VERSION 2.0

MAY 2026

RMCP

RMCP — Group AML/CFT framework under FICA, FSCA Conduct Standards and (for in-scope EU activities) AMLR/AMLD6.

LICENSED FSP

Raise Global SA (Pty) LTD

Reg. 2018/616118/07 · South Africa

FSCA Licence n° 50506

AUTHORIZED REPRESENTATIVE

Raise EU Services D.B LTD

Reg. HE428723 · Cyprus

Under Authorized Representative Agreement on behalf of Raise Global SA (Pty) LTD

VERSION

2.0

EFFECTIVE DATE

19 May 2026

OWNER

Kevin D. Wides · MLRO

REVIEW CYCLE

Annual, or upon regulatory change

RISK MANAGEMENT & COMPLIANCE PROGRAMME

RMCP

Group-level AML/CFT programme binding every RaiseFX entity, aligned to the FIC Act as amended by Act 22 of 2022 (post-greylist regime), FSCA Conduct Standards, and EU AMLR/AMLD6 plus Cypriot AML Law 188(I)/2007 for activities conducted by Raise EU Services D.B LTD as Authorized Representative.

0 Application to the RaiseFX Group

This Risk Management and Compliance Programme (RMCP) applies in its entirety to every entity within the RaiseFX group of companies (the Group). Where this document refers to the FSP, the Broker, RaiseFX or the institution, that reference is to be read as a reference to whichever entity within the Group has accepted the relevant client, individually and collectively, and the obligations bind each entity on the same basis.

ENTITY	IDENTIFIER	ROLE	JURISDICTION
Raise Global SA (Pty) LTD	Reg. 2018/616118/07 — FSCA FSP No. 50506	Licensed FSP and accountable institution under FICA	Republic of South Africa
Raise EU Services D.B LTD	HE428723 — TIN 10428723T — Limassol	Authorized Representative; EU-side client onboarding and servicing	Republic of Cyprus / European Union

Group governance is anchored as follows: David BOTTIN serves as Chief Executive Officer; Kevin D. Wides is the appointed Money Laundering Reporting Officer (MLRO) and Key Individual; a Deputy MLRO is designated for continuity. Where a provision is, by its nature, applicable only to one Group entity (for example, a reference to a national law, regulator, ombudsman or reporting authority), that provision applies to that entity only; all other provisions apply equally.

1 Purpose and legal framework

The RMCP discharges the obligation imposed by section 42 of the Financial Intelligence Centre Act 38 of 2001 (FIC Act) to establish, document, maintain and implement a risk management and compliance programme. It also gives effect to the firm's obligations under the FSCA Conduct Standards and, for activities conducted through Raise EU Services D.B LTD, EU AMLR (Regulation (EU) 2024/1624), AMLD6 (Directive (EU) 2024/1640) and Cypriot AML Law 188(I)/2007 as amended.

Primary South African instruments incorporated by reference:

- Financial Intelligence Centre Act 38 of 2001, as amended by the FIC Amendment Act 1 of 2017 and, materially, the General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act 22 of 2022 (the principal post-greylist instrument).
- Prevention and Combating of Corrupt Activities Act 12 of 2004 (POCDATARA companion).
- Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 (POCDATARA).
- Protection of Personal Information Act 4 of 2013 (POPIA) — interaction with CDD record-keeping.
- FSCA Conduct Standards applicable to authorised FSPs and the Financial Sector Regulation Act 9 of 2017.
- FIC Regulations, including Regulation 22B (cash threshold), Regulation 24(3) (STR timeline) and the updated PEP/DPIP regulations issued post-2022.
- Targeted Financial Sanctions reporting obligations under sections 26B and 26C of FICA, introduced by the 2022 amendments.
- FIC Directive 8 (Directive on the Screening of Employees of Accountable Institutions) issued under section 43A of FICA — employee screening obligations (see §14).

ⓘ

REFERENCE SOURCES

Operational interpretation is guided by FIC Public Compliance Communication 5A (Customer Due Diligence) and PCC 22 (PEP screening). These are practical guidance instruments; they do not displace the Act, the Regulations or this RMCP.

FATF status: South Africa was greylisted by the Financial Action Task Force on 24 February 2023 and removed from the grey list on 24 October 2025 after substantial closure of the action-plan items. RaiseFX continues to treat the residual risks identified in the FATF Mutual Evaluation cycle (beneficial-ownership transparency, sanctions effectiveness, STR quality) as live programme priorities and does not relax controls on the basis of de-listing.

2 Definitions and acronyms

TERM	MEANING IN THIS RMCP
Accountable institution	An institution listed in Schedule 1 to the FIC Act. Raise Global SA is an accountable institution; Raise EU Services D.B is an obliged entity under EU AMLR.
Beneficial owner	Natural person who ultimately owns or exercises effective control over a client or a natural person on whose behalf a transaction is conducted; control threshold 25% or such lower threshold where risk so requires.
Business relationship	An arrangement between the FSP and a client for the purpose of concluding transactions on a regular basis.
CDD / EDD	Customer Due Diligence / Enhanced Due Diligence.
Centre / FIC	Financial Intelligence Centre established under section 2 of the FIC Act.
CTR	Cash Threshold Report under section 28 of FICA.
DPIP	Domestic Prominent Influential Person — Schedule 3A FICA.
FPPO	Foreign Prominent Public Official — Schedule 3B FICA.
MOKAS	Cyprus Unit for Combating Money Laundering; EU-side FIU equivalent of the FIC.
PEP	Politically Exposed Person (FPPO, DPIP and immediate family members / known close associates).
RMCP	This Risk Management and Compliance Programme.
Single transaction	A transaction other than one concluded in the course of a business relationship, where the value is not less than the prescribed threshold.
STR	Suspicious and Unusual Transaction Report under section 29 of FICA.
TFS	Targeted Financial Sanctions reporting under sections 26B/26C of FICA.

3 Risk-based approach

RaiseFX applies a risk-based approach calibrated to the firm's client base (retail and professional FX/CFD traders), distribution model (online onboarding) and geographic footprint. Risk is assessed across four dimensions: client, product/service, channel and geography. A Business Risk Assessment is performed annually and refreshed on material change.

RISK DIMENSION	STANDARD RATING DRIVERS
Client	Occupation, source of wealth, PEP/DPIP/FPPO status, adverse media, sanctions hits, legal-person opacity, age of relationship.
Product / service	Leverage level, ability to fund via third parties, payout method, segregation of funds.
Channel	Non-face-to-face onboarding (default); use of electronic identity verification and liveness.
Geography	Client residency, IP location, FATF high-risk and other monitored jurisdictions, EU/UK/US/UN sanctions lists.

Each client is assigned a Low, Medium or High rating at onboarding and rerated on review or trigger event. The rating dictates the depth of CDD, the frequency of refresh and whether EDD applies.

4 Customer Due Diligence (CDD)

CDD is performed before a business relationship is established or a single transaction is concluded. The FSP does not maintain anonymous accounts and does not accept clients using fictitious names (FICA s.20A).

Identification and verification

- Natural persons: full names, date of birth, identity/passport number, nationality, residential address, contact details, occupation and source of funds.
- Legal persons: registered name, registration number, registered office and principal place of business, nature of business, directors and senior managers, and identification of every beneficial owner holding 25% or more (or exercising effective control below threshold).
- Trusts and partnerships: trust deed / partnership agreement, identification of trustees/partners, settlor, named and class beneficiaries, and any natural person exercising ultimate effective control.
- Verification is performed against independent and reliable sources: government-issued ID, electronic identity verification with liveness, registry extracts, utility/bank statements no older than three months.

Thresholds and timing

- Occasional / single-transaction CDD threshold: R5,000 / EUR 250 / USD 250.
- Records retention: 5 years from the end of the business relationship or the date of the transaction, whichever is later.
- Inability to complete CDD (FICA s.21E): the relationship is not established or is terminated, funds are not released, and the MLRO assesses whether an STR is required.

Established versus prospective clients

Prospective clients are persons with whom no business relationship has yet been formed; established clients are those onboarded and active. The FSP applies full CDD to both before any transaction is processed, and does not rely on grandfathering. Where a client previously onboarded is identified as having incomplete records under current standards, remediation CDD is triggered and trading restrictions are imposed until cleared.

5 Enhanced Due Diligence (EDD)

EDD applies whenever the risk rating is High or any of the following triggers is present: residence or material nexus to a FATF high-risk or other monitored jurisdiction; complex or opaque ownership; cash-intensive source of funds; adverse media on financial crime; or any trigger identified in ongoing monitoring. PEP/DPIP/FPPO status (and immediate family members / known close associates) is treated separately: such persons are **not accepted as clients** under the FSP's client-acceptance policy (see §6), so the EDD route below does not arise for them.

- Senior management approval is required to establish or continue the relationship.
- Source of funds and source of wealth are documented and independently corroborated.
- Account activity is reviewed on a heightened cadence (no less than annually; quarterly for High risk).
- Where ownership is opaque, the FSP traces the chain to the natural-person beneficial owner(s) and records each layer.

COMPLEX OWNERSHIP STRUCTURES

Multi-jurisdictional layering, nominee shareholders, bearer-share regimes and shell entities without economic substance trigger automatic EDD. If the natural-person beneficial owner cannot be identified to the FSP's reasonable satisfaction, the relationship is not opened or is exited.

6 PEPs, DPIPs, FPPOs and Sanctions — Client-Acceptance Policy

PEP screening is performed at onboarding and continuously thereafter against a commercial screening provider whose dataset covers UN, OFAC, EU, UK HMT, FSCA, FIC and Cyprus sanctions and PEP lists. Categories per FICA Schedules 3A and 3B (as updated by the post-2022 regulations) cover FPPOs, DPIPs and immediate family members and known close associates.

⚠ **DPIP / FPPO EXCLUSION — THE FSP DOES NOT ONBOARD POLITICALLY EXPOSED PERSONS**

The FSP has adopted a policy of **not accepting as clients** any person identified as a Domestic Prominent Influential Person (DPIP, Schedule 3A FICA), a Foreign Prominent Public Official (FPPO, Schedule 3B FICA), or an immediate family member or known close associate of such a person. This policy applies at the onboarding stage and to any existing client who subsequently becomes a DPIP, FPPO or associated person during the course of the business relationship.

Rationale. As a small FSP, the enhanced due diligence, source-of-wealth verification, senior-management approval and ongoing enhanced-monitoring obligations imposed in respect of such persons present a compliance burden disproportionate to the scale of the firm's operations. The FSP has determined that the risk of inadvertent non-compliance in respect of these clients outweighs the commercial benefit of accepting them. This client-acceptance policy is effective 2 June 2026, approved by Kevin Douglas Wides (Key Individual / Director / FICA Compliance Officer); the FICA Compliance Officer reviews it at least every six months.

Procedure on identification. Where a prospective client — or the beneficial owner of a prospective client — is identified as falling within the above categories, the employee declines to onboard the client and informs the FICA Compliance Officer (Kevin Douglas Wides). Where an existing client becomes a DPIP, FPPO or associated person, the FICA Compliance Officer notifies the client that the business relationship will be terminated, within a reasonable period, in accordance with the off-boarding procedure, and assesses whether any reporting obligation (STR / TFS) arises. Every positive or partial PEP/DPIP/FPPO screening hit is escalated to the MLRO before any account is funded; FIC PCC 22 is the operative guidance for screening calibration and false-positive disposition.

Sanctions hits are treated separately from PEP hits (see §11). A confirmed sanctions match is never a risk-rating exercise — it is a prohibition.

7 Ongoing monitoring and transaction monitoring

Ongoing CDD (FICA s.21C) requires the FSP to scrutinise transactions undertaken throughout the course of the relationship to ensure they are consistent with the FSP's knowledge of the client, the client's business and risk profile and, where necessary, source of funds.

- Automated transaction monitoring runs daily on deposit, withdrawal and trading patterns.
- Rule library covers: rapid movement of funds, third-party funding, structuring below CTR threshold, dormant-then-active accounts, geographic anomalies and inconsistent risk profile.
- Alerts are triaged by Compliance; escalated alerts are reviewed by the MLRO and dispositioned within 5 business days where practicable.
- Periodic refresh of CDD: Low 36 months, Medium 24 months, High 12 months, or sooner on trigger.

Where information previously obtained gives rise to doubt (FICA s.21D), the FSP re-verifies and, where re-verification fails, applies s.21E (inability to conduct CDD) and considers an STR.

8 Reporting obligations: STRs, CTRs, TFS

Suspicious and Unusual Transaction Reports (STRs)

Every employee who forms a suspicion that a transaction or proposed transaction may involve the proceeds of unlawful activities, terrorism financing or any other matter listed in section 29 of FICA must report internally to the MLRO without delay. The MLRO assesses and, where the suspicion is confirmed, files the STR with the Financial Intelligence Centre via goAML within 15 business days of the determination (FIC Regulation 24(3)). For Raise EU Services D.B activities the equivalent filing is made with MOKAS in Cyprus.

⚠ **STR CONFIDENTIALITY**

The fact that an internal report has been made, that an STR has been filed, or that the Centre is investigating, is strictly confidential. It must not be disclosed to the client, to any related party, or to any employee not authorised by the MLRO. Breach is a criminal offence under FICA s.29(3) and (4).

Cash Threshold Reports (CTRs)

Cash transactions of R49 999 or more, per FIC Regulation 22B, whether as a single amount or as an aggregate of smaller amounts that together come to R49 999 or more, are reported to the Centre within the prescribed period. The FSP's business model does not contemplate cash receipts; any cash tendered is refused and the event itself is escalated to the MLRO for STR consideration.

Targeted Financial Sanctions reporting (TFS)

Under sections 26B and 26C of FICA (introduced by the 2022 Amendment Act), the FSP must, without delay, freeze property and report to the Centre where the FSP holds or controls property owned or controlled by, or on behalf of, a person or entity designated under United Nations Security Council Resolutions or the domestic targeted financial sanctions list. The freeze precedes any client communication, subject to the tipping-off prohibition.

Freezing of property

Where the FSP, in the course of a transaction or on a CDD review, identifies that it holds or controls property belonging to or on behalf of a designated person or entity, the FSP must immediately freeze that property without alerting the client (FICA ss 26B and 26C). Freezing steps are as follows:

- The MLRO issues a freeze instruction to the operations and finance teams; all withdrawals, transfers and dealings in the relevant property are suspended immediately.
- A TFS report is filed with the FIC via goAML within 5 business days of identification; for EU-side activity the equivalent report is filed with MOKAS and the relevant EU competent authority.

- No funds are released, no contract is varied, and no service is rendered in respect of the frozen property, unless authorised by the Centre or a competent court.
- The freeze and all related actions are documented, timestamped and retained for 5 years.
- No information about the freeze is communicated to the client or any third party (tipping-off prohibition — FICA s 29).

⚠ **FREEZE FIRST — NO EXCEPTIONS**

A freeze under ss 26B/26C is mandatory and immediate. No business-unit approval, client instruction or senior-management authorisation can override or delay it. Any employee who releases frozen property without Centre authorisation commits a criminal offence.

9 Record-keeping and information requests

The FSP keeps CDD records (s.22 FICA), transaction records (s.22A FICA) and all internal and external reports, screening evidence and risk-rating decisions for 5 years from the end of the business relationship or the date of the transaction, whichever is later. Records may be kept in electronic form and may be held by a third party provided the FSP retains free and easy access (FICA s.24).

- CDD records: copies of, or references to, identification and verification information obtained by the FSP at onboarding and on refresh.
- Transaction records: nature, amount, currency, date, parties, accounts and instructions for every transaction.
- Reporting records: internal escalation, MLRO disposition, FIC/MOKAS filing reference, and any follow-up correspondence.
- Access by the Centre or an authorised representative (FICA s.27A) is granted on production of the prescribed authorisation; the request and the response are logged.

10 Tipping-off prohibition and confidentiality

⚠ **TIPPING-OFF PROHIBITION**

No employee, officer, director or agent of the FSP may disclose to the client or to any third party that an internal report has been made, that an STR or TFS report has been filed, that information has been furnished to the Centre, or that a transaction is or may be the subject of an investigation. This prohibition is absolute and survives the termination of employment. Breach is a criminal offence under FICA s.29.

Permissible communications include lawful requests for further CDD information from the client, provided they are framed as routine refresh and do not reveal the existence of a report or investigation. All such communications are scripted and approved in advance by the MLRO.

11 Sanctions screening framework

Sanctions screening is performed at onboarding, on every CDD refresh, on every payment instruction and on each sanctions-list update (intra-day, automated). Screening covers UN, OFAC (SDN and sectoral), EU consolidated, UK HMT OFSI, FSCA, FIC TFS designations and Cyprus national designations.

> ⚠ **AUTO-PROHIBITED RULE**
>
> A confirmed sanctions match is a PROHIBITION, not a risk factor. The account is frozen immediately, no funds are released, no communication is sent to the client, and the MLRO files a TFS report under FICA s.26B/26C (or with MOKAS for EU-side activity) without delay. No business unit, including senior management, may override a confirmed sanctions match.

Partial matches and homonym hits are escalated to a four-eyes review. Dispositions and supporting evidence are recorded against the screening event and retained for 5 years.

12 EU layer — Raise EU Services D.B LTD as Authorized Representative

> ⓘ **EU LAYER POINTER**
>
> This section governs activities conducted by Raise EU Services D.B LTD as Authorized Representative of Raise Global SA. It supplements, and does not displace, the FICA-based framework set out in §§1–11.

For activities in or into the European Union, Raise EU Services D.B LTD operates under:

- EU AMLR — Regulation (EU) 2024/1624 on the prevention of the use of the financial system for money laundering or terrorist financing — directly applicable rulebook for obliged entities.
- AMLD6 — Directive (EU) 2024/1640 on the mechanisms to be put in place by Member States, transposed via Cypriot national law.
- The Anti-Money Laundering Authority (AMLA): supervisory expectations applicable once AMLA becomes operational, including direct supervision of selected obliged entities and indirect supervision via national authorities.
- Cypriot AML Law 188(I)/2007, as amended through 2024 — the Prevention and Suppression of Money Laundering and Terrorist Financing Law.
- CySEC Directive on the Prevention and Suppression of Money Laundering and Terrorist Financing — the operative supervisory standard for CIFs and connected entities in Cyprus.
- Cyprus FIU (MOKAS) as the reporting route for STRs originating from Raise EU Services D.B activities — the EU equivalent of the FIC.

Where a client is onboarded by Raise EU Services D.B, the EU framework is the primary regime, with FICA applying only to interactions that touch Raise Global SA. The MLRO function is unified at Group level; the EU entity maintains a local AML compliance contact for MOKAS liaison and CySEC inspections. Mutual access to CDD records is granted between Group entities subject to GDPR and POPIA constraints.

13 Governance: Board, MLRO, Deputy MLRO, Compliance Committee

Under the FSCA Conduct Standards and FICA s.42A, an accountable institution must designate a person responsible for compliance with the Act. RaiseFX has appointed Kevin D. Wides as MLRO with full responsibility for STR filings, sanctions screening oversight and FIC liaison. A Deputy MLRO is appointed for continuity.

ROLE	HOLDER / BODY	CORE RESPONSIBILITIES
Board of Directors	Raise Global SA Board	Approves the RMCP, the Business Risk Assessment and the AML budget; reviews quarterly MI.
CEO	David BOTTIN	Accountable executive for the AML/CFT programme; tone-from-the-top; resourcing.
MLRO	Kevin D. Wides	Receives internal reports; files STRs and TFS reports with the FIC (and MOKAS for EU activity); owns sanctions screening; primary regulator liaison.
Deputy MLRO	Designated alternate	Acts in the MLRO's absence with identical authority; ensures continuity of reporting timelines.
Compliance Committee	MLRO, Compliance, Risk, Legal, Operations	Meets at least quarterly; reviews alerts, EDD cases, training, regulatory change.
Internal Audit	Independent function (may be outsourced)	Performs the periodic independent review of the AML programme (see §15).

14 Training and awareness

Every employee, director and outsourced operator with client-facing or transaction-handling responsibilities completes AML/CFT training at induction and at least annually thereafter. Training is calibrated to role: front-office staff receive client-onboarding and red-flag content; finance and operations receive transaction-monitoring and sanctions content; the Board receives a governance and regulatory-update briefing.

- Content covers FICA (as amended by Act 22 of 2022), the FATF post-greylist environment, FIC PCC 5A and PCC 22, EU AMLR/AMLD6 for EU-facing staff, and the firm's own RMCP.
- Attendance and assessment results are recorded by HR and reviewed by the MLRO.

- Failure to complete mandatory training results in access restrictions until remediated.

Screening of employees — FIC Directive 8

The FSP applies appropriate screening measures to prospective and current employees in compliance with FIC Directive 8 (Directive on the Screening of Employees), issued under section 43A of FICA. The obligation applies to all employees who have, or will have, access to or involvement in:

- client onboarding, CDD and EDD processes;
- transaction processing, withdrawal authorisation or funds handling;
- AML/CFT reporting (STR, CTR, TFS) or sanctions screening;
- compliance, risk or internal audit functions with access to client or AML data.

Screening covers, at minimum: criminal record checks (South African Police Service clearance, or equivalent for foreign nationals); credit and financial-integrity checks where role-relevant; verification of identity, qualifications and employment history; and, for senior or compliance roles, directorships, regulatory-disqualification and adverse-media checks. Screening is repeated on promotion, material role-change and, for high-risk roles, periodically thereafter. Results are retained securely and access is restricted to HR and the MLRO. Where a screening outcome reveals a disqualifying matter, the MLRO is notified and the placement or continued employment is suspended pending a risk decision by senior management.

15 Independent review and Internal Audit

An independent review of the AML/CFT programme is performed at least every 24 months by Internal Audit or by an external specialist not involved in the design or day-to-day operation of the programme. The review covers governance, the Business Risk Assessment, CDD/EDD execution quality, transaction monitoring effectiveness, sanctions screening, STR/CTR/TFS reporting timeliness and accuracy, record-keeping, and training.

Findings are tracked to closure by the Compliance Committee with target dates and owners; material findings are escalated to the Board at the next sitting. Regulator-led inspections (FSCA, FIC, CySEC, MOKAS) are coordinated by the MLRO.

16 Whistleblowing

The FSP maintains a confidential whistleblowing channel through which any employee, contractor or third party may report suspected money laundering, terrorist financing, sanctions evasion or any breach of this RMCP. Reports may be made anonymously. The Protected Disclosures Act 26 of 2000 protects whistleblowers from occupational detriment; the EU Whistleblower Directive (Directive (EU) 2019/1937), as transposed into Cypriot law, provides equivalent protection for EU-facing reports.

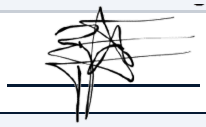
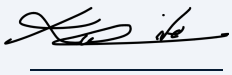
Reports are received by the MLRO and, where the MLRO is conflicted, by the Chair of the Compliance Committee. Retaliation is itself a disciplinary offence.

17 Approval, version and review

FIELD	VALUE
Document	Risk Management and Compliance Programme (RMCP) — RaiseFX Group
Owner	MLRO — Kevin D. Wides
Approved by	Board of Raise Global SA (Pty) LTD
Version	March 2025 — post-greylist-exit refresh
Next scheduled review	Annual, or on material regulatory change
Distribution	All staff via the firm's policy register; provided to FSCA, FIC, CySEC and MOKAS on request

This RMCP supersedes all prior versions. Where a prior procedure conflicts with this document, this document prevails. Operational annexes (screening calibration, EDD checklist templates, training curriculum, BRA workbook) are maintained separately and reviewed on the same cycle.

APPROVAL & SIGN-OFF

APPROVED BY	David BOTTIN
POSITION	Chief Executive Officer (CEO) — RaiseFX Group
SIGNATURE	
APPROVED BY	Kevin Douglas Wides
POSITION	Key Individual & FICA Compliance Officer — Raise Global SA (FSCA n° 50506)
SIGNATURE	
DATE	19 May 2026

DOCUMENT ID
RFX-RMCP-V2.0

VERSION
2.0

EFFECTIVE
19 May 2026

NEXT REVIEW
19 May 2027

OWNER
Kevin D. Wides · MLRO

REGULATOR
FSCA n° 50506

— End of Document —