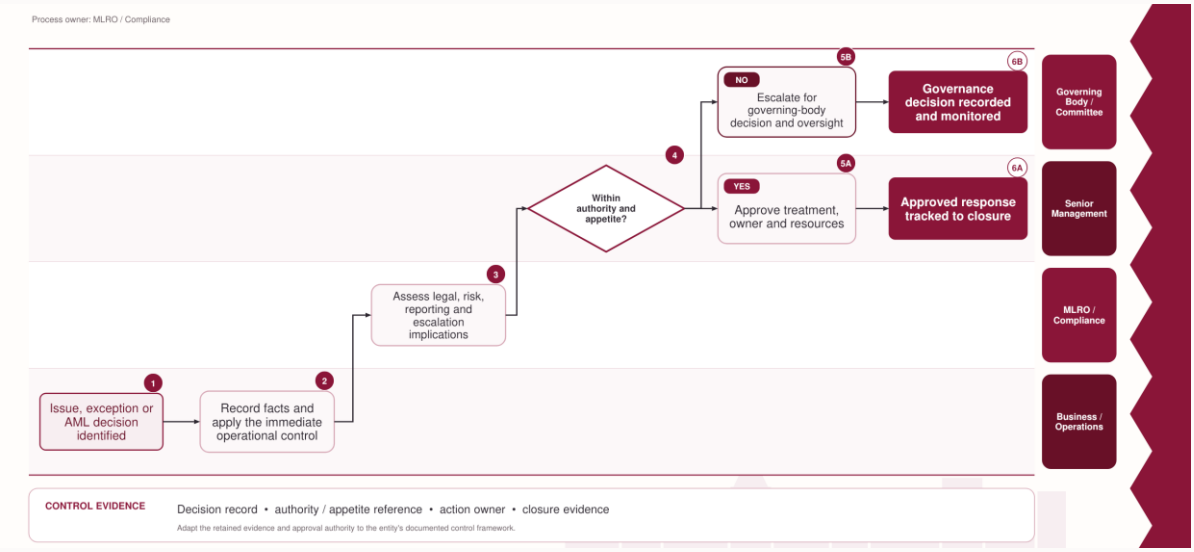
Editable process flowcharts

Embedded process maps	The process maps below are high-resolution images rendered from the companion editable PowerPoint file. The PowerPoint remains the controlled editable source; update its native shapes and re-render the corresponding slide whenever process logic changes.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

FC-01 - AML governance and escalation

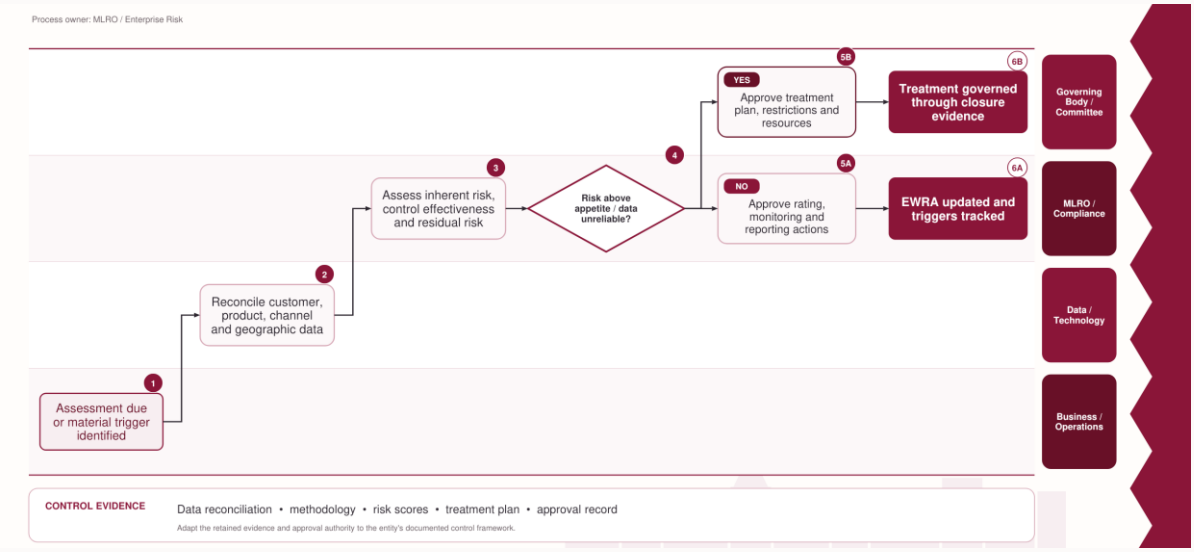
Route policy, risk, incidents and decisions through accountable governance while preserving MLRO independence.



Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

FC-02 - Enterprise-wide risk assessment

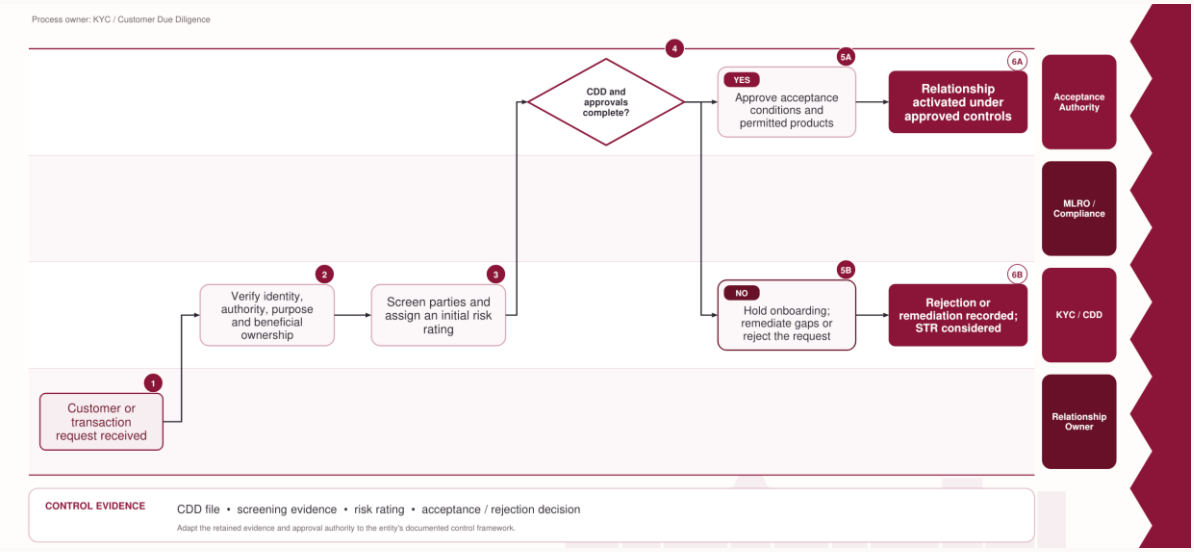
Move from complete data and risk identification to approved residual risk and treatment.



Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

FC-03 - Customer onboarding and CDD

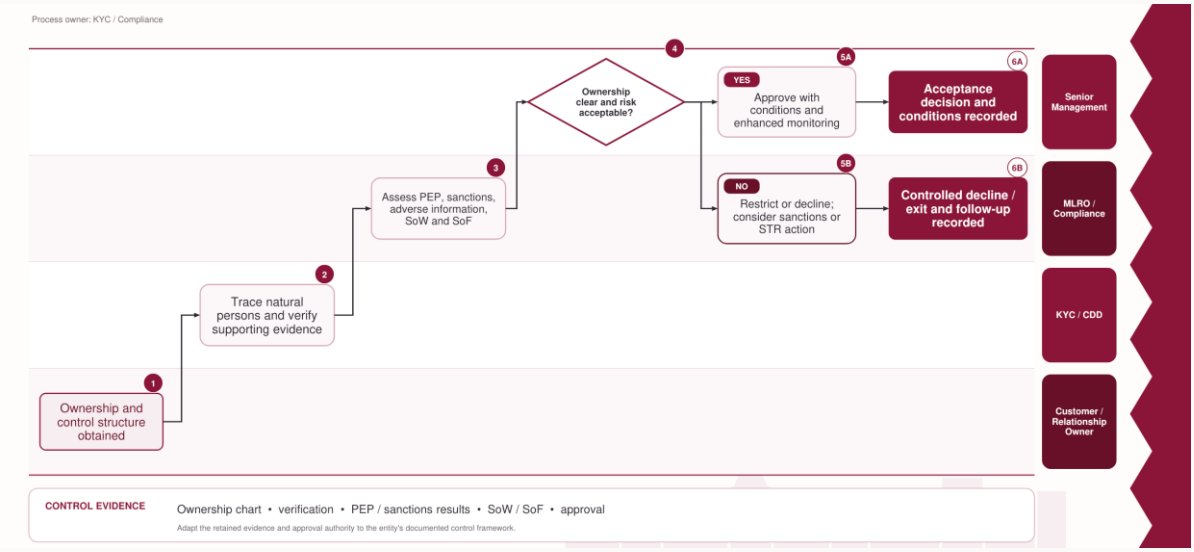
Prevent activation until identity, ownership, screening, risk rating and approval are complete.



Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

FC-04 - Beneficial owner, PEP and EDD

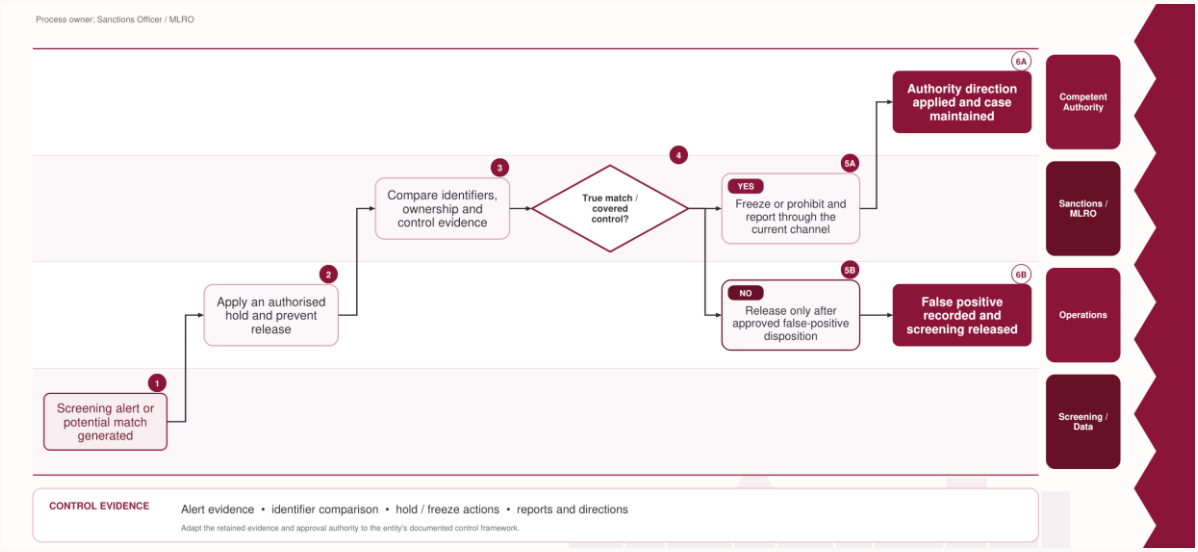
Resolve ownership and high-risk exposure to a natural-person conclusion and risk-specific treatment.



Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

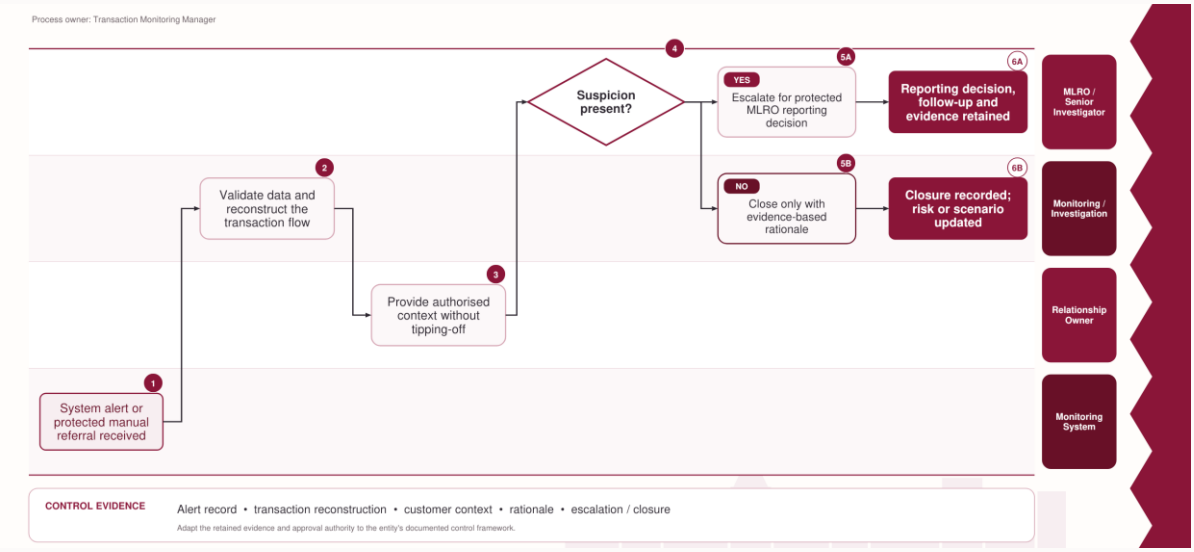
FC-05 - Sanctions screening and TFS action

Resolve a potential match and execute freezing and reporting without delay when required.



FC-06 - Transaction-monitoring alert investigation

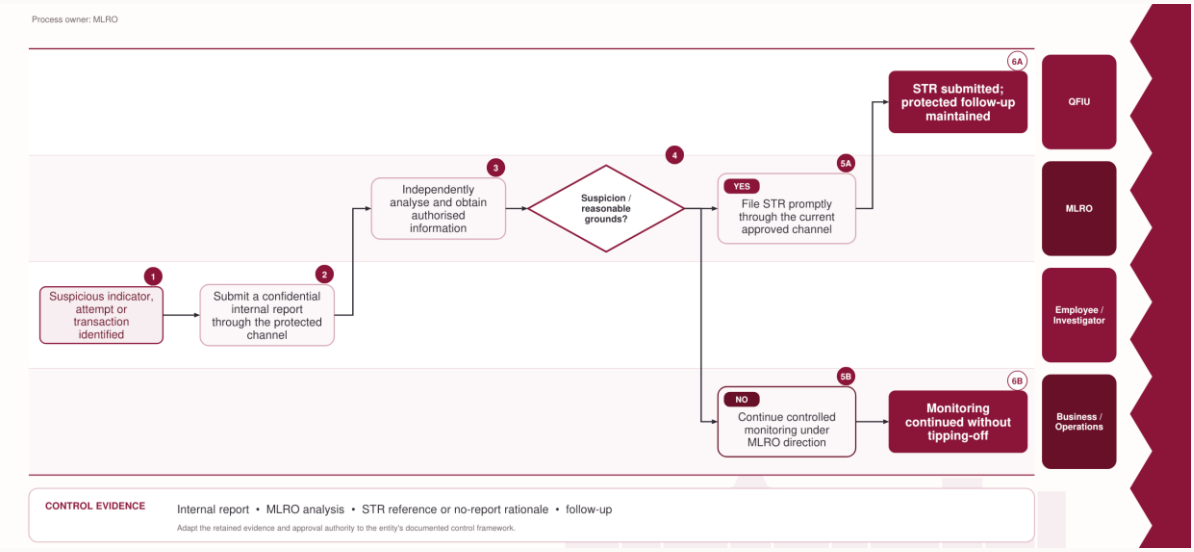
Compare alerted activity with the expected profile, reconstruct the flow and reach a defensible disposition.



Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

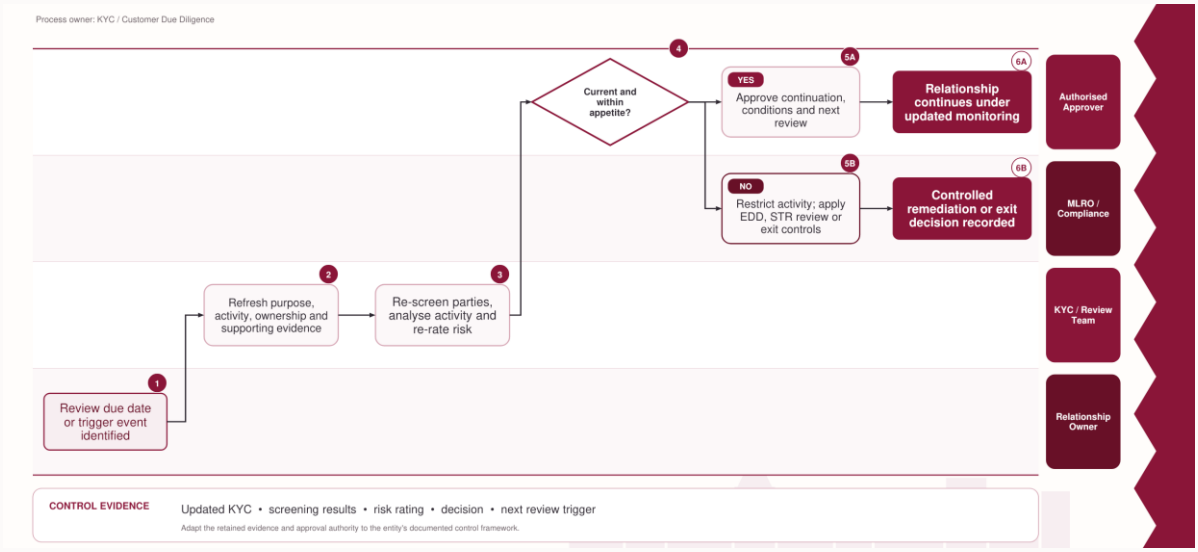
FC-07 - Suspicion to STR

Protect confidentiality and move from internal concern to an independent and timely QFIU filing decision.



FC-08 - Periodic and trigger-based review

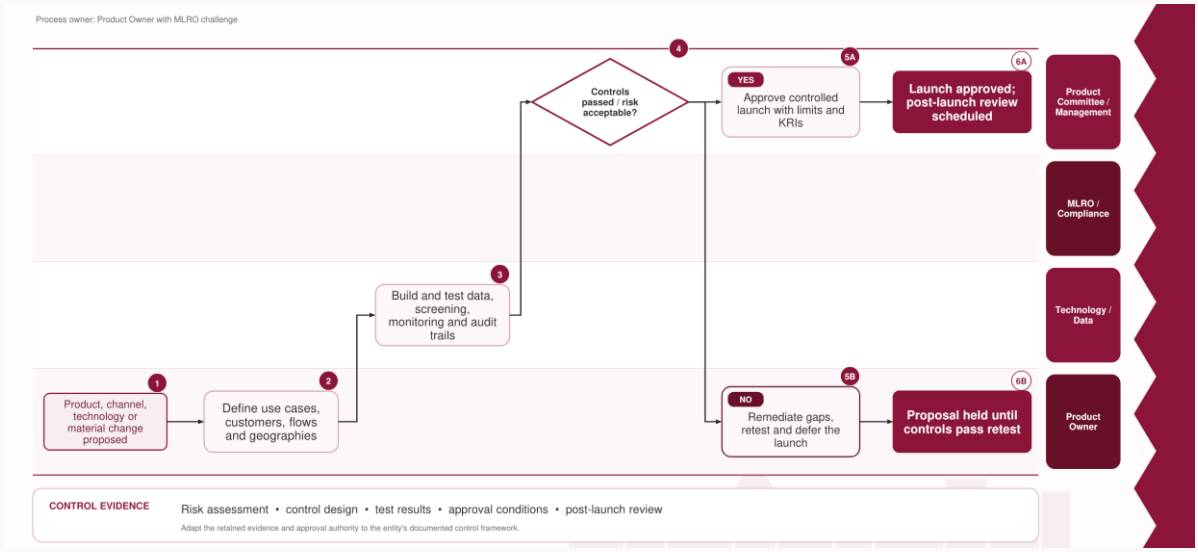
Keep customer knowledge, screening, risk and treatment current throughout the relationship.



Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

FC-09 - New product and technology approval

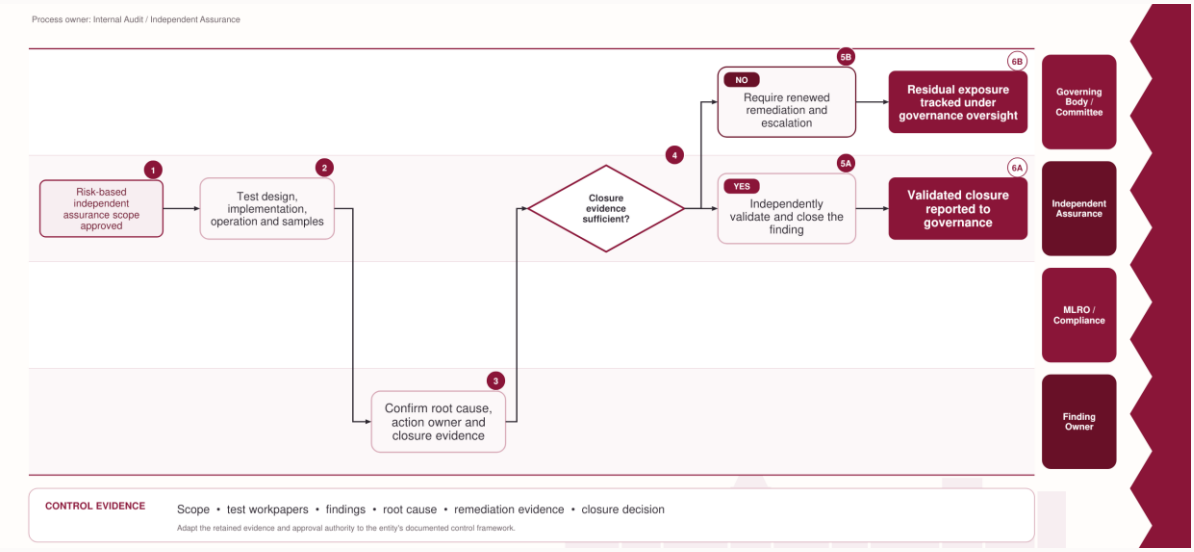
Prevent launch until financial-crime risks, data and controls are designed and tested.



Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

FC-10 - Independent assurance and remediation

Test design and operating effectiveness and close findings only when sustainable operation is evidenced.



Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Professional editable forms

The forms are deliberately uncompleted. The entity shall add legally required fields, system references, authority levels, validation rules and retention classifications before use. Sensitive forms require role-based access and secure storage.

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-01 - Entity and Regulatory Applicability Assessment

Purpose	Determine the entity, licence, regulator, activities and clauses applicable before the manual is approved.
Owner	MLRO / Legal
Approval	Governing Body / Authorised Committee
Classification	Internal - Controlled

Entity profile

Field	Type	Requirement	Response / reference
Legal name	Free text	Required	
Commercial name	Free text	Required	
Legal form	Free text	Required	
Commercial registration number	Free text	Required	
Licence number and category	Free text	Required	
Registered and operating addresses	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Regulatory scope

Field	Type	Requirement	Response / reference
Competent regulator / supervisor	Free text	Required	
Licensed activities	Free text	Required	
Products and services	Free text	Required	
Customer segments	Free text	Required	
Delivery channels	Free text	Required	
Branches, subsidiaries and outsourced activities	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Applicability decision

Field	Type	Requirement	Response / reference
Applicable national instruments	Free text	Required	
Applicable sector instruments	Free text	Required	
Excluded clauses and legal rationale	Free text	Required	

Field	Type	Requirement	Response / reference
Open legal questions	Free text	Required	
Required adaptations and owner	Free text	Required	
Approval and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-02 - EWRA Data and Risk-Factor Input

Purpose	Capture evidence for inherent risk, controls and residual risk across the four FATF risk-factor families.
Owner	AML Risk Function
Approval	MLRO / Risk Committee
Classification	Internal - Restricted

Assessment metadata

Field	Type	Requirement	Response / reference
Assessment period	Free text	Required	
Legal entities and business units in scope	Free text	Required	
Data owner	Free text	Required	
Source system and extraction date	Free text	Required	
Reconciliation reference	Free text	Required	
Known data limitations	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Risk factor

Field	Type	Requirement	Response / reference
Risk-factor family	Customer / Product / Channel / Geography	Required	
Specific risk factor	Free text	Required	
Cause and abuse scenario	Free text	Required	
Exposure measures	Free text	Required	
Inherent likelihood	Free text	Required	
Inherent impact and rationale	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Controls and residual risk

Field	Type	Requirement	Response / reference
Key controls	Free text	Required	
Design effectiveness evidence	Free text	Required	
Operating effectiveness evidence	Free text	Required	
Residual risk and rationale	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Within appetite?	Yes / No	Required	
Treatment, owner and target date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-03 - Customer Acceptance and Prohibited-Exposure Checklist

Purpose	Evidence that required acceptance conditions and prohibited criteria were assessed before activation.
Owner	Business / KYC Operations
Approval	Business Owner / MLRO where required
Classification	Confidential

Relationship request

Field	Type	Requirement	Response / reference
Customer name and reference	Free text	Required	
Requested product/service	Free text	Required	
Purpose and intended nature	Free text	Required	
Expected values and volumes	Free text	Required	
Expected counterparties and jurisdictions	Free text	Required	
Business sponsor and rationale	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Mandatory checks

Field	Type	Requirement	Response / reference
Identity and authority complete?	Yes / No / N/A	Required	
Beneficial ownership complete?	Yes / No / N/A	Required	
Sanctions screening resolved?	Yes / No	Required	
PEP/adverse-media assessment complete?	Yes / No	Required	
Customer risk rating	Free text	Required	
EDD required and completed?	Yes / No / N/A	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Decision

Field	Type	Requirement	Response / reference
Prohibited criterion identified?	Yes / No	Required	
Conditions or restrictions	Free text	Required	
Approver and authority	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Decision	Approve / Reject / Defer	Required	
Activation evidence	Free text	Required	
Reviewer and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

F-04 - Natural Person CDD Record

Purpose	Record and verify a natural person's identity, profile, authority and expected activity.
Owner	KYC Operations
Approval	KYC Reviewer
Classification	Confidential - Personal Data

Identification

Field	Type	Requirement	Response / reference
Full legal name	Free text	Required	
Former / other names	Free text	Required	
Date and place of birth	Free text	Required	
Nationality / nationalities	Free text	Required	
Identification type, number and expiry	Free text	Required	
Residential address and contact details	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Verification and profile

Field	Type	Requirement	Response / reference
Independent verification source	Free text	Required	
Verification date and result	Free text	Required	
Occupation / employer / business	Free text	Required	
Purpose of relationship	Free text	Required	
Expected source and destination of funds	Free text	Required	
Expected transaction profile	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Risk and approval

Field	Type	Requirement	Response / reference
Sanctions/PEP/adverse-media result	Free text	Required	
Risk factors and rating	Free text	Required	
CDD/EDD treatment	Free text	Required	
Open discrepancies	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Reviewer conclusion	Free text	Required	
Approval and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-05 - Legal Person or Arrangement CDD Record

Purpose	Establish legal existence, business, governance, ownership, control and expected activity.
Owner	KYC Operations
Approval	KYC Reviewer / MLRO for high risk
Classification	Confidential

Legal profile

Field	Type	Requirement	Response / reference
Legal name and trading name	Free text	Required	
Legal form and jurisdiction	Free text	Required	
Registration and licence	Free text	Required	
Registered and operating address	Free text	Required	
Business activity and purpose	Free text	Required	
Constitutional documents verified	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Governance and authority

Field	Type	Requirement	Response / reference
Directors / managers / trustees	Free text	Required	
Authorised representatives and authority	Free text	Required	
Ownership and control structure reference	Free text	Required	
Beneficial owners	Free text	Required	
Group and connected entities	Free text	Required	
Public or regulated status	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Relationship and decision

Field	Type	Requirement	Response / reference
Products and purpose	Free text	Required	
Expected activity and counterparties	Free text	Required	
Geographic exposure	Free text	Required	
Risk rating and EDD triggers	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Conditions / restrictions	Free text	Required	
Approval and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-06 - Beneficial Ownership Reconstruction and Verification

Purpose	Document direct and indirect ownership, control by other means and the natural-person conclusion.
Owner	KYC / EDD Analyst
Approval	KYC Manager / MLRO
Classification	Confidential

Structure

Field	Type	Requirement	Response / reference
Customer legal name and reference	Free text	Required	
Ownership chart reference	Free text	Required	
Each ownership layer and jurisdiction	Free text	Required	
Direct and indirect ownership calculations	Free text	Required	
Voting and appointment rights	Free text	Required	
Nominee, trust or control arrangements	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Natural persons

Field	Type	Requirement	Response / reference
Natural person identified	Free text	Required	
Basis: ownership / control / senior managing official	Free text	Required	
Applicable threshold and legal source	Free text	Required	
Identity verification source	Free text	Required	
PEP/sanctions screening result	Free text	Required	
Source of wealth relevance	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Conclusion

Field	Type	Requirement	Response / reference
Complexity and legitimate-purpose assessment	Free text	Required	
Discrepancies and resolution	Free text	Required	
Unresolved limitations	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
EDD or escalation required	Free text	Required	
Analyst conclusion	Free text	Required	
Independent review and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-07 - Customer Risk Rating Record

Purpose	Calculate and evidence the customer risk tier, overrides and required treatment.
Owner	KYC Risk Function
Approval	KYC Manager / MLRO
Classification	Confidential

Inputs

Field	Type	Requirement	Response / reference
Customer reference	Free text	Required	
Customer risk factors	Free text	Required	
Product/service/transaction factors	Free text	Required	
Delivery-channel factors	Free text	Required	
Geographic factors	Free text	Required	
Source dates and evidence	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Calculation

Field	Type	Requirement	Response / reference
Factor scores and weights	Free text	Required	
Base score and tier	Free text	Required	
Mandatory overrides	Free text	Required	
Prohibited criteria	Free text	Required	
Manual judgement and rationale	Free text	Required	
Final tier	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Treatment

Field	Type	Requirement	Response / reference
CDD intensity	Free text	Required	
Approval level	Free text	Required	
Monitoring treatment	Free text	Required	
Review frequency	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Conditions or restrictions	Free text	Required	
Reviewer and approval	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

F-08 - PEP and EDD Assessment

Purpose	Assess PEP category and other EDD triggers and record risk-specific enhanced measures.
Owner	EDD Team
Approval	MLRO / Senior Management
Classification	Strictly Confidential

Trigger and classification

Field	Type	Requirement	Response / reference
Customer / connected person	Free text	Required	
EDD trigger(s)	Free text	Required	
PEP category and public function	Free text	Required	
Jurisdiction and period in office	Free text	Required	
Family / close associate linkage	Free text	Required	
Adverse information	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Enhanced measures

Field	Type	Requirement	Response / reference
Additional identity/background evidence	Free text	Required	
Source of wealth evidence	Free text	Required	
Source of funds evidence	Free text	Required	
Legitimate-purpose assessment	Free text	Required	
Enhanced monitoring plan	Free text	Required	
Review frequency	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Decision

Field	Type	Requirement	Response / reference
Residual risk	Free text	Required	
Suspicion indicators considered	Free text	Required	
Conditions / restrictions	Free text	Required	
MLRO conclusion	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Senior management decision	Free text	Required	
Approval date and expiry/review	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-09 - Source of Wealth and Source of Funds Assessment

Purpose	Distinguish, corroborate and conclude on overall wealth and specific transaction funding.
Owner	EDD Analyst
Approval	MLRO / Authorised Approver
Classification	Strictly Confidential

Subject and transaction

Field	Type	Requirement	Response / reference
Customer / beneficial owner	Free text	Required	
Relationship or transaction reference	Free text	Required	
Amount, currency and date	Free text	Required	
Declared source of wealth	Free text	Required	
Declared source of funds	Free text	Required	
Reason assessment is required	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Evidence

Field	Type	Requirement	Response / reference
Wealth evidence obtained	Free text	Required	
Funds evidence obtained	Free text	Required	
Independent sources consulted	Free text	Required	
Calculation / plausibility analysis	Free text	Required	
Contradictory information	Free text	Required	
Evidence limitations	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Conclusion

Field	Type	Requirement	Response / reference
SoW corroborated?	Yes / Partly / No	Required	
SoF corroborated?	Yes / Partly / No	Required	
Consistency with profile	Free text	Required	

Field	Type	Requirement	Response / reference
Additional action / EDD / STR consideration	Free text	Required	
Analyst conclusion	Free text	Required	
Approval and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-10 - Sanctions Potential-Match Adjudication

Purpose	Provide a complete, independently reviewed record of a screening alert decision.
Owner	Sanctions Operations
Approval	Senior Sanctions Reviewer
Classification	Strictly Confidential

Alert

Field	Type	Requirement	Response / reference
Alert reference and time	Free text	Required	
Screening stage	Free text	Required	
Screened name / party	Free text	Required	
List entry and source	Free text	Required	
Transaction / relationship held	Free text	Required	
System score / match reason	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Identifiers and ownership

Field	Type	Requirement	Response / reference
Name and aliases comparison	Free text	Required	
Date of birth / incorporation	Free text	Required	
Nationality / jurisdiction	Free text	Required	
ID / registration number	Free text	Required	
Address / other identifiers	Free text	Required	
Ownership, control or indirect-benefit analysis	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Decision

Field	Type	Requirement	Response / reference
Classification	False positive / Potential / True match	Required	
Reason and evidence	Free text	Required	
Freeze / prohibit action	Free text	Required	
Competent-authority report	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Parallel STR consideration	Free text	Required	
Reviewer and time	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

F-11 - Targeted Financial Sanctions Freeze and Notification Record

Purpose	Evidence timely freezing, prohibition, notification, confidentiality and subsequent authority.
Owner	MLRO / Sanctions Officer
Approval	Authorised Executive / Legal where applicable
Classification	Strictly Confidential

Trigger

Field	Type	Requirement	Response / reference
True-match reference	Free text	Required	
Designated person/entity	Free text	Required	
Applicable list/decision	Free text	Required	
Date and time confirmed	Free text	Required	
Affected customer/parties	Free text	Required	
Known funds/economic resources	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Actions

Field	Type	Requirement	Response / reference
Systems and products frozen	Free text	Required	
Freeze date and time	Free text	Required	
Services prohibited	Free text	Required	
Branches/providers notified securely	Free text	Required	
Transaction holds	Free text	Required	
Access restrictions	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Reporting and follow-up

Field	Type	Requirement	Response / reference
Competent authority and channel	Free text	Required	
Submission time and receipt	Free text	Required	
Look-back scope and result	Free text	Required	
Release/authorisation reference	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Incident or leakage assessment	Free text	Required	
Final reviewer and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-12 - Transaction-Monitoring Alert Investigation

Purpose	Document the alert, expected-profile deviation, transaction reconstruction, typology and disposition.
Owner	Monitoring Analyst
Approval	Senior Monitoring Reviewer
Classification	Strictly Confidential

Alert and profile

Field	Type	Requirement	Response / reference
Alert reference and scenario	Free text	Required	
Customer and risk tier	Free text	Required	
Expected activity	Free text	Required	
Alerted activity	Free text	Required	
Deviation	Free text	Required	
Data-completeness check	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Investigation

Field	Type	Requirement	Response / reference
Chronology and transaction flow	Free text	Required	
Counterparties and geographies	Free text	Required	
CDD/BO/PEP/sanctions context	Free text	Required	
Prior alerts/STRs	Free text	Required	
Typology and red flags	Free text	Required	
Business explanation and evidence	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Disposition

Field	Type	Requirement	Response / reference
Known facts	Free text	Required	
Inferences and limitations	Free text	Required	
Closure rationale or suspicion basis	Free text	Required	
Internal escalation reference	Free text	Required	

Field	Type	Requirement	Response / reference
Control/data issue	Free text	Required	
Reviewer and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-13 - Internal Suspicion Disclosure

Purpose	Enable personnel to report suspected ML/TF/PF confidentially without requiring proof.
Owner	All Personnel
Approval	MLRO Office
Classification	Strictly Confidential - Need to Know

Reporter and subject

Field	Type	Requirement	Response / reference
Reporter name/role or protected reference	Free text	Required	
Date and time	Free text	Required	
Subject name and reference	Free text	Required	
Relationship / product	Free text	Required	
Connected parties	Free text	Required	
Urgency or transaction status	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Facts

Field	Type	Requirement	Response / reference
What occurred	Free text	Required	
Dates, amounts and currencies	Free text	Required	
Counterparties and jurisdictions	Free text	Required	
Expected behaviour	Free text	Required	
Observed deviation	Free text	Required	
Documents or systems consulted	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Concern

Field	Type	Requirement	Response / reference
Why the activity may be suspicious	Free text	Required	
Possible typology	Free text	Required	
Sanctions indicator?	Yes / No / Uncertain	Required	
Actions already taken	Free text	Required	

Field	Type	Requirement	Response / reference
Persons informed	Free text	Required	
Submission and receipt reference	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

F-14 - MLRO Report / No-Report Decision

Purpose	Record the independent reasoning, evidence and follow-up for every internal suspicion case.
Owner	MLRO
Approval	MLRO
Classification	Strictly Confidential - Need to Know

Case

Field	Type	Requirement	Response / reference
Internal case reference	Free text	Required	
Subjects and relationships	Free text	Required	
Source of referral	Free text	Required	
Date received	Free text	Required	
Urgent actions	Free text	Required	
Information limitations	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Analysis

Field	Type	Requirement	Response / reference
Verified factual chronology	Free text	Required	
Expected-activity deviation	Free text	Required	
Typology and predicate indicators	Free text	Required	
Legitimate explanation considered	Free text	Required	
Supporting and contradictory evidence	Free text	Required	
Suspicion threshold assessment	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Decision

Field	Type	Requirement	Response / reference
Decision	Report / Do not report / Further work	Required	
Reasoned conclusion	Free text	Required	
QFIU filing reference	Free text	Required	
Continued monitoring / restriction / exit	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Supplementary-report trigger	Free text	Required	
MLRO signature and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-15 - STR Filing Quality Checklist

Purpose	Confirm that a proposed STR is complete, factual, internally consistent and ready for the current QFIU channel.
Owner	Authorised STR Preparer
Approval	MLRO
Classification	Strictly Confidential - Need to Know

Subjects and relationship

Field	Type	Requirement	Response / reference
All subjects identified	Free text	Required	
Customer and account/contract references	Free text	Required	
Beneficial owners and connected parties	Free text	Required	
Relationship purpose and risk	Free text	Required	
Prior relevant reports	Free text	Required	
Identity documents attached	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Activity and analysis

Field	Type	Requirement	Response / reference
Chronological activity complete	Free text	Required	
Amounts, dates and currencies reconciled	Free text	Required	
Counterparties and jurisdictions	Free text	Required	
Typology named	Free text	Required	
Deviation clearly explained	Free text	Required	
Evidence list complete	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Submission

Field	Type	Requirement	Response / reference
Current QFIU form/channel verified	Free text	Required	
Tipping-off check complete	Free text	Required	
Attachments virus/quality checked	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
MLRO approval	Free text	Required	
Submission time and receipt	Free text	Required	
Follow-up owner	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-16 - Periodic and Trigger-Based Customer Review

Purpose	Evidence a substantive refresh of CDD, screening, activity, risk and continuation decision.
Owner	KYC Review Team
Approval	KYC Manager / MLRO for high risk
Classification	Confidential

Review initiation

Field	Type	Requirement	Response / reference
Customer and reference	Free text	Required	
Risk tier	Free text	Required	
Scheduled due date	Free text	Required	
Trigger event	Free text	Required	
Review scope	Free text	Required	
Reviewer	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Refresh

Field	Type	Requirement	Response / reference
Identity/registration current	Free text	Required	
Ownership/control changes	Free text	Required	
Authority changes	Free text	Required	
Screening results	Free text	Required	
Actual vs expected activity	Free text	Required	
Open conditions/findings	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Decision

Field	Type	Requirement	Response / reference
Updated risk rating	Free text	Required	
EDD refreshed	Free text	Required	
New monitoring/review treatment	Free text	Required	
Continue / restrict / remediate / exit	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Outstanding actions	Free text	Required	
Approval and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-17 - New Product, Technology and Channel AML Risk Assessment

Purpose	Assess financial-crime exposure, controls, test results and launch readiness.
Owner	Product Owner
Approval	Change Approval Committee
Classification	Internal - Controlled

Proposal

Field	Type	Requirement	Response / reference
Product/change name	Free text	Required	
Owner and sponsor	Free text	Required	
Target customers and markets	Free text	Required	
Transaction/funding flows	Free text	Required	
Channels and intermediaries	Free text	Required	
Planned launch date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Risk and controls

Field	Type	Requirement	Response / reference
ML risk scenario	Free text	Required	
TF risk scenario	Free text	Required	
PF/sanctions risk scenario	Free text	Required	
CDD/BO/CRR design	Free text	Required	
Screening/monitoring design	Free text	Required	
Data, records and contingency	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Readiness

Field	Type	Requirement	Response / reference
Test scenarios and results	Free text	Required	
Critical defects	Free text	Required	
Training and procedures	Free text	Required	
Residual risk and appetite	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Decision and conditions	Free text	Required	
Post-launch review date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

F-18 - AML/CFT/CPF Training and Competence Record

Purpose	Record role-based assignment, completion, assessment, remediation and practical competence.
Owner	Learning and Development
Approval	MLRO / Line Manager
Classification	Internal - Personal Data

Learner and role

Field	Type	Requirement	Response / reference
Employee name and ID	Free text	Required	
Role and business unit	Free text	Required	
Risk-critical duties	Free text	Required	
Required curriculum	Free text	Required	
Assignment trigger	Free text	Required	
Completion deadline	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Completion and assessment

Field	Type	Requirement	Response / reference
Module and version	Free text	Required	
Completion date	Free text	Required	
Assessment score	Free text	Required	
Pass threshold	Free text	Required	
Attempts	Free text	Required	
Scenario/practical result	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Competence

Field	Type	Requirement	Response / reference
Remediation required	Free text	Required	
Coaching / reassessment	Free text	Required	
Duty restriction	Free text	Required	
Manager competence conclusion	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Access decision	Free text	Required	
Final approval and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

F-19 - AML Control Breach, Near Miss and Exception

Purpose	Capture, risk-rate, contain and remediate a breach or lawful time-bound exception.
Owner	Incident Owner
Approval	MLRO / Legal / Authorised Executive
Classification	Restricted

Event

Field	Type	Requirement	Response / reference
Incident / exception reference	Free text	Required	
Date detected and period affected	Free text	Required	
Requirement/control	Free text	Required	
Affected customers/transactions/population	Free text	Required	
How detected	Free text	Required	
Reporter	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Risk and containment

Field	Type	Requirement	Response / reference
Condition and known facts	Free text	Required	
Potential legal/regulatory impact	Free text	Required	
Risk rating	Free text	Required	
Immediate containment	Free text	Required	
Look-back/reprocessing scope	Free text	Required	
Notification assessment	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Resolution

Field	Type	Requirement	Response / reference
Root cause	Free text	Required	
Corrective action and owner	Free text	Required	
Interim/compensating control	Free text	Required	
Target date / exception expiry	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Closure evidence	Free text	Required	
Independent validation	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

F-20 - Independent Assurance Finding and Remediation Tracker

Purpose	Record the 5Cs, risk rating, action ownership, evidence and independent closure validation.
Owner	Internal Audit / Independent Assurance
Approval	Audit Committee / Finding Owner
Classification	Internal - Restricted

Finding

Field	Type	Requirement	Response / reference
Engagement and finding reference	Free text	Required	
Process and control	Free text	Required	
Criteria	Free text	Required	
Condition	Free text	Required	
Root cause	Free text	Required	
Consequence / risk	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Assessment and action

Field	Type	Requirement	Response / reference
Risk rating and rationale	Free text	Required	
Recommendation	Free text	Required	
Management action	Free text	Required	
Accountable owner	Free text	Required	
Target date	Free text	Required	
Interim control	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Validation

Field	Type	Requirement	Response / reference
Evidence submitted	Free text	Required	
Implementation date	Free text	Required	
Operating period tested	Free text	Required	
Sample and acceptance result	Free text	Required	

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Field	Type	Requirement	Response / reference
Validator conclusion	Free text	Required	
Closure / reopen decision and date	Free text	Required	

Validation rule: Complete accurately and attach supporting evidence where applicable

Prepared by Ahmad Abumanei | ahmad.abumanie@outlook.com

Implementation, testing and approval checklist

No.	Acceptance requirement	Evidence / reference	Owner / date
1	The entity information table has been completed from verified registration, licence and governance records.		
2	A qualified Legal/MLRO review has confirmed the applicable national and sector instruments and identified unofficial translations.		
3	The EWRA reflects actual customer, product/service/transaction, channel and geographic exposure and separately considers ML, TF and PF.		
4	Customer acceptance, CDD, BO, PEP/EDD, sanctions, monitoring and STR controls are mapped to systems, owners, evidence and escalation.		
5	All internal decision fields, thresholds, service levels, review cycles, authority levels and risk appetite parameters have been approved.		
6	Data populations, screening and monitoring configurations, list updates, outages and critical workflows have been tested with acceptance criteria.		
7	Sector procedures, RACI assignments, forms and editable flowcharts have been adapted to the actual organisation and operating model.		
8	Role-based training and competence assessment were completed before personnel operated critical controls.		
9	Independent assurance tested both design and operating effectiveness and material findings were remediated or formally escalated.		
10	The governing body or authorised committee approved a controlled version and the entity withdrew superseded copies.		

Final limitations and professional-use notice

Not legal approval	This English document is a professional non-governmental draft. It is not a law, regulatory interpretation, licence condition, QFIU form or approval issued by a Qatari authority. The official Arabic legal text and current sector rules prevail.

Insurance and payments are not interchangeable. Life or investment-linked insurance, general insurance, wallets, merchant acquiring and technology platforms present different value flows and supervisory rules. The institution shall delete irrelevant material and verify all product definitions, thresholds, safeguarding and reporting requirements against the current QCB instrument.

Where entity information, system design, customer population, risk appetite or internal authorities were not supplied, the manual uses blank fields and professional control designs rather than invented facts. Those fields must be completed and tested before the document can support an assertion of compliance.

Prepared by

Name	Ahmad Abumanei
Email	ahmad.abumanie@outlook.com
Edition	English sector edition - Version 1.0
Verification cut-off	21 August 2026