AML/CFT POLICY AND MANUAL

VG MARKETS LIMITED

Anti-Money Laundering and Counter-Financing of Terrorism framework

September 2026

VGM-KM-POL-001 | Version 1.0

PO Box 1212, Hamchako, Mutsamudu, Autonomous Island of Anjouan, Union of Comoros

Company No. 16087 | International Brokerage and Clearing House Licence No. L16087/VGM

DOCUMENT CONTROL

Field	Detail
Document	AML/CFT Policy and Manual
Reference	VGM-KM-POL-001
Version	1.0
Status	Approved and in force
Entity	VG Markets Limited, Autonomous Island of Anjouan, Union of Comoros
Licence	International Brokerage and Clearing House Licence No. L16087/VGM
Regulator	Anjouan Offshore Finance Authority (AOFA)
Document owner	Money Laundering Reporting Officer / Compliance Officer
Approved by	Board of Directors
Effective date	1 September 2026
Review frequency	At least annually, and on any material change to the business, its customers, jurisdictions, products, payment arrangements or regulatory obligations
Next scheduled review	31 August 2027
Classification	Internal and confidential

READING THIS MANUAL

This Manual is the Company's principal financial crime document. It is supported by the **Client Acceptance and Onboarding Procedure** (VGM-KM-PRO-001) and the **Client Risk Assessment Policy and Methodology** (VGM-KM-POL-002), which together give operational effect to the requirements set out here. Where this Manual and a supporting procedure differ, the matter is to be escalated under clause 1.5 and resolved by formal amendment rather than by local practice.

This Manual is written for internal use. It does not form part of the Client Agreement and confers no rights on any client. Where a requirement in this Manual affects the Company's dealings with clients, the corresponding client-facing obligation is set out in the Client Agreement (VGM-LEG-CA-001), the Product Sheet (VGM-LEG-PS-001), the Risk Disclosure Statement (VGM-LEG-RDS-001) or the Privacy Policy (VGM-LEG-PP-001).

> *"Customer" and "Client" are used interchangeably in this Manual and in the supporting procedures. Both mean a Client as defined in the Client Agreement, together with any prospective client and, where the context requires, any beneficial owner, authorised person or controlling person connected with that client.*

1. AML/CFT POLICY STATEMENT

1.1 Policy Statement

VG Markets Limited ("VG Markets", the "Company") is committed to maintaining a robust and effective framework for preventing and detecting money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, corruption and other forms of financial crime.

VG Markets recognises that an international brokerage business may be exposed to financial crime risks through customer onboarding, account funding, withdrawals, trading activity, payment channels, third-party relationships, introducing arrangements, and cross-border transactions. The Company therefore adopts a risk-based approach under which financial crime risks are identified, assessed, managed, monitored and periodically reviewed.

The Company will not knowingly establish or maintain a business relationship where it cannot reasonably identify and verify the customer, understand the beneficial ownership and control structure, establish the nature and purpose of the relationship, or obtain sufficient information to manage the associated financial crime risks.

The Company shall maintain procedures designed to identify suspicious activity, investigate unusual or inconsistent customer behaviour, escalate material concerns to the Money Laundering Reporting Officer ("MLRO"), and make appropriate reports to the competent authority where required.

The Board of Directors recognises that responsibility for AML/CFT compliance ultimately rests with the Company and its senior management. Adequate resources, personnel, systems, training and oversight shall therefore be maintained to support the effective implementation of this Manual.

1.2 Regulatory Commitment

VG Markets operates as an international financial services business under an International Brokerage and Clearing House Licence issued by the Anjouan Offshore Finance Authority.

The Company's AML/CFT framework shall be developed and maintained having regard to the applicable laws and regulatory requirements of Anjouan, including the Money Laundering (Prevention) Act, Act 008 of 2005, together with applicable licence conditions, regulatory requirements and relevant international financial crime prevention standards.

The Anjouan AML legislation establishes obligations concerning customer and beneficial-owner identification, business-transaction records, attention to complex, unusual or large transactions and reporting of suspicious transactions. The legislation also establishes supervisory powers in relation to financial institutions.

The Company shall also have regard, where appropriate to its business and risk exposure, to internationally recognised AML/CFT principles and standards, including the recommendations and risk-based approach promoted by the Financial Action Task Force ("FATF").

1.3 Zero-Tolerance Approach to Deliberate Financial Crime

VG Markets has a zero-tolerance approach to knowingly facilitating money laundering, terrorist financing, sanctions evasion or other criminal activity.

The Company shall not knowingly:

- Establish anonymous or fictitious customer relationships;
- Deal with confirmed sanctioned persons or entities;
- Accept customers whose identity cannot reasonably be verified;
- Maintain relationships where beneficial ownership cannot reasonably be established;
- Accept unexplained or unverifiable sources of funds;
- Facilitate transactions that the Company knows or reasonably suspects are connected with criminal proceeds;
- Permit employees or third parties to circumvent AML/CFT controls.

A customer relationship may only be accepted where the risks have been appropriately assessed and are capable of being managed within the Company's risk appetite.

1.4 Risk-Based Approach

VG Markets does not apply identical AML/CFT controls to every customer or transaction. The Company recognises that financial crime risk varies according to factors such as customer type, geographic exposure, ownership structure, source of funds, source of wealth, products and services, transaction behaviour, delivery channels and other relevant circumstances.

The Company therefore applies enhanced controls to higher-risk customers and activities while maintaining appropriate baseline controls for all customers.

The Company's risk-based framework consists of:

1. Enterprise-wide ML/TF risk assessment;
2. Customer risk assessment;
3. Customer due diligence;
4. Enhanced due diligence;

5. Sanctions and PEP screening;
6. Ongoing customer due diligence;
7. Transaction monitoring;
8. Suspicious activity escalation and reporting;
9. Periodic compliance review;
10. Management oversight.

1.5 Application of the Manual

This Manual establishes the Company's overall AML/CFT framework. It should be read together with the Company's supporting policies and procedures, including:

- Client Acceptance and Onboarding Procedure;
- Client Risk Assessment Methodology;
- Enhanced Due Diligence Procedure;
- Sanctions Screening Procedure;
- Transaction Monitoring Procedure;
- Suspicious Transaction Reporting Procedure;
- Record Keeping Procedure;
- AML/CFT Training Program;
- Enterprise-Wide ML/TF Risk Assessment;
- Compliance Monitoring Program.

Where a conflict arises between this Manual and a specific operational procedure, the matter shall be escalated to the MLRO or Compliance Officer for determination and, where necessary, formal amendment of the relevant documents.

2. REGULATORY AND LEGAL FRAMEWORK

2.1 Purpose of the Regulatory Framework

VG Markets maintains a documented regulatory framework so that its AML/CFT controls can be traced to applicable legal and regulatory obligations. The purpose of this section is to establish the legal and regulatory basis for the Company's AML/CFT program and to ensure that employees understand the sources of the Company's obligations.

The regulatory framework shall be reviewed periodically to identify legislative, regulatory or international-standard changes that may require amendments to this Manual or related procedures.

2.2 Principal Anjouan AML Legislation

The principal AML legislation applicable to VG Markets' Anjouan operations is the Money Laundering (Prevention) Act, Act 008 of 2005.

The Act establishes money laundering as a criminal offence and imposes obligations on financial institutions in relation to customer identification, transaction records, suspicious transaction reporting and related financial crime controls. It also establishes supervisory powers and provides for investigation, freezing, forfeiture and international cooperation.

VG Markets shall maintain procedures designed to give practical effect to these requirements.

2.3 Anjouan Offshore Finance Authority

The Anjouan Offshore Finance Authority ("AOFA") is the statutory authority responsible for licensing and supervising international financial services conducted from the Autonomous Island of Anjouan.

AOFA states that its supervisory mandate includes continuing compliance with anti-money laundering obligations and that the supervisory authority may inspect business-transaction records and ask questions relevant to those records.

VG Markets shall therefore maintain its AML/CFT records and systems in a manner that enables the Company to demonstrate compliance during regulatory inspections, audits and other authorised reviews.

2.4 International Standards

VG Markets shall have regard to internationally recognised AML/CFT principles and standards to the extent relevant to its business and applicable legal obligations.

The Company's framework is intended to reflect the fundamental principles of:

- Risk identification and assessment;
- Customer due diligence;
- Beneficial ownership transparency;
- Enhanced measures for higher-risk relationships;
- Suspicious transaction reporting;
- Sanctions compliance;
- Record keeping;
- Employee training;
- Independent review;
- Senior management oversight.

AOFA itself states that its framework has regard to international AML standards and identifies FATF principles as an important benchmark for its supervisory framework.

2.5 Regulatory Change Management

The Compliance Officer shall monitor relevant legal and regulatory developments affecting the Company's AML/CFT obligations.

Where a material regulatory change is identified, Compliance shall:

1. Assess the impact on the Company's AML/CFT framework;
2. Identify affected policies and procedures;
3. Determine whether systems or controls require amendment;
4. Recommend appropriate changes to senior management;
5. Implement approved changes;
6. Communicate material changes to relevant employees;
7. Maintain evidence of the review and implementation.

The AML/CFT Manual shall be reviewed at least annually and more frequently where material legal, regulatory, business or risk changes occur.

3. AML/CFT GOVERNANCE AND RESPONSIBILITIES

3.1 Governance Framework

Effective AML/CFT compliance requires clear accountability throughout the organisation. VG Markets therefore maintains a governance structure under which the Board retains overall responsibility for the Company's AML/CFT framework, while operational responsibility is delegated to appropriately qualified personnel.

Delegation of responsibility does not remove the Board's ultimate responsibility for ensuring that appropriate AML/CFT systems and controls are established and maintained.

The governance framework shall provide:

- Clear allocation of responsibilities;
- Appropriate segregation of duties;
- Independent escalation channels;
- Adequate resources;
- Appropriate access to information;
- Senior management oversight;

- Regular compliance reporting.

3.2 Board of Directors

The Board of Directors has ultimate responsibility for the Company's AML/CFT framework and risk appetite.

The Board shall:

- Approve this Manual and material amendments;
- Approve the Company's AML/CFT risk appetite;
- Ensure adequate AML/CFT resources are available;
- Appoint appropriately qualified AML/CFT personnel;
- Receive regular reports from the MLRO;
- Review significant AML/CFT risks;
- Review material compliance breaches;
- Ensure appropriate remediation of identified deficiencies;
- Promote a culture of compliance throughout the Company.

The Board shall ensure that AML/CFT considerations form part of the Company's broader governance and risk management framework.

3.3 Money Laundering Reporting Officer

The MLRO shall have sufficient authority, independence, access to information and resources to perform the responsibilities assigned under this Manual.

The MLRO shall be responsible for overseeing the Company's AML/CFT framework and shall have authority to escalate material matters directly to the Board.

The MLRO's responsibilities include:

- Maintaining oversight of AML/CFT compliance;
- Reviewing internal suspicious activity reports;
- Determining whether external reporting is required;
- Managing suspicious transaction investigations;
- Approving High-Risk customer relationships where required;
- Overseeing EDD;
- Reviewing sanctions escalations;
- Monitoring compliance with AML/CFT procedures;
- Maintaining appropriate AML/CFT records;
- Reporting material matters to the Board;
- Coordinating regulatory responses relating to AML/CFT matters;
- Overseeing AML/CFT training.

The MLRO shall exercise independent judgement and shall not permit commercial considerations to override AML/CFT requirements.

3.4 Compliance Officer

The Compliance Officer shall support the MLRO and management in the day-to-day operation of the Company's AML/CFT framework.

Responsibilities include:

- Monitoring implementation of AML/CFT procedures;
- Conducting compliance reviews;
- Reviewing customer risk assessments;
- Monitoring KYC remediation;

- Reviewing screening controls;
- Conducting quality assurance testing;
- Maintaining regulatory obligations registers;
- Supporting AML/CFT training;
- Reporting control deficiencies to the MLRO.

The Compliance Officer shall escalate material deficiencies promptly.

3.5 KYC / Onboarding Personnel

Personnel responsible for customer onboarding shall conduct customer due diligence in accordance with the Client Acceptance and Onboarding Procedure.

They shall:

- Collect required customer information;
- Verify customer identity;
- Identify and verify beneficial owners;
- Conduct screening;
- Complete customer risk assessments;
- Obtain required source-of-funds information;
- Escalate unusual or suspicious circumstances;
- Ensure incomplete applications are not improperly approved.

KYC personnel must not knowingly override or bypass mandatory onboarding controls.

3.6 Operations and Client Services

Operations and Client Services personnel play an important role in identifying unusual customer activity because they may receive information concerning deposits, withdrawals, account changes and customer behaviour.

They shall promptly escalate to Compliance any activity that appears inconsistent with the customer's profile or otherwise raises reasonable financial crime concerns.

Employees must not inform customers that an internal suspicious activity review or potential suspicious transaction report is being considered.

3.7 Employees and Contractors

All employees and relevant contractors are responsible for complying with this Manual and associated AML/CFT procedures.

Personnel shall:

- Complete required AML/CFT training;
- Follow customer acceptance procedures;
- Protect confidential customer and AML information;
- Escalate suspicious or unusual activity;
- Maintain accurate records;
- Avoid tipping off customers;
- Cooperate with compliance reviews.

Failure to comply may result in disciplinary action and, where appropriate, termination of employment or engagement.

3.8 Segregation of Duties

VG Markets shall maintain appropriate segregation between customer onboarding, compliance review, transaction processing and senior management approval.

Where the Company's size or operating model does not permit complete functional separation, compensating controls shall be established and documented.

For example, the person responsible for initial KYC processing should not independently approve a High-Risk customer relationship without the required Compliance or MLRO review.

3.9 Outsourced AML/CFT Functions

Where AML/CFT functions are outsourced to a third-party service provider, VG Markets remains responsible for ensuring that the relevant controls operate effectively.

Before outsourcing a material AML/CFT function, the Company shall conduct appropriate due diligence on the service provider and establish:

- Scope of services;
- Responsibilities;
- Service standards;
- Information access;
- Record ownership;
- Reporting requirements;
- Audit rights;
- Regulatory access;
- Data protection requirements;
- Termination arrangements.

Outsourcing shall not prevent the Company, its auditors or competent authorities from obtaining information necessary to assess AML/CFT compliance.

4. ENTERPRISE-WIDE MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

4.1 Purpose

VG Markets shall maintain an Enterprise-Wide Money Laundering and Terrorist Financing Risk Assessment ("EWRA") to identify, assess and understand the financial crime risks arising from its business model.

The EWRA provides the foundation for the Company's risk-based AML/CFT framework and informs the design and intensity of customer due diligence, transaction monitoring, sanctions controls, training, compliance monitoring and resource allocation.

The EWRA shall consider the Company's specific characteristics as an international brokerage business rather than relying solely on generic industry risk assessments.

4.2 Risk Assessment Methodology

The Company shall assess inherent financial crime risks before considering the effectiveness of existing controls.

The assessment shall consider, at a minimum:

Customer Risk

The Company shall assess risks associated with:

- Individual customers;
- Corporate customers;
- High-net-worth customers;
- Professional customers;
- Introducing arrangements;
- Customers with complex ownership structures.

Geographic Risk

The Company shall consider:

- Customer residence;
- Customer nationality;

- Country of incorporation;
- UBO residence;
- Source of funds jurisdiction;
- Payment destination;
- Trading activity involving higher-risk jurisdictions.

Product and Service Risk

The Company shall consider risks associated with:

- FX trading;
- CFD trading;
- Derivative products;
- Leverage;
- Deposits and withdrawals;
- Cross-border payments;
- Payment service providers;
- Any virtual-asset-related funding or payment arrangements permitted by the Company.

Distribution and Delivery Channel Risk

The Company shall consider risks arising from:

- Online onboarding;
- Non-face-to-face relationships;
- Electronic identification;
- Introducing Brokers;
- Third-party service providers;
- Outsourced onboarding services.

Transaction Risk

The Company shall assess:

- Deposit values;
- Withdrawal patterns;
- Frequency of transactions;
- Third-party payments;
- Rapid movement of funds;
- Multiple payment methods;
- Transactions inconsistent with customer profiles.

4.3 Inherent Risk Assessment

For each material risk category, the Company shall assign an inherent risk rating before considering mitigating controls.

The Company may use the following rating scale:

Rating	Description
1	Low
2	Low-Medium
3	Medium
4	Medium-High

Rating	Description
5	High

The assessment shall consider both the likelihood and potential impact of the relevant risk.

A documented rationale shall be maintained for material risk ratings.

4.4 Control Effectiveness Assessment

Following the assessment of inherent risk, the Company shall assess the effectiveness of its existing controls.

Controls may include:

- Customer identification;
- Beneficial ownership verification;
- PEP screening;
- Sanctions screening;
- Customer risk scoring;
- Transaction monitoring;
- EDD;
- Payment controls;
- Staff training;
- Compliance monitoring;
- Independent review.

Control effectiveness may be classified as:

- Effective;
- Generally Effective;
- Partially Effective;
- Ineffective.

Where controls are found to be ineffective or partially effective, remediation actions shall be documented and assigned to responsible persons.

4.5 Residual Risk

Residual risk represents the level of risk remaining after consideration of the Company's mitigating controls.

The Company shall determine whether residual risk is:

- Low;
- Medium;
- High;
- Outside Risk Appetite.

Where residual risk exceeds the Company's approved risk appetite, management shall determine whether additional controls, restrictions or business changes are required.

The Company shall not rely solely on numerical scoring. Professional judgement and qualitative factors must be considered where appropriate.

4.6 Risk Appetite

VG Markets shall maintain a documented AML/CFT risk appetite.

The Company shall not knowingly establish or maintain relationships involving:

- Confirmed sanctions matches;
- Anonymous customers;

- Unidentified beneficial owners;
- Prohibited jurisdictions;
- Shell banks;
- Criminal activities;
- Circumstances where customer identity cannot reasonably be established;
- Circumstances where material financial crime risks cannot be adequately mitigated.

The Company may apply enhanced controls to higher-risk relationships where the risks can be effectively managed and the relationship falls within the Company's approved risk appetite.

4.7 Brokerage-Specific Financial Crime Risks

Because VG Markets operates an international brokerage business, the EWRA shall specifically consider risks associated with the movement of funds into and out of trading accounts.

Particular attention shall be given to:

- Third-party deposits;
- Third-party withdrawals;
- Rapid deposit and withdrawal activity;
- Deposits followed by limited or no trading;
- Multiple payment instruments;
- Multiple unrelated bank accounts;
- Unusual changes in trading behaviour;
- Transactions inconsistent with declared income or wealth;
- Customers attempting to circumvent funding restrictions;
- Use of payment channels inconsistent with the customer's country of residence;
- Unusual activity involving high-risk jurisdictions.

These indicators shall not automatically constitute evidence of money laundering. Rather, they shall be considered risk indicators requiring further review where appropriate.

4.8 Risk Assessment Frequency

The EWRA shall be reviewed at least annually.

An interim review shall be conducted where there is a material change in:

- Products or services;
- Customer base;
- Geographic markets;
- Payment channels;
- Business model;
- Regulatory requirements;
- Technology;
- Outsourcing arrangements;
- Material financial crime threats.

The MLRO shall document the date, scope, findings and approval of each EWRA review.

4.9 Board Approval and Reporting

The EWRA shall be approved by the Board or an appropriately authorised senior management body.

Material findings shall be reported to the Board, including:

- Significant changes in risk exposure;
- Emerging financial crime risks;

- Material control deficiencies;
- High-risk customer trends;
- Significant suspicious activity;
- Sanctions exposure;
- Remediation requirements.

The Board shall ensure that identified risks are appropriately addressed and that sufficient resources are allocated to manage the Company's AML/CFT risk exposure.

4.10 Documentation and Evidence

VG Markets shall maintain sufficient documentation to demonstrate how the EWRA was performed.

The assessment file should contain:

- Risk assessment methodology;
- Risk factors;
- Data used;
- Risk scoring;
- Control assessment;
- Residual risk;
- Management judgement;
- Identified deficiencies;
- Remediation plan;
- Board approval.

The EWRA must be sufficiently detailed that an independent reviewer or regulator can understand how the Company arrived at its conclusions.

5. CUSTOMER DUE DILIGENCE AND KNOW YOUR CUSTOMER

5.1 Purpose and Policy

Customer Due Diligence (“CDD”) is the principal control through which VG Markets establishes who its customers are, who ultimately owns or controls them, why they require the Company's services, how they are expected to fund and use their accounts, and whether the relationship presents risks that can be appropriately managed.

VG Markets shall conduct CDD on a risk-sensitive basis before establishing a customer relationship and shall maintain sufficient information throughout the relationship to ensure that the Company's understanding of the customer remains current and reasonable. CDD shall not be treated as a one-time administrative exercise. Customer information shall be refreshed and reassessed when required by the customer's risk profile or when circumstances change.

VG Markets shall not knowingly maintain an anonymous or fictitious customer relationship, and shall not establish or continue a relationship where the Company cannot satisfactorily establish the identity of the customer or, where applicable, its beneficial owner.

AOFA identifies customer identification and verification, including identification of beneficial owners, as fundamental AML obligations for licensed institutions.

5.2 When CDD Must Be Performed

CDD shall be completed before account activation and before the customer is permitted to use the Company's services, unless a specific legal or operational exception has been approved by the MLRO and documented.

CDD shall also be performed or refreshed when:

- there is a material change in the customer's circumstances;
- ownership or control of a corporate customer changes;
- the customer changes its country of residence or incorporation;

- there is a material change in expected account activity;
- unusual or potentially suspicious transactions are identified;
- there is doubt concerning previously obtained identification information;
- sanctions or PEP screening generates a relevant alert;
- adverse information concerning the customer or beneficial owner is identified;
- the customer's risk classification changes;
- the existing information is no longer considered sufficiently reliable; or
- a periodic review becomes due.

5.3 Individual Customers

For individual customers, VG Markets shall obtain sufficient information to establish and verify, as appropriate:

- full legal name;
- date of birth;
- nationality;
- residential address;
- country of residence;
- identification document details;
- occupation or principal business activity;
- expected nature and purpose of the account;
- expected trading and funding activity;
- source of funds;
- source of wealth where appropriate;
- tax residency and other information required for applicable regulatory or tax purposes;
- PEP status;
- sanctions status; and
- any other information necessary to understand the customer's financial crime risk.

Identity documents shall be independently reviewed for validity, authenticity and consistency with information provided by the customer.

5.4 Corporate and Legal Entity Customers

For corporate and other legal entity customers, VG Markets shall obtain sufficient information to understand the legal existence, ownership, control and business activities of the customer.

This shall generally include:

- certificate of incorporation or equivalent;
- registered office;
- principal place of business;
- constitutional documents;
- register of shareholders or equivalent ownership information;
- register of directors or equivalent;
- ownership structure;
- beneficial ownership information;
- identification of directors and authorised representatives;
- identification of beneficial owners;
- nature of business;
- expected account activity;

- source of funds;
- source of wealth where appropriate;
- relevant licences or regulatory status;
- countries in which the entity operates;
- expected funding and withdrawal arrangements; and
- any other information necessary to understand the entity's financial crime risk.

Where the corporate structure contains multiple layers of ownership, VG Markets shall take reasonable steps to understand the ownership chain through to the ultimate natural person or persons exercising ownership or control.

5.5 Verification of Identity

Verification shall be based on reliable and independent documentation, data or information.

The Company may use appropriate electronic verification systems, documentary verification, independent corporate registries, regulated third-party databases and other reliable sources, provided that the method used is appropriate to the customer's risk profile.

Where electronic verification is inconclusive, unavailable or inconsistent with other information, additional documentary evidence shall be obtained.

The level of verification shall be proportionate to the customer's risk.

5.6 Non-Face-to-Face Relationships

Because VG Markets operates an international brokerage business in which customers may be onboarded remotely, non-face-to-face onboarding is recognised as an inherent financial crime risk.

The absence of face-to-face contact shall therefore be incorporated into the customer risk assessment.

Additional controls may include:

- enhanced electronic identity verification;
- liveness or biometric verification where available;
- verification of address;
- additional independent data sources;
- enhanced sanctions and adverse media screening;
- verification of source of funds;
- additional verification before withdrawals;
- restrictions on third-party funding;
- enhanced review of unusual account activity.

Non-face-to-face onboarding shall not automatically result in rejection; rather, the associated risk shall be identified and appropriately controlled.

5.7 Reliance on Third Parties

VG Markets may rely on third-party service providers for specific verification functions where appropriate, such as identity verification, sanctions screening or corporate information.

However, outsourcing a verification function shall not transfer ultimate responsibility for AML compliance from VG Markets.

The Company shall ensure that appropriate contractual arrangements, audit rights, data access, service standards and regulatory access are maintained.

5.8 Failure to Complete CDD

Where required CDD cannot be satisfactorily completed, VG Markets shall not activate the account or shall restrict or terminate the relationship as appropriate.

The matter shall be escalated to the MLRO where the failure to complete CDD is associated with unexplained behaviour, inconsistent information, suspected document manipulation, refusal to provide information, unexplained ownership structures or other potential financial crime indicators.

Where the circumstances give rise to suspicion, the matter shall be handled in accordance with the suspicious transaction escalation and reporting procedures.

6. BENEFICIAL OWNERSHIP AND CONTROL

6.1 Purpose

Beneficial ownership transparency is a fundamental component of VG Markets' AML framework. The Company must understand not merely the name of the legal customer, but the natural person or persons who ultimately own or control the customer or on whose behalf the relationship is maintained.

AOFA expressly identifies beneficial-owner identification as mandatory, including where a customer acts through a nominee, agent or intermediary.

6.2 Identification of Beneficial Owners

For corporate customers, VG Markets shall identify the natural person or persons who ultimately:

- own the customer;
- exercise effective control over the customer;
- control management decisions; or
- otherwise exercise ultimate effective control.

As an internal operational standard, VG Markets will generally apply a 25% ownership or control threshold when identifying ownership interests, while recognising that ownership percentage alone does not determine beneficial ownership.

Where no individual can be identified solely through ownership, the Company shall consider control through voting rights, shareholder agreements, management arrangements, contractual rights or other means.

6.3 Ownership Chains

Where a customer is owned by another legal entity, the ownership chain shall be traced through each relevant entity until the ultimate natural persons are identified.

The Company shall not accept a corporate structure merely because the immediate shareholder has been identified.

Where ownership involves:

- offshore entities;
- trusts;
- foundations;
- nominee shareholders;
- private investment vehicles;
- multiple corporate layers;
- bearer-share arrangements where relevant;
- fiduciary arrangements; or
- jurisdictions presenting elevated transparency risk,

additional information shall be obtained and EDD may be required.

6.4 Control Where No 25% Owner Exists

If no natural person owns or controls 25% or more of the customer, VG Markets shall identify the person or persons exercising effective control through other means.

If no individual can reasonably be identified after appropriate investigation, the Company shall document the basis on which the relevant senior managing official or equivalent controlling person is identified for CDD purposes.

The rationale shall be recorded in the customer file.

6.5 Nominees, Agents and Intermediaries

Where a customer acts through a nominee, agent, representative or other intermediary, VG Markets shall establish:

1. the identity of the legal customer;
2. the identity of the intermediary;
3. the authority under which the intermediary acts;
4. the identity of the beneficial owner;
5. the purpose of the arrangement; and
6. whether the arrangement creates additional financial crime risk.

The use of a nominee or intermediary shall not prevent VG Markets from identifying the ultimate beneficial owner.

6.6 Verification

Beneficial ownership information shall be verified using appropriate independent sources.

For corporate customers this may include:

- corporate registries;
- certified corporate documents;
- shareholder registers;
- ownership charts;
- constitutional documents;
- trust deeds;
- partnership agreements;
- reliable commercial databases;
- independent legal or professional documentation; and
- other reliable sources.

The verification method and evidence obtained shall be documented.

6.7 Inability to Identify Beneficial Ownership

VG Markets shall not establish or continue a customer relationship where it cannot reasonably establish who ultimately owns or controls the customer or otherwise understand the ownership and control structure.

Where the inability to establish beneficial ownership appears deliberate or suspicious, the matter shall be escalated to the MLRO.

7. POLITICALLY EXPOSED PERSONS

7.1 Purpose

Politically Exposed Persons (“PEPs”) may present heightened exposure to bribery, corruption, abuse of public office and proceeds of corruption. PEP status shall therefore be incorporated into VG Markets' customer risk assessment.

PEP status shall not, by itself, constitute a reason for automatic rejection. The purpose of the control is to identify and manage the additional risk through appropriate enhanced due diligence.

7.2 Identification

VG Markets shall conduct appropriate screening to identify whether a customer, beneficial owner, director, authorised representative or other relevant connected person is a PEP.

Screening shall cover, as appropriate:

- foreign PEPs;
- domestic PEPs;
- international organisation PEPs;
- family members of PEPs; and
- known close associates of PEPs.

7.3 PEP Risk Assessment

Where a PEP relationship is identified, VG Markets shall consider:

- the nature of the person's public position;
- the jurisdiction involved;
- the level of political influence;
- the person's source of wealth;
- source of funds;
- expected account activity;
- business interests;
- family and close-associate relationships where relevant;
- adverse media;
- corruption indicators;
- sanctions exposure; and
- other relevant risk factors.

7.4 Enhanced Due Diligence

PEP relationships shall generally be subject to enhanced controls proportionate to the risk, including enhanced source-of-wealth and source-of-funds verification where appropriate.

As an internal control, VG Markets shall require appropriate senior management approval before establishing or continuing a higher-risk PEP relationship.

The approval shall be documented and shall not be treated as a substitute for CDD or EDD.

7.5 Ongoing Monitoring

PEP customers shall be subject to enhanced ongoing monitoring.

The Company shall promptly reassess the relationship where:

- the customer obtains a new public position;
- the customer's political status changes;
- adverse information is identified;
- transaction activity materially changes; or
- source of wealth or funds becomes inconsistent with the Company's understanding.

8. SANCTIONS SCREENING

8.1 Purpose

VG Markets maintains sanctions controls to prevent the Company from providing services to persons or entities subject to applicable financial sanctions and to identify potential sanctions evasion.

AOFA's current regulatory materials state that licensees must screen against United Nations sanctions measures and other sanctions regimes applicable to their business and act on a match without delay.

8.2 Screening Scope

Sanctions screening shall, as appropriate, cover:

- customers;
- beneficial owners;
- directors;
- authorised representatives;
- relevant counterparties;

- payment beneficiaries;
- payment senders;
- introducers or intermediaries; and
- other persons relevant to a transaction or relationship.

VG Markets may use additional international sanctions lists as an internal risk-management control where relevant to its business, counterparties, banking arrangements or customer base.

8.3 Screening at Onboarding

Sanctions screening shall be performed before account activation.

No customer shall be activated where a potential sanctions match has not been appropriately resolved.

8.4 Ongoing Screening

Customers and relevant connected persons shall be screened periodically and against material changes to sanctions lists where the Company's screening system supports ongoing or event-driven screening.

8.5 Potential Match

A potential match shall not automatically be treated as a confirmed sanctions match.

The Compliance function shall conduct appropriate review, considering:

- full name;
- date of birth;
- nationality;
- country of residence;
- address;
- entity registration information;
- ownership information;
- other identifiers.

The rationale for clearing or escalating the alert shall be recorded.

8.6 Confirmed or Unresolved Match

Where a potential match cannot be reasonably cleared, the account shall be escalated immediately to the MLRO or designated senior compliance officer.

The Company shall consider whether:

- onboarding must be stopped;
- transactions must be suspended;
- withdrawals or deposits must be restricted;
- assets must be frozen where legally required;
- external reporting is required; and
- legal advice or regulatory guidance is required.

No employee shall inform the customer that a suspicious activity or sanctions investigation is being conducted where doing so could constitute prohibited tipping off or otherwise prejudice an investigation.

9. SOURCE OF FUNDS AND SOURCE OF WEALTH

9.1 Purpose

Understanding the customer's Source of Funds (“SoF”) and, where relevant, Source of Wealth (“SoW”) enables VG Markets to determine whether the customer's financial profile is consistent with the expected activity and whether the funds entering the brokerage relationship appear legitimate.

The depth of verification shall be proportionate to the customer's risk.

9.2 Source of Funds

Source of Funds refers to the origin of the particular money or assets being used for a transaction or account.

Examples may include:

- employment income;
- business income;
- investment proceeds;
- dividends;
- sale of property;
- inheritance;
- loan proceeds;
- corporate treasury funds;
- investment portfolio liquidation; or
- other legitimate sources.

The Company shall distinguish between the source of the money used for the transaction and the customer's overall wealth.

9.3 Source of Wealth

Source of Wealth refers to the origin of the customer's overall accumulated wealth.

Depending on the customer profile, evidence may include:

- employment history;
- business ownership;
- audited financial statements;
- investment records;
- property transactions;
- inheritance documentation;
- dividend records;
- sale of a business;
- tax or financial records;
- credible public information; or
- other reliable evidence.

9.4 When Enhanced Verification Is Required

Enhanced SoF/SoW verification should generally be considered where:

- the customer is high risk;
- the customer is a PEP;
- the transaction size is inconsistent with the customer's profile;
- the customer is involved in a high-risk industry;
- wealth is derived from complex offshore structures;
- funds originate from unrelated third parties;
- the customer uses multiple payment channels;
- the customer's stated income does not reasonably support the activity; or
- adverse information raises concerns regarding the legitimacy of wealth.

9.5 Third-Party Funding

Third-party deposits shall be restricted and subject to enhanced review in accordance with VG Markets' payment controls.

Where third-party funding is permitted, the Company shall establish:

- identity of the third-party payer;
- relationship between payer and customer;
- reason for the payment;
- source of funds;
- whether the payment is consistent with the customer's profile; and
- whether any sanctions, fraud or financial crime concerns exist.

Where the third party cannot be satisfactorily identified or the purpose of the payment cannot reasonably be established, the payment shall be escalated and may be rejected or returned in accordance with applicable procedures.

9.6 Unexplained Funds

The existence of unexplained funds shall be treated as a risk indicator rather than automatically as evidence of criminal activity.

However, where the explanation and supporting evidence are inadequate, the Company shall not simply rely on the customer's verbal explanation. The matter shall be escalated for enhanced review.

10. ENHANCED DUE DILIGENCE

10.1 Purpose

Enhanced Due Diligence ("EDD") applies where the customer, transaction, jurisdiction, product, delivery channel or other circumstance presents elevated ML/TF or financial crime risk.

EDD is intended to provide the Company with a deeper understanding of the customer and to determine whether the relationship can reasonably be accepted within VG Markets' risk appetite.

10.2 Circumstances Requiring EDD

EDD may be required for:

- high-risk customers;
- PEPs;
- complex ownership structures;
- trusts and foundations;
- nominee arrangements;
- customers from higher-risk jurisdictions;
- high-risk occupations or industries;
- customers with significant adverse media;
- unusual funding patterns;
- third-party funding;
- unexplained wealth;
- high-value or unusual transactions;
- customers using multiple payment instruments;
- suspected attempts to circumvent restrictions;
- customers with significant virtual-asset exposure where relevant;
- unexplained rapid movement of funds; and
- other circumstances identified through the risk assessment or monitoring process.

10.3 EDD Measures

Depending on the circumstances, EDD may include:

- additional identity verification;
- additional beneficial ownership evidence;
- detailed corporate structure review;
- enhanced adverse media searches;
- enhanced sanctions screening;
- independent verification of business activities;
- detailed SoF verification;
- detailed SoW verification;
- bank statements or equivalent financial evidence;
- tax or financial records;
- verification of expected trading activity;
- senior management approval;
- increased transaction monitoring;
- more frequent customer reviews; and
- restrictions on particular funding or withdrawal methods.

10.4 EDD Decision

Completion of EDD does not automatically require acceptance.

The Company shall assess whether the identified risk can be effectively managed within its risk appetite.

Where the residual risk remains outside risk appetite, the relationship shall be rejected, restricted or terminated as appropriate.

10.5 EDD Documentation

The customer file shall clearly document:

- why EDD was triggered;
- information requested;
- evidence received;
- analysis performed;
- unresolved issues;
- decision taken;
- person approving the decision; and
- any ongoing restrictions or monitoring requirements.

11. ONGOING CUSTOMER DUE DILIGENCE AND PERIODIC REVIEW

11.1 Purpose

Customer Due Diligence does not end when an account is opened. VG Markets shall maintain an ongoing understanding of its customers and shall periodically reassess whether the customer's identity, ownership, source of funds, source of wealth, expected activity and overall risk profile remain accurate and appropriate.

Ongoing monitoring is particularly important for an international brokerage business because the financial crime risk associated with a customer may become apparent only after trading and payment activity commences. The Company's ongoing CDD framework therefore combines periodic customer reviews with event-driven reviews arising from changes in customer circumstances, transaction behaviour, screening results or other risk indicators.

11.2 Periodic Review

Customers shall be subject to periodic review based on their assigned risk classification.

As an internal control, VG Markets will generally apply the following review cycle:

Customer Risk	Minimum Review Frequency
Low	Every 36 months
Medium	Every 24 months
High	Every 12 months
PEP / enhanced-risk customer	At least every 12 months
Trigger event	Immediately or as soon as reasonably practicable

The review frequency may be increased where the MLRO or Compliance Officer considers the customer's risk to warrant more frequent review.

11.3 Event-Driven Review

A customer review shall be initiated outside the normal review cycle where a material trigger event occurs.

Examples include:

- change of beneficial ownership;
- change of directors or controlling persons;
- change of country of residence;
- change of business activity;
- material increase in account turnover;
- significant deposits inconsistent with the customer's profile;
- unusual withdrawals;
- third-party funding;
- sanctions alert;
- PEP identification;
- adverse media;
- law-enforcement or regulatory request;
- unusual trading behaviour;
- unexplained changes in payment methods;
- suspected account takeover;
- suspicious activity indicators; or
- any other event that materially changes the customer's risk.

11.4 Review of Customer Information

The reviewer shall determine whether the existing customer file remains complete and accurate.

Depending on the customer's risk, the review may include:

- identity documents;
- residential or registered address;
- occupation/business activity;
- corporate documents;
- ownership structure;
- beneficial ownership;
- PEP status;
- sanctions status;

- adverse media;
- source of funds;
- source of wealth;
- expected trading activity;
- payment methods;
- transaction history; and
- previous compliance alerts.

11.5 Risk Reassessment

The customer risk rating shall be reconsidered during each periodic review and following material trigger events.

The revised assessment shall document:

- current risk factors;
- changes since the previous assessment;
- effectiveness of existing controls;
- transaction behaviour;
- new risk indicators;
- residual risk; and
- resulting risk classification.

Where the customer's risk increases, the Company shall apply additional controls without waiting for the next scheduled review.

11.6 Failure to Provide Updated Information

Where a customer fails to provide information reasonably required for an ongoing CDD review, VG Markets may restrict account activity, suspend certain services or terminate the relationship, depending on the circumstances.

Where refusal or avoidance appears deliberate or suspicious, the matter shall be escalated to the MLRO.

12. TRANSACTION MONITORING

12.1 Purpose

Transaction monitoring is designed to identify activity that is inconsistent with the Company's understanding of a customer or that may indicate money laundering, terrorist financing, fraud, sanctions evasion or other financial crime.

VG Markets shall maintain transaction-monitoring controls proportionate to the nature, scale and complexity of its brokerage business.

AOFA specifically requires licensed institutions to pay special attention to complex, unusual or large transactions.

12.2 Scope of Monitoring

Monitoring shall, to the extent relevant to the Company's systems and business model, cover:

- deposits;
- withdrawals;
- transfers;
- payment method changes;
- third-party payments;
- trading activity;
- account turnover;
- rapid movement of funds;
- multiple payment instruments;

- changes in account behaviour;
- linked accounts;
- unusual geographic activity;
- potentially sanctioned counterparties; and
- other activity relevant to financial crime risk.

12.3 Customer Profile Comparison

Transaction activity shall be considered against the customer's known profile.

The Company shall consider whether activity is consistent with:

- occupation;
- stated income;
- source of wealth;
- source of funds;
- residence;
- business activity;
- expected trading activity;
- historical account behaviour; and
- assigned risk classification.

An unusual transaction does not automatically constitute suspicious activity. It is an indicator requiring appropriate review.

12.4 Brokerage-Specific Indicators

VG Markets shall maintain awareness of indicators particularly relevant to FX/CFD brokerage activity, including:

- substantial deposits followed by little or no genuine trading;
- rapid deposits followed by withdrawals;
- repeated deposits and withdrawals over short periods;
- withdrawals to accounts unrelated to the customer;
- third-party deposits;
- use of multiple unrelated payment methods;
- frequent changes of payment instruments;
- activity inconsistent with stated income or wealth;
- unusual activity involving high-risk jurisdictions;
- attempts to circumvent payment restrictions;
- splitting transactions to avoid internal controls;
- use of multiple related trading accounts;
- unusual transfers between apparently connected customers;
- unexplained use of corporate accounts for personal trading;
- unusual activity immediately following account restrictions;
- repeated failed payment attempts;
- suspected use of another person's payment instrument; and
- behaviour suggesting that the trading account is being used primarily as a payment or value-transfer mechanism.

12.5 Automated Monitoring

Where automated monitoring systems are used, VG Markets shall maintain appropriate rules, thresholds and alert configurations.

The Company shall periodically assess whether monitoring scenarios remain appropriate considering:

- customer population;
- transaction volumes;
- products;
- payment channels;
- jurisdictions;
- emerging financial crime risks; and
- historical alerts.

Automated monitoring shall not replace human judgement.

12.6 Manual Monitoring

Where automated monitoring is unavailable or insufficient, Compliance and Operations shall apply documented manual monitoring procedures.

Manual monitoring may include periodic review of:

- high-value transactions;
- unusual deposits and withdrawals;
- high-risk customer accounts;
- third-party payments;
- unusual payment destinations;
- customer complaints involving payment activity; and
- other risk-based samples.

12.7 Alert Management

Each material transaction-monitoring alert shall be:

1. recorded;
2. assigned to an appropriate reviewer;
3. investigated within a reasonable timeframe;
4. supported by relevant customer and transaction information;
5. documented with the reviewer's rationale; and
6. escalated where concerns remain.

Alerts shall not be closed merely because the transaction is commercially reasonable or because the customer provides an unsupported explanation.

12.8 Escalation

Where monitoring identifies potentially suspicious activity, the matter shall be escalated to the MLRO.

The MLRO shall determine whether:

- additional information is required;
- enhanced due diligence is appropriate;
- the customer's risk rating should change;
- account restrictions are necessary;
- further monitoring is required;
- the relationship should be terminated; or
- an external suspicious transaction report should be considered.

13. SUSPICIOUS TRANSACTION IDENTIFICATION, ESCALATION AND REPORTING

13.1 Purpose

VG Markets shall maintain procedures to ensure that suspicions of money laundering, terrorist financing or other relevant financial crime are identified, documented, escalated and reported to the appropriate competent authority where required.

The Company's internal process shall distinguish between:

- an unusual transaction;
- a transaction requiring investigation; and
- a transaction giving rise to a reasonable suspicion requiring escalation and potential external reporting.

The existence of an unusual transaction alone does not necessarily mean that money laundering has occurred.

13.2 Sources of Suspicion

A suspicion may arise from:

- customer onboarding;
- transaction monitoring;
- sanctions screening;
- adverse media;
- customer behaviour;
- payment activity;
- employee observations;
- complaints;
- third-party information;
- law-enforcement enquiries;
- regulatory requests;
- changes in beneficial ownership;
- unusual trading behaviour; or
- other internal or external information.

13.3 Internal Escalation

Employees who identify potentially suspicious activity shall promptly escalate the matter through the Company's internal AML escalation process.

Employees shall not attempt to independently determine whether an external suspicious transaction report should be filed.

The matter shall be referred to the MLRO or designated AML decision-maker.

13.4 MLRO Investigation

The MLRO shall conduct an appropriate review based on the available information.

The investigation may consider:

- customer identification information;
- beneficial ownership;
- transaction history;
- deposit and withdrawal history;
- trading activity;
- source of funds;
- source of wealth;
- payment counterparties;
- geographic exposure;

- sanctions results;
- adverse media;
- previous alerts;
- explanations provided by the customer; and
- other relevant information.

The investigation shall be proportionate to the circumstances.

13.5 Suspicion Assessment

The MLRO shall determine whether the available information gives rise to a reportable suspicion under applicable law.

The decision shall be documented regardless of whether a report is ultimately made.

The file should record:

- the initial trigger;
- information reviewed;
- analysis performed;
- relevant risk factors;
- conclusion;
- reporting decision;
- date of decision; and
- MLRO or authorised decision-maker.

13.6 External Reporting

Where the applicable legal threshold for reporting is met, VG Markets shall make the required report to the competent Supervisory Authority in accordance with applicable law and procedure.

AOFA's current materials state that licensed institutions must report suspicions promptly to the Supervisory Authority and that good-faith reporting is protected from liability.

The Company shall not delay a required report merely because the internal investigation is incomplete, where the applicable law requires prompt reporting.

13.7 No Customer Notification

The Company shall not disclose to the customer, or to another unauthorised person, that:

- a suspicious activity investigation is being conducted;
- a suspicious transaction report has been made;
- a report is being considered; or
- information has been provided to a competent authority,

where such disclosure would constitute prohibited tipping off or otherwise prejudice an investigation.

13.8 Good-Faith Reporting

Employees and officers who escalate concerns in good faith shall not be disadvantaged for doing so.

Commercial considerations, customer complaints or potential revenue loss shall not override AML escalation obligations.

14. TIPPING-OFF AND CONFIDENTIALITY

14.1 Purpose

Confidentiality is essential to preserve the effectiveness of the Company's AML framework and to avoid prejudicing regulatory or law-enforcement investigations.

AOFA's current materials expressly identify tipping off as a separate offence.

14.2 Prohibited Disclosure

Employees shall not disclose information concerning a suspicious activity investigation or report to:

- the customer concerned;
- the customer's representative;
- another customer;
- unauthorised employees;
- external counterparties; or
- any other person who does not have a legitimate need to know.

14.3 Internal Need-to-Know Principle

AML information shall be shared internally only with persons who require the information to perform their responsibilities.

For example, Operations may need to know that a transaction is subject to a compliance restriction but does not necessarily need to know the full contents of an MLRO investigation.

14.4 Customer Communications

Where account restrictions are necessary, communications should use neutral operational language and should not reveal confidential AML information.

Employees shall not invent explanations designed to conceal a report, but shall refer sensitive matters to Compliance or the MLRO.

14.5 Confidential Records

Suspicious activity files, investigation records and regulatory communications shall be maintained separately or with appropriate access restrictions.

Access shall be limited to authorised personnel.

15. CUSTOMER AND PAYMENT TRANSACTION CONTROLS

15.1 Purpose

Because VG Markets operates a brokerage business involving customer deposits and withdrawals, payment activity represents a material component of the Company's financial crime risk.

Payment controls shall therefore be integrated with the AML framework rather than treated solely as an operational or finance function.

15.2 Customer-Owned Payment Methods

As a general control, deposits and withdrawals should be made through payment instruments associated with the verified customer.

Where the name of the payment-account holder differs from the customer, the transaction shall be subject to enhanced review.

15.3 Third-Party Deposits

Third-party deposits shall not be routinely accepted as ordinary customer funding.

Where an exception is permitted under the Company's operational procedures, Compliance shall assess:

- identity of the third party;
- relationship to the customer;
- reason for the payment;
- source of funds;
- sanctions exposure;
- fraud risk; and

- whether the arrangement is consistent with the customer's profile.

15.4 Withdrawals

Withdrawals shall generally be returned through an appropriate verified payment channel associated with the customer.

Requests to withdraw funds to a new or unrelated third party shall be subject to enhanced review.

The Company shall consider whether the request could indicate:

- fraud;
- account takeover;
- money laundering;
- sanctions evasion;
- misuse of the brokerage account; or
- circumvention of payment controls.

15.5 Payment Method Changes

Material changes to payment methods shall be subject to appropriate verification.

Additional review may be required where a customer:

- changes payment method shortly before withdrawal;
- introduces a new country or bank;
- uses multiple unrelated payment accounts;
- changes payment details repeatedly; or
- requests withdrawals to an account not previously associated with the customer.

15.6 Payment Service Providers

VG Markets shall conduct appropriate due diligence on payment service providers and other material payment partners.

Due diligence should consider, where relevant:

- licensing or regulatory status;
- ownership and control;
- jurisdiction;
- AML framework;
- sanctions controls;
- reputation;
- adverse media;
- services provided;
- transaction monitoring capabilities; and
- contractual rights and responsibilities.

The Company shall maintain sufficient documentation to demonstrate why the payment provider was considered acceptable.

15.7 High-Risk Payment Channels

Payment channels presenting elevated risks shall be subject to enhanced controls.

The Company shall consider restricting or prohibiting channels where the financial crime risk cannot be effectively managed.

15.8 Virtual Assets

Where virtual-asset-related funding or payment activity is permitted by the Company's business model, it shall be subject to additional risk assessment and appropriate AML controls.

The Company shall consider:

- customer identity;
- origin and destination of funds;
- wallet information where available;
- counterparty or VASP;
- sanctions exposure;
- blockchain analytics where appropriate;
- source of funds;
- transaction size and pattern; and
- applicable Travel Rule or other requirements.

Such activity shall not be accepted merely because the underlying blockchain transaction can be traced.

16. RECORD KEEPING AND INFORMATION MANAGEMENT

16.1 Purpose

VG Markets shall maintain complete, accurate and retrievable records sufficient to demonstrate compliance with its AML/CFT obligations and to enable the Company to respond effectively to regulatory, law-enforcement, audit and other legitimate information requests.

AOFA's current materials state that business transaction records must be maintained for not less than six years and made available to competent authorities.

16.2 Records to Be Maintained

The Company's AML records shall include, as applicable:

- customer identification records;
- verification evidence;
- beneficial ownership information;
- corporate documents;
- customer risk assessments;
- PEP screening;
- sanctions screening;
- adverse media checks;
- source-of-funds evidence;
- source-of-wealth evidence;
- EDD records;
- transaction records;
- deposits and withdrawals;
- transaction-monitoring alerts;
- investigation records;
- suspicious activity escalation records;
- external reporting records;
- customer review records;
- AML training records;
- compliance monitoring records;
- AML risk assessments;
- Board approvals;
- policy reviews;

- remediation records; and
- relevant correspondence.

16.3 Retention Period

The minimum retention period required under the applicable Anjouan AML framework is six years. **The Company applies a standard retention period of seven (7) years**, running from the termination of the customer relationship or from the date of the relevant record, whichever is later. The seven-year standard is applied because the Company has given a contractual undertaking to that effect in the Client Agreement (clause 7.10), the Product Sheet (section 10.8) and the Privacy Policy (sections 14.1 and 14.2). Records must not be destroyed at six years.

Where another applicable legal, contractual, regulatory or litigation requirement requires a longer period, the longer period shall apply.

The Company shall ensure that records subject to a legal hold, regulatory investigation, dispute or other preservation requirement are not destroyed merely because the ordinary retention period has expired.

16.4 Accessibility

Records shall be maintained in a manner that allows authorised personnel to retrieve information promptly.

The Company shall be capable of producing records in a reasonably understandable form for:

- AOFA;
- the competent AML Supervisory Authority;
- law enforcement;
- auditors;
- authorised regulators;
- banks or counterparties where legally and contractually appropriate.

AOFA states that the AML Supervisory Authority may enter the premises of a licensed institution, inspect business transaction records and ask questions relevant to those records.

16.5 Accuracy and Integrity

Records shall be:

- accurate;
- complete;
- dated;
- attributable to the person who created or approved them;
- protected against unauthorised alteration;
- appropriately backed up; and
- capable of being reproduced when required.

Records shall not be falsified, deliberately altered or destroyed to conceal activity.

AOFA identifies falsification or destruction of relevant records as an offence.

16.6 Electronic Records

Electronic records may be maintained provided that they can be reliably retrieved and reproduced.

The Company shall maintain appropriate access controls and backup arrangements to reduce the risk of:

- unauthorised access;
- data loss;
- manipulation;
- accidental deletion; or
- system failure.

16.7 Regulatory Requests

Where the Company receives a legitimate regulatory or law-enforcement request for AML information, the request shall be referred promptly to the MLRO, Compliance Officer or other designated responsible person.

The Company shall maintain a record of:

- request received;
- requesting authority;
- information requested;
- information provided;
- date of response;
- person responsible; and
- any applicable legal advice or approval.

17. AML/CFT TRAINING AND STAFF AWARENESS

17.1 Purpose

An effective AML/CFT framework depends on employees and relevant contractors understanding their responsibilities and being able to identify and escalate potential financial crime risks. VG Markets shall therefore maintain an AML/CFT training programme proportionate to the nature and complexity of its business.

Training shall not be limited to providing employees with a copy of this Manual. Personnel shall understand how the Company's policies operate in practice, including customer identification, risk assessment, sanctions screening, transaction monitoring, suspicious activity escalation, confidentiality and tipping-off restrictions.

17.2 Initial Training

All relevant employees, officers and contractors shall receive AML/CFT training before, or as soon as reasonably practicable after, commencing duties involving customer onboarding, payments, operations, compliance, finance, trading support or other activities presenting financial crime exposure.

Initial training shall cover, as applicable:

- the Company's AML/CFT framework;
- relevant legal and regulatory obligations;
- roles and responsibilities;
- customer identification and verification;
- beneficial ownership;
- customer risk assessment;
- PEP identification;
- sanctions screening;
- source of funds and source of wealth;
- transaction monitoring;
- suspicious activity indicators;
- internal escalation procedures;
- tipping-off restrictions;
- record keeping;
- payment fraud and account takeover risks;
- confidentiality;
- consequences of non-compliance; and
- relevant developments in financial crime risk.

17.3 Role-Based Training

Training shall be tailored to the responsibilities of the employee.

For example:

KYC and onboarding personnel shall receive detailed training on identity verification, beneficial ownership, risk assessment and EDD.

Operations and payment personnel shall receive enhanced training on deposits, withdrawals, third-party funding, payment anomalies and account takeover indicators.

Compliance personnel shall receive more advanced training covering investigations, sanctions, transaction monitoring, suspicious activity assessment, regulatory reporting and emerging financial crime typologies.

Senior management and directors shall receive training sufficient to understand their governance responsibilities, risk exposure and reporting obligations.

17.4 Refresher Training

AML/CFT training shall be refreshed periodically and at least annually for personnel with material AML responsibilities.

Additional training shall be provided when there are material changes to:

- applicable law;
- regulatory expectations;
- the Company's AML framework;
- products or services;
- payment channels;
- customer types;
- jurisdictions;
- systems; or
- identified financial crime risks.

17.5 Training Effectiveness

Training shall be designed to achieve practical understanding rather than merely satisfy an attendance requirement.

Where appropriate, VG Markets may use:

- knowledge assessments;
- case studies;
- scenario-based exercises;
- quizzes;
- practical demonstrations; and
- targeted remediation training.

Training deficiencies shall be documented and addressed.

17.6 Training Records

The Company shall maintain an AML training register recording:

- employee name;
- position;
- training date;
- training subject;
- training provider;
- training method;
- completion status;

- assessment result where applicable; and
- outstanding training requirements.

18. EMPLOYEE SCREENING, CONDUCT AND INTERNAL REPORTING

18.1 Purpose

VG Markets recognises that employees and contractors may themselves present financial crime risks, particularly where they have access to customer information, payment systems, account controls or compliance processes.

The Company shall therefore maintain proportionate personnel controls designed to promote integrity and prevent employees from circumventing AML/CFT controls.

18.2 Fit and Proper Considerations

Personnel performing material compliance, management, payment, onboarding or financial control functions shall be subject to appropriate due diligence and suitability assessment.

Depending on the role and applicable requirements, this may include:

- identity verification;
- employment history;
- qualifications;
- references;
- relevant regulatory history;
- conflicts of interest;
- disciplinary history; and
- other information reasonably relevant to fitness and propriety.

18.3 Conflicts of Interest

Employees shall disclose actual or potential conflicts of interest.

An employee shall not be permitted to make or approve a customer decision where the employee has a personal or financial interest that could compromise independent judgement.

18.4 Employee Obligations

Employees must:

- follow this Manual and related procedures;
- complete required AML training;
- maintain confidentiality;
- escalate suspicious activity;
- comply with sanctions controls;
- maintain accurate records;
- avoid tipping off;
- avoid circumventing customer controls; and
- cooperate with compliance reviews.

18.5 Internal Reporting

Employees shall have a clear mechanism for reporting concerns to Compliance or the MLRO.

An employee is not required to establish that criminal activity has occurred before escalating a concern.

A reasonable concern or suspicion is sufficient to trigger internal escalation.

18.6 Protection for Good-Faith Escalation

Employees who raise AML/CFT concerns in good faith shall not be subject to retaliation merely because the concern is subsequently determined not to constitute reportable suspicious activity.

18.7 Employee Breaches

Failure to comply with AML/CFT requirements may result in:

- additional training;
- enhanced supervision;
- restriction of system access;
- disciplinary action;
- termination of employment or engagement; and
- regulatory or law-enforcement escalation where appropriate.

19. OUTSOURCING, INTRODUCERS, AGENTS AND THIRD-PARTY RELIANCE

19.1 Purpose

VG Markets may use external service providers, technology providers, introducing partners, agents or other third parties in connection with its business.

Outsourcing does not transfer the Company's responsibility for compliance. VG Markets shall remain responsible for ensuring that outsourced AML-related activities are subject to appropriate oversight.

AOFA describes continuing supervision of licensed entities and expects licensees to maintain appropriate compliance with AML obligations.

19.2 Pre-Appointment Due Diligence

Before appointing a material AML-related service provider or business partner, VG Markets shall conduct proportionate due diligence.

The assessment may include:

- legal identity;
- ownership and control;
- jurisdiction;
- regulatory status;
- licences;
- AML framework;
- sanctions controls;
- reputation;
- adverse media;
- financial standing;
- service capability;
- information-security arrangements; and
- relevant management experience.

19.3 Contractual Requirements

Material outsourcing arrangements should contain appropriate contractual provisions covering:

- scope of services;
- AML responsibilities;
- applicable standards;

- information sharing;
- record keeping;
- confidentiality;
- data protection;
- audit rights;
- regulatory access;
- incident notification;
- subcontracting;
- business continuity;
- termination; and
- cooperation with investigations.

19.4 Introducers

Where introducing brokers or similar intermediaries are used, VG Markets shall assess the risks associated with the introducer.

The Company shall establish clear responsibility for:

- customer identification;
- beneficial ownership;
- risk assessment;
- sanctions screening;
- PEP screening;
- ongoing monitoring;
- suspicious activity escalation; and
- customer information maintenance.

VG Markets shall not allow an introducer's commercial interests to override the Company's AML requirements.

19.5 Reliance on Third Parties

Where the Company relies on a third party to perform part of the CDD process, it shall ensure that sufficient information and supporting evidence remain available to VG Markets.

The Company shall retain the ability to obtain relevant records and conduct additional verification where necessary.

19.6 Ongoing Oversight

Material third parties shall be reviewed periodically.

The Company shall consider:

- service performance;
- AML incidents;
- audit findings;
- regulatory developments;
- changes in ownership;
- sanctions exposure;
- adverse media;
- complaints;
- control deficiencies; and
- changes to the Company's risk exposure.

20. BUSINESS PARTNER, COUNTERPARTY AND CORRESPONDENT DUE DILIGENCE

20.1 Purpose

VG Markets' financial crime exposure does not arise solely from customers. Banks, payment service providers, liquidity providers, brokers, introducing partners, technology providers and other material counterparties can also introduce AML, sanctions, fraud and reputational risks.

VG Markets shall therefore apply risk-based due diligence to material business relationships.

20.2 Counterparty Identification

Before entering a material relationship, the Company shall establish, as appropriate:

- legal name;
- registered address;
- jurisdiction;
- ownership and control;
- directors and senior management;
- regulatory status;
- licences;
- nature of business;
- services provided;
- relevant AML controls;
- sanctions exposure; and
- reputation.

20.3 Regulated Counterparties

Where the counterparty is regulated, VG Markets should independently verify the relevant licence or regulatory status using an authoritative source.

A regulatory licence shall not by itself eliminate the need for due diligence.

The Company shall also consider the counterparty's business model and the nature of services provided.

20.4 Correspondent and Banking Relationships

Where VG Markets establishes a correspondent or similar cross-border financial relationship, enhanced due diligence shall be performed where appropriate.

The Company shall consider:

- jurisdiction;
- ownership;
- management;
- regulatory status;
- AML framework;
- sanctions controls;
- reputation;
- services;
- expected transaction volumes;
- customer exposure; and
- relevant regulatory or enforcement history.

AOFA states that institutions engaged in cross-border business are expected to be capable of meeting internationally recognised correspondent-banking due diligence expectations, including the Wolfsberg Correspondent Banking Due Diligence Questionnaire where requested by a correspondent.

20.5 Prohibited or Unacceptable Counterparties

VG Markets shall not knowingly establish relationships with counterparties where:

- ownership cannot reasonably be established;
- regulatory status cannot be verified where regulation is expected;
- material AML deficiencies cannot be satisfactorily addressed;
- sanctions concerns remain unresolved;
- the counterparty is associated with prohibited activity; or
- the relationship creates financial crime risks outside the Company's risk appetite.

20.6 Counterparty Monitoring

Material counterparties shall be periodically reassessed.

Changes in:

- ownership;
- regulatory status;
- jurisdiction;
- services;
- sanctions exposure;
- AML reputation;
- adverse media; or
- financial crime risk

shall trigger an appropriate review.

21. INDEPENDENT AML REVIEW, COMPLIANCE MONITORING AND TESTING

21.1 Purpose

The effectiveness of an AML framework cannot be demonstrated solely by having written policies.

VG Markets shall maintain a compliance monitoring and testing programme designed to assess whether AML controls are operating as intended and whether identified weaknesses are appropriately remediated.

21.2 Compliance Monitoring

The Compliance Officer or another appropriately independent person shall conduct periodic monitoring of AML controls.

Monitoring may include sample testing of:

- customer files;
- identity verification;
- beneficial ownership;
- risk assessments;
- PEP screening;
- sanctions screening;
- EDD;
- source-of-funds verification;
- transaction monitoring;
- alerts;
- suspicious activity escalations;
- payment controls;
- periodic reviews;

- training records; and
- record retention.

21.3 Sample-Based Testing

Testing shall use a risk-based sample.

Higher-risk customers and higher-risk processes should receive greater testing coverage.

The testing methodology shall be documented sufficiently to explain:

- population tested;
- sample selection;
- testing period;
- testing criteria;
- findings;
- exceptions;
- severity;
- remediation; and
- follow-up.

21.4 Control Effectiveness

Each material AML control should be assessed as appropriate.

The Company may use ratings such as:

- Effective;
- Generally Effective;
- Partially Effective; or
- Ineffective.

Material deficiencies shall be escalated to senior management and, where appropriate, the Board.

21.5 Independent Review

An independent AML review shall be conducted periodically and where warranted by the Company's risk profile.

The reviewer should have sufficient independence from the day-to-day AML controls being tested.

The review may be performed by:

- an internal audit function;
- an independent compliance professional;
- an external consultant;
- an external auditor with appropriate expertise; or
- another appropriately qualified independent party.

21.6 Remediation

Each material finding shall have:

- a clearly defined issue;
- risk classification;
- responsible owner;
- corrective action;
- target completion date;
- management oversight; and
- evidence of completion.

Outstanding material findings shall be reported to senior management and, where appropriate, the Board.

21.7 Regulatory Inspection Readiness

VG Markets shall maintain its AML framework so that it can demonstrate to AOFA or another competent authority:

1. what risks it identified;
2. what controls it implemented;
3. how those controls operate;
4. how controls are tested;
5. what deficiencies were identified; and
6. how deficiencies were remediated.

This is particularly important given AOFA's stated power to inspect business transaction records and ask questions relevant to those records.

22. AML MANAGEMENT INFORMATION AND BOARD REPORTING

22.1 Purpose

The Board and senior management must receive sufficient information to understand the Company's financial crime exposure and determine whether AML controls remain appropriate.

The MLRO or Compliance Officer shall therefore provide periodic AML management information (“MI”).

22.2 Minimum AML Reporting

Depending on the Company's size and activity, management reporting should include:

- customer numbers by risk category;
- new customers onboarded;
- rejected applications;
- high-risk customers;
- PEP customers;
- sanctions alerts;
- transaction-monitoring alerts;
- suspicious activity escalations;
- external reports made;
- overdue customer reviews;
- overdue EDD;
- CDD deficiencies;
- payment-related AML incidents;
- training completion;
- compliance monitoring results;
- outstanding remediation;
- material regulatory developments; and
- emerging financial crime risks.

22.3 Material Issues

The MLRO shall escalate material matters to the Board or appropriate senior management promptly rather than waiting for the next scheduled report.

Examples include:

- confirmed sanctions exposure;

- material AML control failure;
- significant suspicious activity;
- regulatory investigation;
- serious data or record loss;
- material payment fraud;
- repeated third-party funding concerns;
- significant deficiencies identified through independent review; or
- any matter that could materially affect the Company's licence or reputation.

22.4 Board Review

The Board shall review AML reporting and challenge management where appropriate.

Board minutes should evidence meaningful consideration of material AML issues rather than merely recording that a report was received.

22.5 Management Accountability

Where the Board identifies weaknesses, appropriate action shall be assigned to responsible management.

The Board shall monitor whether agreed remediation has been completed.

23. BREACHES, REMEDIATION, ENFORCEMENT AND POLICY REVIEW

23.1 Purpose

A strong AML programme requires a formal mechanism for identifying, escalating and correcting failures.

VG Markets shall treat AML breaches as control failures requiring appropriate investigation and remediation.

23.2 Types of Breaches

AML breaches may include:

- failure to complete CDD;
- failure to identify beneficial ownership;
- inaccurate customer risk classification;
- failure to perform sanctions screening;
- failure to conduct required EDD;
- failure to investigate transaction-monitoring alerts;
- failure to escalate suspicious activity;
- unauthorised disclosure;
- tipping off;
- failure to maintain required records;
- deliberate circumvention of controls;
- failure to complete mandatory training; or
- failure of an outsourced AML control.

23.3 Breach Assessment

Each material breach shall be assessed considering:

- nature of the failure;
- duration;
- customers affected;
- transactions affected;

- financial crime exposure;
- whether the failure was isolated or systemic;
- whether the failure has been repeated;
- whether external reporting is required; and
- whether regulatory notification is required.

23.4 Immediate Remediation

Where a material control failure is identified, the Company shall take reasonable steps to contain the risk.

Depending on the circumstances, this may include:

- restricting account activity;
- conducting retrospective customer reviews;
- re-screening affected customers;
- reviewing historical transactions;
- suspending a payment channel;
- increasing monitoring;
- correcting system configurations;
- obtaining additional documentation;
- terminating relationships; or
- engaging independent specialists.

23.5 Root Cause Analysis

Material or repeated breaches shall be subject to root cause analysis.

The analysis should determine whether the underlying cause relates to:

- people;
- systems;
- procedures;
- training;
- management oversight;
- outsourcing;
- technology;
- insufficient resources; or
- inadequate risk assessment.

The Company shall address the underlying cause rather than merely correcting the immediate error.

23.6 Disciplinary Action

Where an employee deliberately circumvents AML controls or fails to comply with material obligations, appropriate disciplinary action may be taken.

Intentional concealment, falsification, tipping off or deliberate destruction of records shall be treated as particularly serious matters.

AOFA identifies money laundering, tipping off and falsification or destruction of relevant records as offences under the applicable AML legislation.

23.7 Regulatory Cooperation

VG Markets shall cooperate appropriately with lawful requests from competent authorities.

The Company shall maintain procedures to ensure that regulatory requests are:

- identified promptly;

- escalated to appropriate personnel;
- responded to accurately;
- provided within required timeframes; and
- documented.

The Company's internal confidentiality requirements shall not be used to obstruct a lawful regulatory or law-enforcement request.

23.8 Annual Policy Review

This Manual shall be reviewed at least annually.

The review shall consider:

- changes in applicable law;
- AOFA regulatory developments;
- changes in the Company's business model;
- new products;
- new jurisdictions;
- new payment channels;
- customer risk;
- transaction-monitoring results;
- sanctions developments;
- internal audit findings;
- compliance monitoring;
- regulatory inspections;
- external financial crime developments; and
- material incidents.

23.9 Interim Review

The Manual shall also be reviewed outside the annual cycle where there is a material change to:

- the Company's ownership;
- management;
- licence;
- products;
- customer base;
- geographic footprint;
- payment arrangements;
- technology;
- outsourcing arrangements;
- regulatory requirements; or
- financial crime threat environment.

23.10 Approval

Material amendments to this Manual shall be approved by the Board or appropriately authorised senior management in accordance with the Company's governance arrangements.

Each approved version shall identify:

- version number;
- effective date;
- approval date;

- approving body/person;
- material amendments; and
- next scheduled review date.

APPENDIX A — ENTERPRISE AML/CFT RISK ASSESSMENT MATRIX

A.1 Purpose

This Appendix establishes the methodology used by VG Markets Limited to identify, assess and document the money laundering, terrorist financing and related financial crime risks arising from its business model.

The Enterprise-Wide ML/TF Risk Assessment (“EWRA”) shall be maintained as a separate controlled document or as an approved component of this Manual. It shall be reviewed at least annually and whenever a material change occurs in the Company's business, customers, jurisdictions, products, payment arrangements, technology, outsourcing arrangements or financial crime environment.

The EWRA is intended to demonstrate that VG Markets has considered its inherent risks, assessed the effectiveness of its controls, determined residual risk and allocated appropriate resources.

A.2 Risk Assessment Framework

VG Markets shall assess inherent risk across the following five principal categories:

Risk Category	Weight
Geographic Risk	30%
Customer Profile Risk	20%
PEP / Sanctions / Financial Crime Exposure	20%
Source of Funds / Source of Wealth Risk	15%
Product / Transaction Risk	15%
Total	100%

The weighting reflects the Company's assessment that geographic exposure is particularly relevant to an international brokerage business, while customer type, PEP/sanctions exposure, source of wealth/funds and transaction/product characteristics also materially affect the overall risk profile.

The Company may amend the weighting where the business model changes, provided that the methodology and rationale are documented and approved.

A.3 Risk Rating Scale

Each relevant risk factor shall generally be assessed on a scale of 1 to 5:

Score	Rating	General Description
1	Low	Limited identifiable financial crime exposure
2	Low-Medium	Some risk factors but generally manageable
3	Medium	Meaningful risk requiring standard enhanced controls

Score	Rating	General Description
4	Medium-High	Elevated risk requiring additional controls
5	High	Significant financial crime exposure requiring EDD and senior review

The score shall not be determined mechanically. The person performing the assessment shall apply reasonable professional judgement and document material qualitative considerations.

A.4 Geographic Risk

Geographic risk shall consider all jurisdictions relevant to the customer and transaction, including:

- country of residence;
- nationality;
- incorporation jurisdiction;
- principal place of business;
- beneficial owner's jurisdiction;
- source-of-funds jurisdiction;
- source-of-wealth jurisdiction;
- payment-origin jurisdiction;
- payment-destination jurisdiction; and
- jurisdictions associated with counterparties or intermediaries.

The Company shall not rely on a static list of “high-risk countries”. Country risk shall be assessed using current and reasonably reliable information, including applicable FATF information, sanctions regimes, regulatory information, corruption and financial crime indicators, transparency considerations and other relevant sources.

Geographic Risk Guide

Risk Score	Indicative Circumstances
1	Established, transparent jurisdiction with effective financial crime controls and no material relevant concerns
2	Generally acceptable jurisdiction with limited additional concerns
3	Jurisdiction presenting identifiable AML, corruption, transparency or regulatory concerns
4	Higher-risk jurisdiction, significant regulatory concerns, elevated corruption/financial crime exposure or other material concerns
5	Sanctioned/prohibited jurisdiction, severe financial crime concerns, or jurisdiction outside the Company's risk appetite

The final assessment shall reflect the current circumstances rather than relying solely on country classification.

A.5 Customer Profile Risk

Customer risk shall consider:

- individual versus corporate customer;
- occupation;

- industry;
- business activity;
- customer wealth;
- expected account size;
- expected transaction volume;
- customer complexity;
- PEP status;
- sanctions exposure;
- adverse media;
- ownership structure;
- use of nominees;
- use of trusts or foundations;
- use of intermediaries;
- regulated versus unregulated status; and
- other relevant financial crime indicators.

A.6 PEP, Sanctions and Financial Crime Exposure

The following shall receive heightened consideration:

- confirmed PEP status;
- family member or close associate of a PEP;
- sanctions match or unresolved potential match;
- significant adverse media;
- known regulatory enforcement;
- suspected fraud;
- corruption allegations;
- criminal proceedings;
- previous suspicious activity;
- unexplained financial activity;
- previous account termination by another financial institution for financial crime concerns.

A confirmed sanctions match shall be handled under the Company's sanctions escalation procedure and may fall outside the Company's risk appetite.

A.7 Source of Funds / Source of Wealth Risk

The Company shall assess whether the customer's stated financial circumstances reasonably support the expected account activity.

Factors include:

- occupation;
- business income;
- declared wealth;
- investment activity;
- inheritance;
- property ownership;
- corporate income;
- investment proceeds;
- unexplained wealth;

- third-party funding;
- cash-intensive activity;
- crypto/virtual-asset exposure; and
- complexity of wealth structures.

A.8 Product and Transaction Risk

The Company shall consider risks arising from:

- FX trading;
- CFD trading;
- leveraged products;
- derivatives;
- deposits;
- withdrawals;
- cross-border transfers;
- multiple payment channels;
- third-party payments;
- rapid movement of funds;
- inactive trading accounts receiving significant deposits;
- unusual trading/payment patterns; and
- any permitted virtual-asset-related activity.

A.9 Control Effectiveness

After determining inherent risk, the Company shall assess the effectiveness of existing controls.

Controls to be considered include:

- customer identification;
- beneficial ownership verification;
- PEP screening;
- sanctions screening;
- customer risk scoring;
- source-of-funds controls;
- source-of-wealth controls;
- EDD;
- transaction monitoring;
- payment controls;
- suspicious activity escalation;
- AML training;
- compliance monitoring;
- independent review;
- outsourcing oversight; and
- management oversight.

Control effectiveness may be rated:

Rating	Meaning
Effective	Control is appropriately designed and operating effectively

Rating	Meaning
Generally Effective	Minor weaknesses exist but control remains broadly effective
Partially Effective	Material improvement is required
Ineffective	Control does not adequately mitigate the identified risk

A.10 Residual Risk

Residual risk represents the risk remaining after consideration of existing controls.

The Company shall classify residual risk as:

- Low;
- Medium;
- High; or
- Outside Risk Appetite.

A high residual risk does not automatically mean that the business or relationship must be rejected. The Company shall determine whether the risk can be effectively managed.

Where risk remains outside risk appetite, the Company shall not knowingly accept or maintain the exposure.

A.11 Risk Appetite

VG Markets shall not knowingly accept relationships involving:

- anonymous or fictitious customers;
- unidentified beneficial owners;
- confirmed sanctions prohibitions;
- prohibited jurisdictions;
- unexplained criminal proceeds;
- shell banks where relevant;
- deliberate concealment of ownership;
- materially false information;
- financial crime risks that cannot be mitigated; or
- activity otherwise prohibited by law or Company policy.

A.12 EWRA Approval

The EWRA shall be approved by the Board or appropriately authorised senior management.

The Board shall receive information concerning:

- overall risk rating;
- material risk changes;
- control weaknesses;
- high residual-risk areas;
- remediation;
- emerging threats; and
- resource requirements.

APPENDIX B — CUSTOMER RISK ASSESSMENT SCORING MATRIX

B.1 Purpose

This Appendix provides the operational scoring methodology for individual customer risk assessments.

The Customer Risk Assessment ("CRA") shall be completed before customer acceptance and updated periodically or following a material trigger event.

The score is a decision-support mechanism and shall not replace professional judgement.

B.2 Weighted Categories

Category	Weight
Geographic Risk	30%
Customer Profile	20%
PEP / Sanctions / Financial Crime	20%
Source of Funds / Source of Wealth	15%
Product / Transaction	15%
Total	100%

B.3 Scoring Method

Each category receives a score from 1 to 5.

The weighted score is calculated as:

Weighted Score = Category Score × Category Weight

The overall customer risk score is the sum of all weighted category scores.

Overall Classification

Final Score	Customer Risk
1.00–2.00	Low
2.01–3.50	Medium
3.51–5.00	High

Where an automatic high-risk trigger exists, the customer shall be treated as High Risk irrespective of the numerical result.

B.4 Automatic High-Risk Triggers

The following shall generally result in a High Risk classification or mandatory MLRO review:

- foreign PEP;
- significant PEP-related risk;
- unresolved sanctions concern;
- complex ownership structure without a clear commercial rationale;
- nominee arrangements;
- trust/foundation structures presenting elevated opacity;
- significant adverse media;
- unexplained source of wealth;

- unexplained source of funds;
- high-risk payment arrangements;
- material third-party funding;
- VASP/MSB or similarly higher-risk financial activity;
- customer activity inconsistent with stated profile;
- suspected attempts to circumvent Company controls;
- material regulatory or law-enforcement concerns.

A trigger does not necessarily require rejection. It requires enhanced assessment and appropriate controls.

B.5 Individual Customer Matrix

Factor	Low	Medium	High
Occupation	Salaried/professional	Self-employed/business	High-risk or opaque industry
Income	Verifiable and consistent	Some complexity	Unclear or inconsistent
Wealth	Easily explainable	Some complexity	Unexplained/complex
Residence	Low-risk	Medium-risk	Higher-risk
PEP	None	Domestic/limited exposure	Foreign PEP/significant exposure
Adverse Media	None	Minor/unsubstantiated	Material/relevant
Funding	Own account	Some complexity	Third-party/unexplained
Account Activity	Consistent	Moderately unusual	Highly inconsistent

B.6 Corporate Customer Matrix

Corporate customers shall be assessed according to:

- jurisdiction;
- ownership transparency;
- number of ownership layers;
- beneficial owners;
- directors;
- business activity;
- regulatory status;
- source of funds;
- source of wealth;
- expected turnover;
- payment arrangements;
- PEP exposure;
- sanctions exposure;
- adverse media; and
- use of nominees/intermediaries.

Indicative Corporate Risk Levels

Low Risk: Simple ownership, transparent beneficial ownership, regulated or established business, credible source of funds and straightforward payment arrangements.

Medium Risk: Some ownership complexity, international operations, moderately higher-risk industry or jurisdiction, or increased payment complexity.

High Risk: Multiple offshore layers, nominee arrangements, unclear beneficial ownership, high-risk business activity, unexplained wealth, significant PEP exposure, material adverse media or unusual payment structures.

B.7 Risk Overrides

The MLRO or Compliance Officer may override the numerical risk score where circumstances justify a different classification.

Any override shall document:

1. original numerical score;
2. proposed classification;
3. reason for override;
4. additional controls;
5. approving person; and
6. review date.

B.8 Review Frequency

Risk	Review
Low	At least every 36 months
Medium	At least every 24 months
High	At least every 12 months
PEP / Enhanced Risk	At least annually
Trigger Event	Immediate / event-driven

APPENDIX C — INDIVIDUAL CUSTOMER KYC CHECKLIST

C.1 Purpose

This checklist is intended to provide the onboarding team with a practical minimum standard for individual customer KYC.

The checklist shall be completed before the customer is activated unless an approved exception exists.

C.2 Identity Information

☐ Full legal name obtained ☐ Date of birth obtained ☐ Nationality obtained ☐ Country of residence obtained ☐ Residential address obtained ☐ Identification document obtained ☐ Identification document validity checked ☐ Identification document authenticity assessed ☐ Identity independently verified ☐ Electronic verification completed where applicable ☐ Customer information is internally consistent

C.3 Address Verification

☐ Residential address obtained ☐ Appropriate proof of address obtained where required ☐ Document reviewed for date and authenticity ☐ Address consistent with customer profile ☐ Any discrepancy investigated

C.4 Employment / Occupation

☐ Occupation obtained ☐ Employer/business identified where relevant ☐ Business activity understood where self-employed ☐ Occupation assessed for financial crime risk ☐ Expected income/activity considered

C.5 PEP Screening

☐ Customer screened ☐ PEP result recorded ☐ Family/close associate consideration completed where relevant ☐ False positive cleared where applicable ☐ PEP escalation completed where applicable ☐ Senior approval obtained where required

C.6 Sanctions Screening

☐ Customer screened against applicable sanctions lists ☐ Potential match investigated ☐ False positive documented where applicable ☐ Confirmed/unresolved match escalated ☐ Screening evidence retained

C.7 Adverse Media

☐ Relevant adverse media search conducted ☐ Search results assessed ☐ Material findings escalated ☐ Decision documented

C.8 Source of Funds / Wealth

☐ Expected source of funds recorded ☐ Source of wealth considered ☐ Evidence obtained where required ☐ Information consistent with customer profile ☐ High-risk source of funds escalated

C.9 Expected Account Activity

☐ Expected deposit level established ☐ Expected withdrawal level established ☐ Expected trading activity established ☐ Expected payment methods established ☐ Expected countries/payment destinations considered ☐ Expected activity consistent with customer profile

C.10 Customer Risk Assessment

☐ CRA completed ☐ Geographic risk assessed ☐ Customer profile assessed ☐ PEP/sanctions risk assessed ☐ SoF/SoW risk assessed ☐ Product/transaction risk assessed ☐ Overall score calculated ☐ Automatic high-risk triggers checked ☐ Risk classification approved

C.11 EDD

Where applicable:

☐ EDD trigger identified ☐ Additional documentation requested ☐ Source of wealth independently verified ☐ Source of funds independently verified ☐ Adverse media reviewed ☐ Senior approval obtained ☐ Enhanced monitoring established

C.12 Final Acceptance

☐ All mandatory KYC completed ☐ No unresolved sanctions concern ☐ Beneficial ownership requirement not applicable / satisfied ☐ Risk rating approved ☐ Account restrictions recorded where applicable ☐ Account approved for activation ☐ KYC records saved in approved system

Reviewer: ______________________ Date: ______________________ Risk Rating: ______________________ Approver: ______________________

APPENDIX D — CORPORATE CUSTOMER KYC AND UBO CHECKLIST

D.1 Purpose

This checklist applies to companies and other legal entities seeking to establish a relationship with VG Markets.

The purpose is to establish the entity's legal existence, ownership, control, business purpose, beneficial ownership and financial crime risk.

D.2 Corporate Identity

☐ Certificate of incorporation / registration obtained ☐ Legal name verified ☐ Registration number verified ☐ Registered address verified ☐ Principal business address obtained ☐ Business activity established ☐ Constitutional documents obtained where applicable ☐ Corporate registry information independently checked

D.3 Directors and Officers

☐ Current directors identified ☐ Directors verified ☐ Authorised signatories identified ☐ Authorised representatives verified ☐ Relevant management identified ☐ PEP screening completed ☐ Sanctions screening completed ☐ Adverse media screening completed where appropriate

D.4 Shareholding Structure

☐ Current shareholder information obtained ☐ Shareholding percentages verified ☐ Ownership chart obtained where appropriate ☐ Intermediate corporate shareholders identified ☐ Ownership chain traced ☐ Complex structures explained ☐ Nominees identified ☐ Trust/foundation involvement identified ☐ Control arrangements considered

D.5 Beneficial Ownership

☐ Beneficial owners identified ☐ 25% ownership threshold assessed ☐ Control through other means considered ☐ Controlling person identified where no 25% owner exists ☐ Beneficial owners independently verified ☐ Beneficial ownership evidence retained ☐ Any unexplained ownership structure escalated

D.6 Business Profile

☐ Nature of business understood ☐ Principal markets identified ☐ Countries of operation identified ☐ Regulatory status verified where applicable ☐ Licence obtained/verified where applicable ☐ Expected trading purpose established ☐ Expected account activity established

D.7 Source of Funds / Wealth

☐ Corporate source of funds identified ☐ Ultimate source of funds considered ☐ Source of wealth assessed where appropriate ☐ Financial statements obtained where appropriate ☐ Bank evidence obtained where appropriate ☐ Funding arrangements understood ☐ Third-party funding assessed

D.8 Risk Assessment

☐ Geographic risk assessed ☐ Customer/business risk assessed ☐ PEP/sanctions risk assessed ☐ SoF/SoW risk assessed ☐ Product/transaction risk assessed ☐ Overall score calculated ☐ Risk classification approved ☐ EDD trigger assessed

D.9 EDD

Where applicable:

☐ Ownership structure independently verified ☐ Additional corporate documents obtained ☐ UBO evidence enhanced ☐ SoF/SoW enhanced ☐ Adverse media enhanced ☐ Senior management approval obtained ☐ Enhanced monitoring established

D.10 Account Activation

☐ All required KYC complete ☐ UBO confirmed ☐ Directors/signatories confirmed ☐ Sanctions cleared ☐ PEP review completed ☐ Risk rating approved ☐ Account restrictions documented ☐ Final approval completed

Entity: ______________________ Risk Rating: ______________________ Reviewer: ______________________ Approver: ______________________ Date: ______________________

APPENDIX E — ENHANCED DUE DILIGENCE CHECKLIST

E.1 Purpose

This checklist provides a practical framework for customers subject to Enhanced Due Diligence.

EDD shall be proportionate to the specific risk and does not require every item below to be obtained in every case. The reviewer shall document which measures were applied and why.

E.2 EDD Trigger

☐ High-risk customer ☐ PEP ☐ High-risk jurisdiction ☐ Complex ownership ☐ Nominee structure ☐ Trust/foundation ☐ High-risk occupation/business ☐ Significant adverse media ☐ Unexplained source of wealth ☐ Unexplained source of funds

☐ Third-party funding ☐ Unusual transaction activity ☐ Sanctions concern ☐ Financial crime concern ☐ Other: ____________________

E.3 Enhanced Identity Verification

☐ Additional identity document obtained ☐ Independent database verification ☐ Enhanced electronic verification ☐ Additional address verification ☐ Video/liveness verification where appropriate ☐ Identity discrepancies resolved

E.4 Enhanced Ownership Verification

☐ Full ownership chart obtained ☐ Corporate registry records obtained ☐ Shareholder evidence reviewed ☐ Control arrangements reviewed ☐ UBO independently verified ☐ Nominee relationship explained ☐ Trust/foundation documents reviewed where applicable

E.5 Enhanced Source of Wealth

Potential evidence may include:

☐ Employment records ☐ Business ownership evidence ☐ Audited financial statements ☐ Investment statements ☐ Property sale records ☐ Inheritance documents ☐ Dividend records ☐ Sale-of-business documentation ☐ Tax/financial records ☐ Credible independent public information ☐ Other reliable evidence

E.6 Enhanced Source of Funds

☐ Bank statements ☐ Payment evidence ☐ Investment liquidation evidence ☐ Loan documentation ☐ Business revenue evidence ☐ Dividend evidence ☐ Sale proceeds evidence ☐ Third-party funding explanation ☐ Source independently corroborated

E.7 Enhanced Adverse Media

☐ Search conducted ☐ Search terms documented ☐ Relevant jurisdictions searched ☐ Criminal allegations considered ☐ Corruption allegations considered ☐ Regulatory enforcement considered ☐ Fraud allegations considered ☐ Material results escalated

E.8 Enhanced Transaction Review

☐ Historical deposits reviewed ☐ Historical withdrawals reviewed ☐ Trading activity reviewed ☐ Payment methods reviewed ☐ Third-party transactions reviewed ☐ Geographic flows reviewed ☐ Related accounts considered ☐ Unusual activity investigated

E.9 Senior Approval

Where required:

☐ EDD report prepared ☐ Risk accepted by authorised senior person ☐ Conditions imposed ☐ Monitoring frequency increased ☐ Account restrictions imposed where appropriate ☐ Review date established

EDD Conclusion:

Risk Classification: ____________________ Approved By: ____________________ Date: ____________________

APPENDIX F — PEP AND SANCTIONS ESCALATION FORM

F.1 Purpose

This form shall be used when a PEP, sanctions or related screening alert requires escalation beyond ordinary onboarding or screening procedures.

A screening alert shall not automatically be treated as a confirmed match. The reviewer must determine whether the alert relates to the actual customer or connected person.

F.2 Customer Information

Customer Name: ______________________________

Customer ID: ______________________________

Customer Type: ☐ Individual ☐ Corporate ☐ Other

Country of Residence/Incorporation: ______________________

Risk Rating: ______________________

F.3 Alert Type

☐ PEP ☐ PEP Family Member ☐ PEP Close Associate ☐ UN Sanctions ☐ Other Applicable Sanctions ☐ Potential Sanctions Match ☐ Adverse Media ☐ Other: ______________________

F.4 Screening Information

Screening Date: ______________________

Screening System/Source: ______________________

Name Matched: ______________________

Date of Birth / Registration Information: ______________________

Nationality / Jurisdiction: ______________________

List / Database: ______________________

F.5 Match Assessment

☐ False positive ☐ Potential match requiring further investigation ☐ Confirmed match ☐ Unable to determine

Basis for Decision

F.6 PEP Assessment

Where the alert concerns a PEP:

Position / Public Function: ______________________

Jurisdiction: ______________________

Current or Former Position: ______________________

PEP Category: ______________________

Family / Close Associate Relationship: ______________________

Source of Wealth: ______________________

Source of Funds: ______________________

Adverse Information: ______________________

F.7 Risk Assessment

☐ Standard risk ☐ Enhanced risk ☐ High risk ☐ Outside risk appetite

Reasoning:

F.8 Required Action

☐ Clear alert ☐ Obtain additional information ☐ Conduct EDD ☐ Obtain SoW evidence ☐ Obtain SoF evidence ☐ Senior management approval ☐ Enhanced monitoring ☐ Restrict account ☐ Reject onboarding ☐ Suspend relationship/activity ☐ Escalate to MLRO ☐ Consider regulatory reporting ☐ Other: ______________________

F.9 MLRO Decision

Decision:

Reasoning:

MLRO Name: ______________________

Signature/Approval: ______________________

Date: ______________________

Next Review Date: ______________________

APPENDIX G — TRANSACTION MONITORING RED-FLAG MATRIX FOR FX/CFD BROKERAGE

G.1 Purpose

This Appendix establishes indicative transaction-monitoring red flags relevant to VG Markets' FX/CFD brokerage business.

A red flag is an indicator requiring review. It does not, by itself, establish that money laundering, terrorist financing or other criminal conduct has occurred.

The Company shall consider multiple indicators together, together with the customer's profile, transaction history and available explanation.

G.2 Rapid Deposit and Withdrawal

Scenario: Customer deposits a substantial amount and seeks withdrawal shortly afterwards with limited or no genuine trading activity.

Potential Risk: Brokerage account may be being used primarily as a vehicle for moving funds.

Review Actions:

- review trading activity;
- identify source of deposit;
- identify withdrawal destination;
- compare funding and withdrawal amounts;
- establish reason for activity;
- check third-party involvement;
- review customer profile.

Possible Escalation: EDD / MLRO review where explanation is inadequate.

G.3 Third-Party Deposit

Scenario: Funds are received from an account or payment instrument belonging to another person.

Potential Risk: Concealment of source of funds, fraud, mule activity or third-party money movement.

Review Actions:

- identify payer;
- establish relationship;
- verify source of funds;
- determine reason;
- assess sanctions/fraud risk;
- review previous third-party activity.

G.4 Third-Party Withdrawal

Scenario: Customer requests withdrawal to an unrelated person or account.

Potential Risk: Movement of funds to an undisclosed beneficiary or account takeover.

Review Actions:

- verify withdrawal beneficiary;
- confirm relationship;
- verify customer instruction;
- assess account security;
- review transaction history;
- escalate where unexplained.

G.5 Multiple Payment Instruments

Scenario: Customer uses numerous cards, bank accounts, wallets or payment methods without a reasonable explanation.

Potential Risk: Layering, payment fraud, account misuse or attempts to circumvent controls.

Review Actions:

- identify payment instruments;
- determine ownership;
- establish reason for multiple methods;
- compare jurisdictions;
- review transaction pattern.

G.6 Geographic Inconsistency

Scenario: Customer resides in one jurisdiction but repeatedly funds from unrelated jurisdictions or withdraws to unrelated countries.

Potential Risk: Use of third-party accounts, sanctions evasion, concealment of source/destination.

Review Actions:

- identify source/destination;
- determine relationship;
- review customer profile;
- assess jurisdictional risk;
- obtain explanation/evidence where appropriate.

G.7 Unusual Account Turnover

Scenario: Transaction volumes materially exceed the customer's expected activity.

Potential Risk: Account being used for purposes inconsistent with the customer's stated profile.

Review Actions:

- compare historical activity;
- review source of funds;
- reassess customer risk;
- obtain updated financial information;
- consider EDD.

G.8 Inconsistent Wealth or Income

Scenario: Customer's trading deposits are materially inconsistent with stated income or wealth.

Potential Risk: Unexplained wealth or illegitimate source of funds.

Review Actions:

- review SoF;
- review SoW;
- obtain supporting documentation;
- reassess customer risk;
- escalate where explanation is insufficient.

G.9 Minimal Trading With Significant Funding

Scenario: Large amounts are deposited but only limited trading activity occurs.

Potential Risk: Brokerage account may be functioning as a value-transfer mechanism.

Review Actions:

- assess trading rationale;
- review deposit/withdrawal timing;
- identify payment counterparties;
- review source of funds;
- assess whether behaviour is consistent with customer profile.

G.10 Rapid Movement of Funds

Scenario: Funds move through the account shortly after receipt.

Potential Risk: Layering or movement of funds without an apparent legitimate investment purpose.

Review Actions:

- map funds;
- identify origin and destination;
- review timing;
- compare trading activity;
- identify linked accounts;
- escalate where appropriate.

G.11 Repeated Failed Transactions

Scenario: Customer repeatedly attempts payments that fail before eventually succeeding through another method.

Potential Risk: Use of compromised payment instruments, fraud or attempts to circumvent controls.

Review Actions:

- review failed payment history;
- identify payment instruments;
- assess account security;
- check for unusual behavioural changes;
- escalate fraud concerns.

G.12 Account Changes Before Withdrawal

Scenario: Customer changes personal information, bank details or payment method shortly before requesting a withdrawal.

Potential Risk: Account takeover, fraud or diversion of funds.

Review Actions:

- independently verify change;
- confirm customer identity;
- review recent login/account activity where available;
- delay or restrict withdrawal where appropriate;
- escalate suspicious circumstances.

G.13 Related Accounts

Scenario: Multiple customers appear connected through common devices, payment instruments, addresses, bank accounts or other indicators.

Potential Risk: Coordinated activity, account sharing, fraud, mule networks or attempts to circumvent controls.

Review Actions:

- identify relationship;
- assess common funding;

- compare trading patterns;
- investigate common beneficiaries;
- consider group-level monitoring.

G.14 Unusual Corporate Activity

Scenario: Corporate customer uses the brokerage account in a manner inconsistent with its business purpose.

Potential Risk: Personal use of corporate funds, layering or concealment of beneficial ownership.

Review Actions:

- review business purpose;
- identify beneficial owner;
- review source of funds;
- review authorised signatories;
- reassess corporate risk.

G.15 High-Risk Jurisdiction Activity

Scenario: Significant activity involves jurisdictions presenting elevated AML, sanctions, corruption or regulatory risks.

Potential Risk: Increased exposure to sanctions evasion, illicit proceeds or weak financial controls.

Review Actions:

- assess jurisdiction;
- screen relevant parties;
- identify source/destination;
- perform EDD where appropriate;
- consider whether activity falls within risk appetite.

G.16 Potential Sanctions Evasion

Scenario: Customer changes names, addresses, payment routes or counterparties in circumstances suggesting an attempt to avoid sanctions controls.

Potential Risk: Sanctions evasion.

Review Actions:

- immediately escalate;
- conduct enhanced screening;
- identify beneficial ownership;
- review transaction history;
- identify related parties;
- consider whether transactions must be suspended or otherwise restricted;
- refer to MLRO.

G.17 Virtual-Asset-Related Activity

Where virtual-asset-related transactions are permitted, indicators may include:

- unexplained transfers involving virtual assets;
- rapid movement between fiat and virtual assets;
- exposure to high-risk or opaque VASPs;
- significant unexplained wallet activity;
- sanctions exposure;
- inability to establish source of funds;

- use of mixers/tumblers or other high-risk services where relevant;
- transaction activity inconsistent with the customer's profile.

Such indicators require risk-based investigation and may justify EDD or escalation.

G.18 Red-Flag Assessment

When a red flag is identified, the reviewer shall consider:

1. What occurred?
2. Why is the activity unusual?
3. Is it consistent with the customer's known profile?
4. Is there a legitimate explanation?
5. Can the explanation be independently supported?
6. Are there additional related red flags?
7. Does the activity require EDD?
8. Should the customer risk rating change?
9. Should enhanced monitoring be applied?
10. Does the matter need to be escalated to the MLRO?

G.19 Alert Closure

An alert may only be closed where the reviewer has documented a reasonable basis for doing so.

The record should include:

- alert description;
- customer information reviewed;
- transaction(s) reviewed;
- explanation obtained;
- supporting evidence;
- analysis;
- conclusion;
- reviewer;
- date; and
- escalation decision.

An alert shall not be closed solely by stating:

“Customer explanation satisfactory.”

The record should explain why the explanation was considered satisfactory and what evidence supports the conclusion.

G.20 Escalation to MLRO

The matter shall be escalated where:

- the explanation remains inadequate;
- multiple red flags exist;
- there is evidence of deliberate concealment;
- source of funds cannot reasonably be established;
- third-party activity remains unexplained;
- sanctions concerns exist;
- the customer appears to be circumventing controls;
- the activity is materially inconsistent with the customer profile;
- adverse information materially increases risk; or

- the reviewer has a reasonable suspicion that financial crime may be involved.

The MLRO shall determine the appropriate next step, including whether additional investigation, EDD, enhanced monitoring, account restriction, relationship termination or external reporting should be considered.

G.9 Operational escalation principle

The Company's transaction-monitoring framework shall operate according to the following principle:

Unusual → Investigate → Understand → Evidence → Assess → Escalate where necessary → Document.

The purpose of transaction monitoring is not to prohibit legitimate customer activity merely because it is unusual. The purpose is to ensure that unusual or potentially suspicious activity receives an appropriate and documented risk-based assessment.

APPENDIX H — SUSPICIOUS ACTIVITY INTERNAL ESCALATION FORM

H.1 Purpose

This form is designed to provide employees, Operations, Compliance and other relevant personnel with a consistent mechanism for escalating potentially suspicious activity to the MLRO.

Employees are not required to determine whether an external suspicious transaction report is legally required. Their responsibility is to identify and promptly escalate reasonable concerns. The MLRO is responsible for determining the appropriate investigation, escalation and reporting action.

H.2 Customer Information

Customer Name: ____

Customer ID / Account Number: __________________________

Customer Type:

☐ Individual ☐ Corporate ☐ Trust / Foundation ☐ Other: __________________________

Customer Country: _______________________________________

Current Risk Rating:

☐ Low ☐ Medium ☐ High

PEP: ☐ Yes ☐ No ☐ Unknown

Sanctions Alert: ☐ Yes ☐ No

H.3 Source of Concern

☐ Customer onboarding ☐ KYC review ☐ Beneficial ownership review ☐ Transaction monitoring ☐ Deposit ☐ Withdrawal ☐ Third-party payment ☐ Payment method change ☐ Trading activity ☐ Sanctions screening ☐ PEP screening ☐ Adverse media ☐ Employee observation ☐ Customer complaint ☐ Law-enforcement/regulatory enquiry ☐ Other: __________________________

H.4 Description of Activity

Date(s) of Activity: _____________________________________

Amount(s): ____

Currency: ____

Payment Method: ____

Origin: ____

Destination: ____

Relevant Transaction ID(s): _____________________________

Description

Provide a factual description of the activity, including why it appears unusual or inconsistent with the customer's known profile.

H.5 Red Flags Identified

☐ Unexplained source of funds ☐ Unexplained source of wealth ☐ Third-party funding ☐ Unusual withdrawal ☐ Rapid deposit and withdrawal ☐ Minimal trading / significant funding ☐ Multiple payment methods ☐ Geographic inconsistency ☐ Unusual account turnover ☐ Potential account takeover ☐ Potential fraud ☐ Potential sanctions evasion ☐ Complex ownership ☐ Nominee arrangement ☐ Adverse media ☐ PEP concern ☐ Unusual trading activity ☐ Related accounts ☐ Other: ______________________

H.6 Customer Explanation

Explanation obtained from customer:

Supporting evidence provided:

Is the explanation independently corroborated?

☐ Yes ☐ Partially ☐ No ☐ Not applicable

H.7 Initial Employee Assessment

Reason for escalation:

Supporting documents attached:

☐ Yes ☐ No

Employee Name: __________________________________

Department: _____________________________________

Date: ____

Signature / electronic approval: _____________________

H.8 MLRO Assessment

Investigation Required:

☐ No ☐ Yes

EDD Required:

☐ No ☐ Yes

Risk Rating Change:

☐ No change ☐ Increase ☐ Decrease

Enhanced Monitoring Required:

☐ No ☐ Yes

Account Restriction Required:

☐ No ☐ Yes

External Reporting Consideration:

☐ No ☐ Yes ☐ Further investigation required

MLRO Analysis

MLRO Decision

MLRO: ____

Date: ____

H.9 Confidentiality

This document is confidential and shall be restricted to authorised personnel.

The customer must not be informed that a suspicious activity investigation or report is being considered or has been made where such disclosure would constitute prohibited tipping off.

APPENDIX I — PERIODIC CUSTOMER REVIEW CHECKLIST

I.1 Purpose

This checklist shall be used when conducting scheduled or event-driven customer reviews.

The purpose is to confirm that the Company's understanding of the customer remains current and that the customer's risk classification continues to be appropriate.

I.2 Review Information

Customer: ____

Customer ID: ____

Customer Type: _______________________________________

Current Risk Rating: __________________________________

Previous Review Date: ________________________________

Current Review Date: _________________________________

Reviewer: ____

Review Type:

☐ Periodic ☐ Trigger Event ☐ PEP Review ☐ High-Risk Review ☐ Remediation Review ☐ Other: _________________________

I.3 Identity Review

☐ Identity information remains current ☐ Identification document remains valid/acceptable ☐ Address remains current ☐ Contact information remains current ☐ Material discrepancies investigated

I.4 Corporate Review

Where applicable:

☐ Certificate / registration information current ☐ Directors current ☐ Shareholders current ☐ Beneficial owners current ☐ Ownership structure unchanged ☐ Authorised signatories current ☐ Business activity unchanged ☐ Regulatory licence/status remains valid

I.5 PEP and Sanctions

☐ PEP screening refreshed ☐ Sanctions screening refreshed ☐ Adverse media screening conducted where appropriate ☐ Previous alerts reviewed ☐ Changes in PEP status considered ☐ Changes in sanctions exposure considered

I.6 Source of Funds / Wealth

☐ Existing SoF information remains adequate ☐ Existing SoW information remains adequate ☐ Customer financial profile remains consistent ☐ New evidence required ☐ Additional evidence obtained ☐ Material discrepancy identified

I.7 Transaction Review

Review period: ____________________ to ____________________

☐ Deposits reviewed ☐ Withdrawals reviewed ☐ Trading activity reviewed ☐ Payment methods reviewed ☐ Third-party transactions reviewed ☐ Geographic activity reviewed ☐ Transaction-monitoring alerts reviewed ☐ Unusual activity investigated ☐ Related accounts considered

I.8 Expected vs Actual Activity

Expected activity:

Actual activity:

Material difference identified?

☐ No ☐ Yes

If yes:

I.9 Risk Reassessment

Risk Factor	Previous	Current
Geographic	____	____
Customer Profile	____	____
PEP/Sanctions	____	____
SoF/SoW	____	____
Product/Transaction	____	____
Overall Risk	____	____

New Risk Rating: ________________________________

Reason for change:

I.10 Review Outcome

☐ Continue relationship ☐ Continue with enhanced monitoring ☐ EDD required ☐ Account restrictions required ☐ Senior approval required ☐ Relationship termination to be considered ☐ MLRO escalation required ☐ No further action

Reviewer: ______________________________________

Date: ____

Approver: ______________________________________

APPENDIX J — AML/CFT TRAINING REGISTER AND ANNUAL TRAINING PLAN

J.1 Purpose

This Appendix establishes the Company's minimum documentation requirements for AML/CFT training.

The training programme shall ensure that relevant employees understand the Company's AML obligations and can identify and escalate financial crime concerns.

J.2 Annual Training Plan

Training Area	Target Personnel	Frequency
AML/CFT Framework	All relevant staff	Annual
KYC/CDD	KYC / Compliance / Onboarding	Annual
Beneficial Ownership	KYC / Compliance	Annual
PEP & Sanctions	Compliance / Operations / Onboarding	Annual
Transaction Monitoring	Compliance / Operations	Annual

Training Area	Target Personnel	Frequency
Suspicious Activity Escalation	All relevant staff	Annual
Payment/Fraud Risks	Operations / Finance	Annual
Tipping Off & Confidentiality	All relevant staff	Annual
Regulatory Updates	Relevant personnel	As required
Role-Specific Training	Relevant personnel	As required

J.3 New Employee Training

New employees performing AML-sensitive functions shall receive appropriate AML training before independently performing material AML-related responsibilities.

Training shall be proportionate to:

- role;
- access to customer information;
- access to payment systems;
- decision-making authority; and
- financial crime exposure.

J.4 Training Register

Employee	Position	Training Date	Subject	Provider	Assessment	Completion

J.5 Training Effectiveness

Where appropriate, training shall include a knowledge assessment.

Assessment results shall be retained.

Where an employee demonstrates inadequate understanding of material AML responsibilities, additional training shall be provided.

J.6 Training Evidence

The Company shall retain, as appropriate:

- training materials;
- attendance records;
- training certificates;
- assessment results;
- training provider details;
- employee acknowledgements; and
- remediation records.

J.7 Annual Training Review

At least annually, Compliance shall assess whether training remains appropriate considering:

- regulatory developments;
- internal incidents;
- transaction-monitoring results;
- audit findings;

- new products;
- new payment channels;
- emerging financial crime typologies; and
- employee competency.

APPENDIX K — AML/CFT COMPLIANCE MONITORING AND TEST PLAN

K.1 Purpose

This Appendix provides a framework for testing whether the AML/CFT controls described in this Manual are operating effectively.

The monitoring programme shall be risk-based and shall focus greater attention on higher-risk areas.

K.2 Annual Monitoring Programme

Control Area	Test	Frequency
Individual KYC	File sample review	Quarterly / Risk-based
Corporate KYC	File sample review	Quarterly / Risk-based
UBO	Ownership verification sample	Quarterly
PEP Screening	Sample test	Quarterly
Sanctions Screening	Sample/system test	Quarterly
Risk Scoring	Recalculation sample	Quarterly
EDD	High-risk file review	Quarterly
Transaction Monitoring	Alert sample review	Quarterly
Suspicious Activity	Escalation file review	Quarterly
Payment Controls	Deposit/withdrawal testing	Quarterly
Periodic Reviews	Overdue review testing	Quarterly
Training	Training register review	Semi-annual
Outsourcing	Provider review	Annual
EWRA	Methodology review	Annual
AML Manual	Policy review	Annual
Independent AML Review	Independent testing	Periodic

The exact frequency may be adjusted according to the Company's size, transaction volumes and risk profile.

K.3 KYC Testing

A sample of customer files shall be tested to determine whether:

- required identity information was collected;
- documents were appropriately verified;
- beneficial ownership was established;
- risk assessment was completed;
- PEP screening occurred;

- sanctions screening occurred;
- SoF/SoW was obtained where required;
- EDD was completed where required; and
- approval was properly documented.

K.4 Transaction Monitoring Testing

Testing shall assess whether:

- relevant alerts were generated;
- alerts were assigned;
- investigations were conducted;
- supporting information was reviewed;
- conclusions were documented;
- suspicious matters were escalated; and
- alerts were closed appropriately.

The test shall consider both false negatives and false positives where practicable.

K.5 Sanctions Testing

Compliance shall periodically test whether:

- screening is performed at onboarding;
- screening lists are appropriately configured;
- relevant customer fields are screened;
- alerts are appropriately investigated;
- potential matches are escalated;
- confirmed matches are appropriately handled; and
- screening evidence is retained.

K.6 Payment Control Testing

Testing shall consider:

- customer-owned payment methods;
- third-party payments;
- withdrawal beneficiaries;
- payment method changes;
- unusual payment activity;
- rejected transactions;
- payment restrictions; and
- escalation procedures.

K.7 Finding Classification

Findings may be classified:

Critical: Immediate and significant financial crime or regulatory exposure.

High: Material control deficiency requiring prompt remediation.

Medium: Meaningful weakness requiring corrective action.

Low: Minor deficiency that should be corrected through normal improvement processes.

K.8 Remediation Register

Finding	Risk	Owner	Action	Due Date	Status

K.9 Follow-Up Testing

Material findings shall be subject to follow-up testing.

The finding shall not be marked “closed” merely because management states that remediation has occurred. Evidence of remediation shall be reviewed.

APPENDIX L — MLRO ANNUAL REPORT TO THE BOARD

L.1 Purpose

The MLRO shall provide the Board with periodic reporting concerning the operation and effectiveness of the Company's AML/CFT framework.

The following template may be used for the annual MLRO report.

L.2 Reporting Period

Reporting Period: ___________________________________

Prepared By: ____

Date: ____

L.3 Executive Summary

The MLRO shall provide a concise assessment of:

- overall AML/CFT risk;
- material changes during the year;
- effectiveness of the AML framework;
- material incidents;
- significant deficiencies;
- regulatory developments;
- outstanding remediation; and
- key priorities for the following year.

MLRO Assessment

L.4 Customer Risk Profile

Category	Number
Total Customers	
Low Risk	
Medium Risk	
High Risk	
PEP Customers	
Customers Subject to EDD	
Customers Rejected	
Relationships Terminated	

L.5 AML Activity

Indicator	Number
KYC Reviews Completed	
Overdue Reviews	
Transaction Monitoring Alerts	
Alerts Escalated to MLRO	
Suspicious Activity Investigations	
External Reports Made	
Sanctions Alerts	
Confirmed Sanctions Matches	
PEP Escalations	
EDD Cases	

L.6 Material AML Issues

The MLRO shall identify any material:

- suspicious activity;
- sanctions matters;
- fraud;
- payment-related financial crime;
- regulatory enquiries;
- control failures;
- employee breaches;
- outsourcing deficiencies;
- data/record issues; or
- other financial crime concerns.

Details

L.7 Compliance Monitoring

Reviews completed: ________________________________

Material findings: ________________________________

High-risk findings: _______________________________

Outstanding findings: ______________________________

Summary

L.8 Training

Employees requiring AML training: ____________________

Completed: ____

Outstanding: _______________________________________

Additional training required: _________________________

L.9 Risk Assessment

The MLRO shall report any material changes to:

- customer risk;
- geographic risk;
- payment risk;
- product risk;
- sanctions exposure;
- transaction-monitoring risk;
- outsourcing risk; and
- emerging financial crime threats.

Assessment

L.10 Remediation

Issue	Risk	Action	Owner	Due Date	Status

L.11 MLRO Recommendations

The MLRO shall provide recommendations concerning:

- policy amendments;
- systems;
- staffing;
- training;
- monitoring;
- risk appetite;
- payment controls;
- customer restrictions;
- outsourcing;
- independent testing; and
- Board oversight.

Recommendations

L.12 Board Acknowledgement

The Board acknowledges that it has reviewed the MLRO's report and considered the material AML/CFT matters identified.

Director: ________________________________

Signature: ________________________________

Date: ____________________________________

APPENDIX M — AML/CFT DEFINITIONS AND GLOSSARY

M.1 Purpose

This Glossary establishes consistent terminology for the AML/CFT framework.

Where a term has a specific legal meaning under applicable legislation, the statutory definition shall prevail over this internal glossary.

"AML"

Anti-Money Laundering.

Refers to measures designed to prevent, detect and respond to the laundering of proceeds of criminal activity.

"Beneficial Owner"

The natural person or persons who ultimately own or control a customer or on whose behalf a transaction or relationship is conducted.

"CDD"

Customer Due Diligence.

The process of identifying and verifying a customer, understanding beneficial ownership and obtaining information concerning the nature and purpose of the relationship.

"CFT"

Counter-Terrorist Financing.

Measures designed to prevent and detect the financing of terrorism or terrorist activity.

"Compliance Officer"

The person responsible for the day-to-day administration and monitoring of the Company's compliance framework, subject to the governance structure established by the Company.

"EDD"

Enhanced Due Diligence.

Additional customer due diligence measures applied where the financial crime risk is elevated.

"EWRA"

Enterprise-Wide Risk Assessment.

The Company's assessment of ML/TF and related financial crime risks across its business.

"Financial Crime"

For purposes of this Manual, financial crime includes money laundering, terrorist financing, sanctions evasion, fraud, corruption and other criminal or prohibited activity relevant to the Company's business.

"High-Risk Customer"

A customer whose risk assessment indicates elevated exposure to ML/TF or other financial crime risk requiring enhanced controls.

"KYC"

Know Your Customer.

The processes used to identify, verify and understand customers.

"MLRO"

Money Laundering Reporting Officer.

The person appointed by VG Markets to oversee the Company's AML/CFT framework, including suspicious activity escalation and reporting.

"Money Laundering"

The processing, concealment, conversion, transfer or use of proceeds of criminal activity with the purpose or effect of disguising their illicit origin, as defined under applicable law.

"Ongoing CDD"

The continuing process of reviewing customer information and transaction activity to ensure that the Company's understanding of the customer remains current and appropriate.

"PEP"

Politically Exposed Person.

An individual who is or has been entrusted with a prominent public function, together with relevant family members and close associates where applicable.

"Risk Appetite"

The level and type of financial crime risk that VG Markets is prepared to accept after considering its controls and regulatory obligations.

"Sanctions"

Financial or economic restrictions imposed by competent authorities or applicable sanctions regimes.

"Source of Funds"

The origin of the particular money or assets used for a transaction or account.

"Source of Wealth"

The origin of the customer's overall accumulated wealth.

"STR / Suspicious Transaction Report"

A report made to the relevant competent authority concerning a transaction or activity giving rise to the required level of suspicion under applicable law.

"Supervisory Authority"

The authority designated under applicable Anjouan AML legislation to perform the relevant AML supervisory and suspicious transaction reporting functions.

This term should not automatically be treated as synonymous with AOFA. The Company's final controlled document should preserve the distinction between AOFA as the financial-services regulator and the statutory AML Supervisory Authority established under the Money Laundering (Prevention) Act, Act 008 of 2005.

"Tipping Off"

The unauthorised disclosure of information concerning a suspicious transaction investigation, report or related regulatory/law-enforcement action where such disclosure is prohibited by applicable law.

"Transaction Monitoring"

The process of reviewing customer transactions and activity to identify unusual or potentially suspicious behaviour.

"UBO"

Ultimate Beneficial Owner.

The natural person or persons who ultimately own or control a customer.

"Third-Party Funding"

A deposit or payment made by a person other than the verified customer or an appropriately authorised account holder.

"Unusual Transaction"

A transaction or activity that differs materially from the customer's known profile, expected behaviour or normal activity.

An unusual transaction is not necessarily suspicious and requires appropriate assessment.

APPENDIX M.2 GOVERNANCE OF THE GLOSSARY

The MLRO or Compliance Officer shall review this Glossary when:

- applicable legislation changes;
- regulatory guidance changes;
- the Company's business model changes;
- new products are introduced;
- new financial crime typologies emerge; or
- material ambiguity in terminology is identified.

Where a statutory definition differs from an internal definition, the applicable law shall prevail.

APPENDIX M.3 DOCUMENT HIERARCHY

The following hierarchy shall apply when interpreting this Manual:

1. Applicable law;
2. Applicable licence conditions and regulatory requirements;
3. Applicable directions or requirements of competent authorities;
4. Board-approved AML/CFT Policy and Manual;
5. Supporting AML/CFT procedures;
6. Operational checklists and forms.

Where an inconsistency is identified, the matter shall be escalated to the MLRO/Compliance Officer for review and, where appropriate, legal advice.

End of AML/CFT Policy and Manual