

KYC & AML POLICY

RaiseFx is committed to the highest standards of the Anti-Money Laundering (AML) compliance and Counter-Terrorism Financing (CTF).

To help the governments fight the funding of terrorism and money laundering activities, law requires all financial institutions to obtain, verify, and record information that identifies each person opening an account.

Definitions

RaiseFx uses the following definitions :

- Money laundering – the process of converting funds, received from illegal activities (such as fraud, corruption, terrorism, etc.), into other funds or investments that look legitimate to hide or distort the real source of funds.

The process of money laundering can be divided into three sequential stages:

- Placement. At this stage, funds are converted into financial instruments, such as checks, bank accounts, and money transfers, or can be used for purchasing high-value goods that can be resold. They can also be physically deposited into banks and non-bank institutions (e.g., currency exchangers). To avoid suspicion by the company, the launderer may as well make several deposits instead of depositing the whole sum at once, this form of placement is called smurfing.
- Layering. Funds are transferred or moved to other accounts and other financial instruments. It is performed to disguise the origin and disrupt the indication of the entity that made the multiple financial transactions. Moving funds around and changing in their form makes it complicated to trace the money being laundered.
- Integration. Funds get back into circulation as legitimate to purchase goods and services.

RaiseFx adheres to the principles of Anti-Money Laundering and actively prevents any actions that aim or facilitate the process of legalizing of illegally gained funds. AML policy means preventing the use of the company's services by criminals, with the aim of money laundering, terrorist financing or other criminal activity.

To prevent money laundering, RaiseFx neither accepts nor pays cash under any circumstances. The company reserves the right to suspend any client's operation, which can be regarded as illegal or, may be related to money laundering in the opinion of the staff.

KYC & AML POLICY

Company Procedures

RaiseFx will make sure that it is dealing with a real person or legal entity.

RaiseFx will also perform all the required measures in accordance with applicable law and regulations, issued by monetary authorities. The AML policy is being fulfilled within RaiseFx by means of the following:

- Know your customer policy and due diligence
- Monitoring of client activity
- Record keeping

Know Your Customer and Due Diligence

Because of the company's commitment to the AML and KYC policies, each client of the company has to comply with a verification procedure.

Before RaiseFx can have full cooperation with the client, the company ensures that satisfactory evidence is produced or such other measures that will produce satisfactory evidence of the identity of any customer or counterparty are taken.

The company as well applies heightened scrutiny to clients, who are residents of sensitive countries, having inadequate AML standards or that may represent a high risk for crime and corruption and to beneficial owners who reside in and whose funds are sourced from named countries.

Individual clients

To get the full privileges of working with RaiseFx, each client provides personal information, specifically: full name; date of birth; country of origin; and complete residential address.

For this purpose, the client must send the following documents (in case the documents are written in non-Latin characters: to avoid any delays in the verification process, it is necessary to provide a notarized translation of the document in English) because of the requirements of KYC and to confirm the indicated information:

- Current valid passport (showing the first page of the local or international passport, where the photo and the signature are clearly visible); or Driving license which bears a photograph; or National identity card (showing both front and back pages);

KYC & AML POLICY

- Documents proving current permanent address (such as utility bills, bank statements, etc.) containing the client's full name and place of residence. These documents should not be older than 3 months from the date of filing.

Corporate clients

In case the applicant company is listed on a recognised or approved stock exchange or when there is independent evidence to show that the applicant is a wholly owned subsidiary or a subsidiary under the control of such a company, no further steps to verify identity will normally be required.

In case the company is unquoted and none of the principal directors or shareholders already has an account with RaiseFx, the following documentations must be provided:

- Certificate of Incorporation or any national equivalent;
- Memorandum and Articles of Association and statutory statement or any national equivalent;
- Certificate of good standing or other proof of registered address of the company;
- Resolution of the board of directors to open an account and confer authority on those who will operate it;
- Copies of powers of attorney or other authorities given by the directors in relation to the company;
- Proof of identity of directors in case he/she will deal with Vantage on behalf of the Customer (according to the Individual identity verification rules described above);
- Proof of identity of the beneficial owner(s) and/or the person(s) on whose instructions the signatories on the account are empowered to act (according to the Individual identity verification rules described above).

Monitoring of client activity

In addition to gathering information from the clients, RaiseFx continues to monitor the activity of every client to identify and prevent any suspicious transactions.

A suspicious transaction is known as a transaction that is inconsistent with the client's legitimate business or the usual client's transaction history known from client activity monitoring. RaiseFx has implemented the system of monitoring the named transactions (both automatic and, if needed, manual) to prevent using the company's services by criminals.

KYC & AML POLICY

Record keeping

Records must be kept of all transaction data and data obtained for the purpose of identification, as well as of all documents related to money laundering topics (e.g. files on suspicious activity reports, documentation of AML account monitoring, etc.). Those records are kept for a minimum of 5 years after the account is closed.

Deposit and withdrawal requirements

All deposits and withdrawals on trading accounts held with RaiseFx the following strict requirements:

Due to AML laws and standards, RaiseFx cannot receive or deposit funds to third parties.

Funds sent to RaiseFx must be from a bank account, Credit/Debit card or Alternative Payment Method under the same name as the trading account name with RaiseFx.

All funds withdrawn from a trading account must go to a bank account, Credit/Debit card or Alternative Payment Method under the same name as the trading account name with RaiseFx.

All withdrawal requests are processed on First-in-First-Out (FIFO) basis according to the funding source of origination. For example, a deposit is made via Debit/Credit Card; then a subsequent withdrawal request is received. The amount of funds sent back to the relevant Debit/Credit Card, when a withdrawal request is received, may not exceed the original amount deposited. Any profits made in excess of the deposited amount will be transferred to a nominated bank account; which must be held in the same name as the trading account.

For example, a customer deposits \$100 via Credit Card and earns a profit of \$1,000. Requesting a withdrawal of \$1,000, he will get \$100 to his Credit Card and the rest \$900 to his bank account.

All initial withdrawal requests must be verified for safety and security by provision of a bank statement; which includes account holder information and bank details. RaiseFx will not accept deposits or withdrawals made under a different name than the registered RaiseFx account.

If a trading account was credited in a way that cannot be used for funds withdrawal, the funds may be withdrawn to a bank account under the same name as the trading account

KYC & AML POLICY

name with RaiseFx as long as the client provides satisfactory evidence of the ownership of bank account where the funds originated from as well as the destination bank account.

Measures taken

In cases of an attempt to execute transactions which RaiseFx suspects are related to money laundering or other criminal activity, it will proceed in accordance with the applicable law and report suspicious activity to the regulating authority.

A handwritten signature in black ink, appearing to read "Daniel Sun", is written over a horizontal line. The signature is stylized and somewhat cursive.

date: 11/11/2023

position: MLRO



RAISE GLOBAL SA (Pty) Ltd

2018/616118/07

PEP & Sanctions Monitoring - iDenfy

An authorised Financial Services Provider FSP No: 50506

AUGUST 2023



1. iDenfy as AML and eKYC Service Provider:

RaiseFX relies on iDenfy, a reputable provider of AML (Anti-Money Laundering) and eKYC (Electronic Know Your Customer) services. iDenfy is recognized as a leading vendor in the market, trusted by many financial institutions such as the National Bank of Lithuania.

2. Daily AML & Sanctions & PEP Monitoring:

AML, Sanctions, and PEP (Politically Exposed Persons) monitoring are integral components of RaiseFX's risk management strategy. This monitoring is conducted daily for both new and existing clients using iDenfy's services. Therefore, in the instance an existing client has been recently flagged for an AML issue, iDenfy will automatically notify RaiseFX via API.

3. Integration with iDenfy via API Callback:

The integration with iDenfy is facilitated through API callbacks, ensuring a seamless and real-time connection for obtaining monitoring results. This approach enhances the efficiency of the AML and eKYC processes at RaiseFX.

4. Details on iDenfy's Services and Integration:

For a comprehensive understanding of iDenfy's services and its integration with RaiseFX, detailed information can be found in the provided links:

iDenfy's Anti-Money Laundering Services:

<https://help.idenfy.com/space/RC/415399948/Anti-Money+Laundering>

iDenfy's AML Sanctions List:

<https://help.idenfy.com/space/RC/415563796/AML+sanctions+list>

5. Probability and Fuzziness in AML Monitoring:

RaiseFX has implemented a sophisticated scoring system for AML monitoring, assigning a default score of 95 out of 100. This score allows for a certain level of flexibility, accommodating minor variations such as misspelled letters in clients' names. The stringent criteria help maintain a high level of accuracy in identifying potential risks.

6. Logic Used in AML and Sanction Monitoring:

The logic applied in AML and Sanction monitoring is outlined in detail in the provided link:

iDenfy's Logic for AML Sanction Monitoring:

<https://documentation.idenfy.com/fraud/AmlSanctionMonitoring>

In summary, RaiseFX has chosen iDenfy as a trusted partner for AML, PEP & Sanctions Monitoring and eKYC services, employing a robust daily monitoring process supported by advanced scoring and logic to ensure comprehensive compliance with regulations and to mitigate financial risks associated with money laundering and sanctioned entities. We have attached one of iDenfy's company presentation PDFs for your review.



RaiseFX
YOUR TRADING PARTNER

RAISE GLOBAL SA (Pty) Ltd

2018/616118/07

RISK MONITORING COMPLIANCE FRAMEWORK

An authorised Financial Services Provider FSP No: 50506

AUGUST 2023



Table of Contents

1.	Overview	3
2.	What is Compliance Risk Management?	3
3.	What is Compliance Risk?	4
4.	Establishment of an Independent Compliance function	4
5.	Compliance Risk Control Strategy	4
6.	Monitoring Framework	6
7.	Corrective measures	7
8.	Governance Structure	8
9.	Tools	8
10.	Authority and Mandate	8



1. Overview

RAISE GLOBAL SA (PTY) LTD has outsourced their Compliance to - **Oracle Compliance (Pty) Ltd**. They are an External FAIS Compliance Practice accredited by the Financial Services Conduct Authority. They are an independent compliance practice with an appropriate skills base to support Financial Services Providers (FSP's) in the identification and management of its compliance risks, to find solutions to compliance risk issues and to provide a professional compliance risk analysis, control, reporting and monitoring service to the FSP.

The practice seeks to provide a service that conforms to the standards of conduct set out by the Compliance Institute of South Africa. These standards stipulate a need to promote ethical behaviour, promote desired standards of conduct and to benchmark standards of expected behaviour and conduct amongst other requirements. The Practice therefore has a responsibility to mentor and guide FSP's in the spirit of various legislations and industry to empower the FSP to maintain its integrity and to provide professional services in line with customer needs and expectations.

Oracle Compliance has designed a Compliance risk management framework that describes the processes, systems and tools for compliance management. It entails developing and communicating an effective compliance risk programme which addresses the structural, operational and maintenance elements of compliance risk management. The compliance risk management framework is an integral part of the overall enterprise risk management plan for financial services providers to ensure that compliance obligations and processes are properly understood and incorporated into the business model. This is also necessary to assist management to appreciate their extent of accountability for compliance and that once compliance processes are imbedded they are applied consistently to all business processes.

Oracle Compliance assists the FSP with practical processes and procedures to help ensure that the FAIS and FICA obligations amongst other legislations are complied with and that the client is lead into making an informed decision. Its work ethic is based on years of experience in sound compliance & legal research in financial services.

As external FAIS Compliance Officers, they have an obligation to ensure that FAIS compliance processes and controls are embedded within the Financial Services Provider to ensure compliance with the requirements. To this end, a formal monitoring programme is required. Each monitoring session will focus on a different theme and over the year all the majority of FAIS required controls will be monitored and reviewed.

Oracle Compliance uses a customisation of The Compliance Institute of South Africa's (CI) risk management methodology. This methodology is an industry "best practice" for compliance risk management. Control measures are defined to mitigate the risks highlighted in a Risk management plan (RMP). A monitoring checklist is constructed based on the high and medium risks identified in the RMP. This is used throughout the period under review together with our audit report tool to test whether the control measures in the RMP are being adhered to.

2. What is Compliance Risk Management?

Compliance risk management entails adherence to legislation, regulations, and supervisory requirements. These range from managing conflicts of interest, observing proper standards of market conduct, treating customers fairly by ensuring that they understand products offered and that the product suits the needs of the client. and ensuring suitability of customer advice. Compliance ranges from requirements that are legally binding to that require a mere demonstration of honesty, integrity and ethical conduct.



3. What is Compliance Risk?

This is the risk that rises from non-compliance with legal or regulatory requirements, supervisory requirements or industry codes of conduct. Consequences of non-compliance could mean imprisonment or sanction for non-compliance, material financial loss, reputational damage, claims for damages, withdrawal or suspension of licence. Therefore, Oracle compliance has a role to ensure that management and internal audit are satisfied that effective compliance policies and procedures are in place and that the appropriate corrective action is taken by management in the event of breaches of laws, regulations or supervisory requirements. Further that proper and adequate reporting is communicated to the Authority in cases of compliance and non-compliance.

4. Establishment of an Independent Compliance function

In line with the Financial Advisory and Intermediary Services Act, Oracle compliance must establish an independent compliance function that is free from any actual or perceived conflict of interest. Oracle Compliance as an External compliance function shall at all times function independently from functions such as internal audit and shall be able to demonstrate its independence.

5. Compliance Risk Control Strategy

Oracle Compliance in collaboration with the internal compliance representative of the FSP will identify, risk-weight and interpret applicable generic laws, regulations and supervisory requirements posing a compliance risk to the FSP.

Oracle compliance has devised means of controlling compliance risks by:

1.	Devising a compliance management framework that is appropriate, effective and utilised in managing the risks of the organisation. The framework endeavours to accurately identify compliance requirements and is made readily available to management.
2.	Identifying areas in which legal, regulatory breach may occur. This is when the FSP does not meet its obligations, processes or standards of conduct. These are structured at the organisational level, or by division, department, function or process, for example, human resources, accounting, sales, marketing, etc. Determine their scope of applicability and disciplinary procedures. These must be available to all employees, relevant stakeholders and must be user friendly.
3.	Identifying, designing and implementing controls in areas that are not regulated but are germane to the success of the business such as industry codes of conduct, policies and procedures and quality management.



4.	Identifying and communicating any changes to laws and regulations, changes to or the introduction of new obligations that may have and direct or indirect impact on the organisation both on a minimal or major scale.
5.	Ensure that there are controls in place to monitor the FSP's compliance with obligations emanating from laws, regulations, industry codes and conduct and acceptable ethical conduct.
6.	Ensure that FSP's have a compliance risk management framework to manage the FSP such as processes, controls, policies, templates, registers
7.	Ensure that all compliance requirements stipulated by law or regulations are adopted
8.	Work with management to devise a compliance risk universe where all risks identified are categorised in order of priority and impact and that appropriate controls are implemented to minimise the risks identified. This ranges from low to high risk depending on the gravity of the risk.
9.	Create a regulatory risk compliance framework where risks pertaining to Legislation, Regulation, Government Directives, Contract or Standards linked to Government Directives, Licenses, Permits or Accreditations are tabulated, ranked and complied with.
10.	Imbed mechanism of identifying which actions must be taken to comply with obligations and the extent of the compliance.
11.	Making sure the status of the organisation's compliance obligations is regularly monitored, reviewed and minuted in quarterly management meetings. Monitoring may be routine/on-going monitoring procedures, or through the application of specific monitoring techniques. The compliance monitoring must be conducted by management in liaison with Oracle.
12.	Monitoring allows the practice to identify compliance weaknesses, monitor effectiveness of controls and to review the integrity of the compliance framework
13.	Report as required any breaches to management and the Authority
14.	Promote a culture of compliance within the organisation
15.	Promote compliance awareness, train staff on applicable legislation, follow up on non-compliance, compile exception reports that are timeous, accurate and comprehensive enough to understand the business activities

Compliance risks and the shortcomings of controls may also be identified by:

- The identification of generic and business specific compliance risks;
- analysis of incidents of past and current incidents of non-compliance including past losses and adverse outcomes;
- monitoring current incidents of compliance process breakdowns and losses;
- monitoring the audit process and the assessment of business performance relating to compliance; and
- assessment of the effectiveness of the compliance risk management processes.

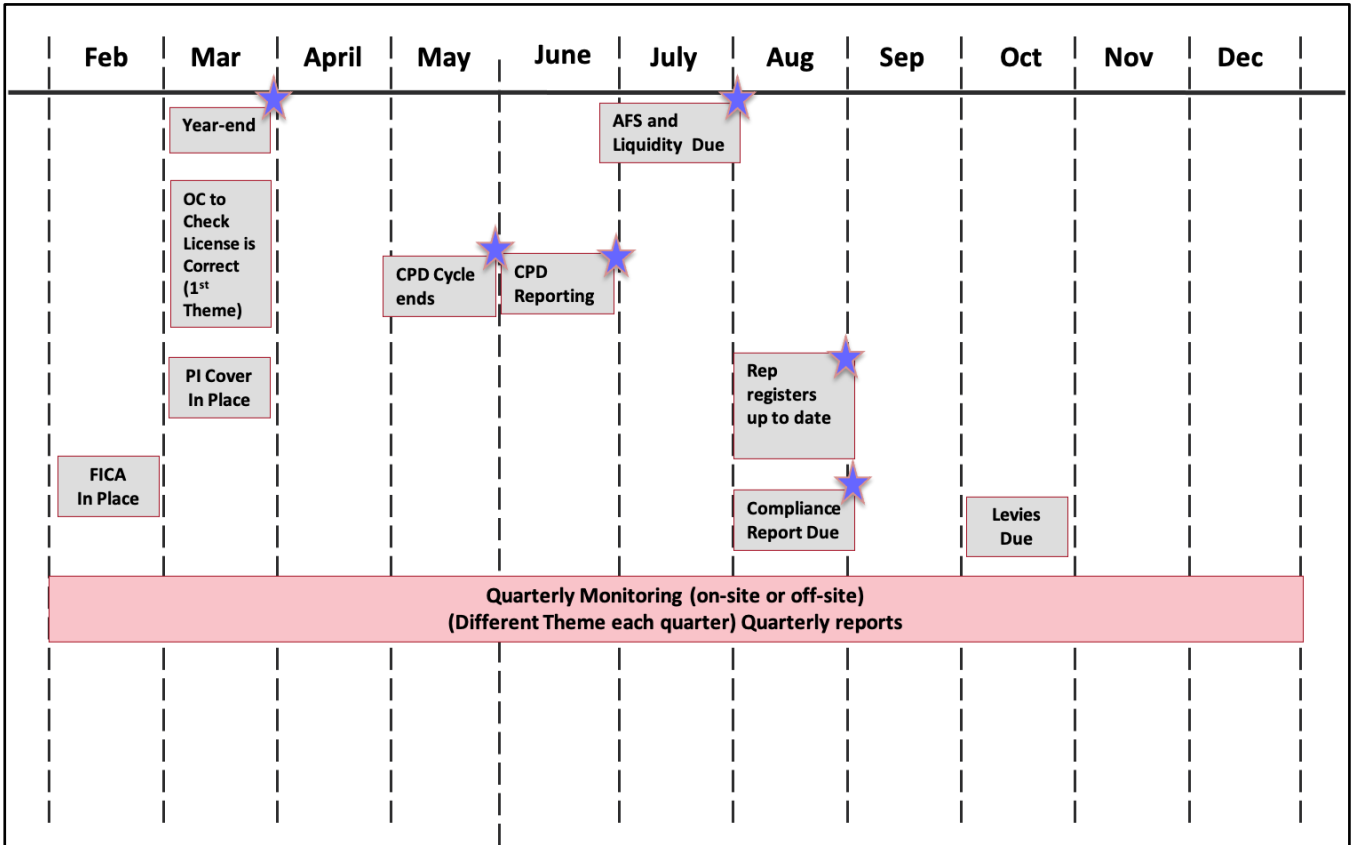


6. Monitoring Framework





High level yearly plan



7. Corrective measures

Oracle Compliance will compile a list of issues identified during monitoring such as:

- all instances of non-compliance;
- report non-compliance to management and stakeholders with immediate effect;
- agree on corrective action with all concerned;
- implement corrective action without undue delay;
- document findings and corrective action;
- monitor the implementation and progress of the corrective action up to sign-off of non-compliance resolution;
- report on progress of corrective action to the Authority and the relevant risk and audit committees up to sign-off of non-compliance resolution;



8. Governance Structure

The Board and Executive management of the FSP ensures that there is proper governance of the Financial Services Provider resulting in the promotion of sustainable growth of the business. This elevates confidence within stakeholders by meeting market and customer expectations and the community. This also aligns Financial Services providers to international standards and best practice building confidence in the financial services sector.

The Board and executive are ultimately liable for the success or failure of the compliance risk management function and overall risk management.

The responsibility to ensure that FSP's comply with all relevant laws, regulations and supervisory requirements rests with the Boards of Directors, Management Boards, Business Entity Heads, Senior Management, Management and Employees of the FSP. The relevant management and executive boards and committees must ensure that compliance risks are identified, that appropriate compliance risk management plans are in place at all levels of the organisation and that these plans are adhered to. The Compliance risk management is therefore an integral part thereof.

Kevin Wides (Key Individual) and Charmaine Mavhunga (Director of Operations) of the FSP is tasked with ensuring that appropriate, effective and efficient risk management processes, systems and monitoring structures are in place and integrated in the day to day activities for the business entity in accordance with this framework. This includes managing compliance risk. This responsibility is delegated by the Boards of Directors to the management and is a duty of every employee to ensure that risks within their confines are mitigated by the head of each business entity. The Board and executive management must demonstrate commitment to compliance, the compliance objectives, and the minimum standards to ensure a culture of compliance by all parties.

If the FSP has an internal audit function; this will assess the internal business management and control processes within this framework and progress with corrective actions and report thereon independently to the relevant audit committees. Internal audit will assess the effectiveness and adequacy of the compliance process and assist the compliance function generally with independent monitoring of compliance within the FSP.

The external audit function provides an independent assessment of the integrity and quality of the compliance reporting to the Boards of Directors and Executive Management of the entities of the FSP. Furthermore, this function has an obligation in terms of specific FAIS to submit reports in prescribed formats to the Authority.

9. Tools

Oracle has purchased an on-line audit tool which is used to conduct most of our on-site monitoring and a repository tool to store all client policies and procedures.

10. Authority and Mandate


The Corporate Governance Policy is approved by way of approved resolution / agenda item of the OIH Board's meeting minutes. Senior Management is responsible for the adherence to and implementation of this Governance Policy throughout the organization.



This Compliance Framework has been adopted as follows:

Signed Name: Dany Mawas

Signed Date: August 28th, 2023

Signature: 



RaiseFX
YOUR TRADING PARTNER

RAISE GLOBAL SA (PTY) LTD
2018/616118/07

An authorised Financial Services Provider with FSP No: 50506

RISK MANAGEMENT AND COMPLIANCE PROGRAMME

August 2023

Contents

PREAMBLE.....	4
A RISK-BASED APPROACH	5
DEFINITIONS.....	6
"beneficial owner"	6
"business relationship"	6
"cash"	6
"Centre"	6
"client"	6
"domestic prominent influential person"	6
"entity"	8
"foreign prominent public official"	8
"immediate family member"	8
"institution"	8
"legal person".....	8
"money laundering"	9
"offence relating to the financing of terrorist and related activities"	9
"POCDATARA Act"	9
"property"	9
"single transaction"	9
"terrorist and related activities"	9
"trust"	9
CONTROL MEASURES FOR MONEY LAUNDERING AND FINANCING OF TERRORIST AND RELATED ACTIVITIES	10
Customer due diligence	10
Anonymous clients and clients acting under false or fictitious names (section 20A)	10
Identification of clients and other persons (section 21)	10
Understanding and obtaining information on a business relationship (section 21A)	19
Additional due diligence relating to legal persons, trusts and partnerships (section 21B)	
Ongoing due diligence (section 21C)	20
Doubts about veracity of previously obtained information (section 21D)	22
Inability to conduct customer due diligence (section 21 E)	22
Foreign prominent public official (section 21F)	22
Domestic prominent influential person (section 21G)	23
Reliance on customer due diligence performed by another accountable institution	24

Duty to keep records.....	24
Obligation to keep customer due diligence records (section 22).....	24
Obligation to keep transaction records (section 22A).....	24
Period for which records must be kept (section 23).....	25
Records may be kept in electronic form and by third parties (section 24).....	25
Reporting duties and access to information.....	27
Reporting obligations to advise Centre of clients (section 27).....	27
Powers of access by authorised representative to records (section 27 A).....	27
Cash transactions above prescribed limit (section 28).....	27
Property associated with terrorist and related activities (section 28A).....	29
Suspicious and unusual transactions (section 29).....	30
Conveyance of cash to or from Republic (section 30).....	32
Electronic transfers of money to or from Republic (section 31).....	32
Reporting procedures and furnishing of additional information (section 32).....	32
Continuation of transactions (section 33).....	33
Intervention by Centre (section 34).....	33
Monitoring orders (section 35).....	33
Reporting duty, obligation to provide information not affected by confidentiality rules (section 37).....	34
Protection of persons making reports (section 38).....	34
Measures to promote compliance.....	35
Risk Management and Compliance Programme (section 42).....	35
Distinguishing between prospective clients and established clients (section 42).....	
Implementation of the RMCP in branches, subsidiaries and foreign countries (section 42) . Error! Bookmark not defined.	
Review of Risk Management and Compliance Programme (section 42).....	35
Availability of Risk Management and Compliance Programme to employees (section 42).....	35
Availability of Risk Management and Compliance Programme to Centre (section 42).....	35
Governance of compliance (section 42A).....	36
Training of employees (section 43).....	36
Registration with the Centre (section 43B).....	36
COMPLIANCE AND ENFORCEMENT.....	38
APPROVAL OF RISK MANAGEMENT COMPLIANCE PROGRAMME.....	40

PREAMBLE

The Financial Intelligence Centre Act, 2001 (“the FIC Act”), together with the Prevention of Organised Crime Act, 1998 (“POCA”) and the Protection of Constitutional Democracy against Terrorist and related activities Act (“POCDATARA”) form the statutory framework to combat money laundering and suppress the financing of terrorism in South Africa.

A money laundering offence may be described as the performing of any act in connection with property by a person who knows or ought reasonably to have known that the property is or forms part of the proceeds of unlawful activities and that may result in concealing or disguising the nature, source, location, disposition or movement of the proceeds of the crime, the ownership thereof or any interest anyone may have in respect thereof or enabling or assisting a person to avoid prosecution or to remove or diminish the proceeds of crime.

While money laundering has been criminalised in section 4 of POCA, the FIC Act is a key regulatory tool to protect the South African financial system against money laundering, the proceeds of crime and the financing of terrorism.

Raise Global SA (“the institution”) is an accountable institution as envisaged in the FIC Act. This Act requires the *board of directors* of the institution to ensure compliance by the institution and its employees with the provisions of the FIC Act and a Risk Management and Compliance Programme.

This document embodies the Risk Management Compliance Programme of the institution and has been updated to include the 2 October 2017 amendments made to the FIC Act by the Financial Intelligence Centre Amendment Act, No. 1 of 2017.

This programme enables the institution to identify, assess, monitor, mitigate and manage the risk of money laundering activities or the financing of terrorist and related activities that the provision of products or services may involve.

A RISK-BASED APPROACH

Raise Global SA (pty) LTD “RGSA” follows a risk-based approach to client identification and verification regarding the type of information by means of which it will establish clients’ identities and the means of verification of such information.

Application of a risk-based approach implies RGSA can accurately assess the risk involved. It also implies that the institution can take an informed decision based on its risk assessment as to the appropriate methods and levels of verification that should be applied.

RGSA applies simplified measures where lower risks have been identified and enhanced measures where higher risks are identified. To assess the risk factors, the institution makes use of a risk framework which forms part of the institution’s policies and procedures to address money laundering and terrorist financing.

RGSA applies the concept of a single client view in respect of each client when applying the provisions of the FIC Act. A single client view allows all the business units within the institution to access an existing client’s identification and verification information from a central point. A single client view is in line with the national and international move towards a risk-based approach.

The risk-based approach requires RGSA to understand its exposure to money laundering and terrorist financing risks. By understanding and managing its money laundering and terrorist financing risks, the institution not only protects and maintains the integrity of its business, but also contributes to the integrity of the South African financial system.

DEFINITIONS

"**beneficial owner**", in respect of a legal person, means a natural person who, independently or together with another person, directly or indirectly owns the legal person or exercises effective control of the legal person;

"**business relationship**" means an arrangement between a client and the institution for concluding transactions on a regular basis;

"**cash**" means coin and paper money of the Republic or of another country that is designated as legal tender and that circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue; travellers' cheques;

"**Centre**" means the Financial Intelligence Centre. The contact details for the Centre are as follows:

Address:	The Financial Intelligence Centre Private Bag X177 Centurion 0046
Tel Number:	+27 12 641 6000 (Press 1 for the Compliance Contact Centre).

"**client**", in relation to the institution, means a person who has entered into a business relationship or a single transaction with the institution;

"**domestic prominent influential person**" means an individual who holds, including in an acting position for a period exceeding six months, or has held at any time in the preceding 12 months, in the Republic-

- a prominent public function including that of
 - o the President or Deputy President;
 - o a government minister or deputy minister;
 - o the Premier of a province;
 - o a member of the Executive Council of a province;

- o an executive mayor of a municipality elected in terms of the Local Government: Municipal Structures Act, 1998;
- o a leader of a political party registered in terms of the Electoral Commission Act, 1996;
- o a member of a royal family or senior traditional leader as defined in the Traditional Leadership and Governance Framework Act, 2003;
- o the head, accounting officer or chief financial officer of a national or provincial department or government component, as defined in section 1 of the Public Service Act, 1994;
- o the municipal manager of a municipality appointed in terms of section 54A of the Local Government: Municipal Systems Act, 2000, or a chief financial officer designated in terms of section 80 (2) of the Municipal Finance Management Act, 2003;
- o the chairperson of the controlling body, the chief executive officer, or a natural person who is the accounting authority, the chief financial officer or the chief investment officer of a public entity listed in Schedule 2 or 3 to the Public Finance Management Act, 1999;
- o the chairperson of the controlling body, chief executive officer, chief financial officer or chief investment officer of a municipal entity as defined in section 1 of the Local Government: Municipal Systems Act, 2000;
- o a constitutional court judge or any other judge as defined in section 1 of the Judges' Remuneration and Conditions of Employment Act, 2001;
- o an ambassador or high commissioner or other senior representative of a foreign government based in the Republic; or
- o an officer of the South African National Defence Force above the rank of major-general;
- any of the following positions in of a company, as defined in the Companies Act, 2008, if the company provides goods or services to an organ of state and the annual transactional value of the goods or services or both exceeds an amount determined by the Minister by notice in the Gazette-
 - o chairperson of the board of directors;
 - o chairperson of the audit committee;
 - o executive officer; or
 - o chief financial officer ; or

- the position of head, or other executive directly accountable to that head, of an international organisation based in the Republic;

“entity” with reference to Sections 3, 4, 14, 22, 23 and 25 of POCDATARA, means a natural person, or a group of two or more natural person (whether acting in the furtherance of a common purpose or conspiracy or not) or syndicate, gang, agency, trust, partnership, fund or other unincorporated association or organisation or any incorporated association or organisation or other legal person, and includes, where appropriate , a cell, unit, section, sub-group or branch thereof or any combination thereof;

“foreign prominent public official” means an individual who holds, or has held at any time in the preceding 12 months, in any foreign country a prominent public function including that of a-

- Head of State or head of a country or government;
- member of a foreign royal family;
- government minister or equivalent senior politician or leader of a political party;
- senior judicial official;
- senior executive of a state-owned corporation; or
- high-ranking member of the military;

“immediate family member” means

- the spouse, civil partner or life partner;
- previous spouse, civil partner or life partner, if applicable;
- children and step children and their spouse, civil partner or life partner;
- parents; and
- sibling and step sibling and their spouse, civil partner or life partner;

“institution” means Semi-State Bodies and State Owned Enterprises

"legal person" means any person, other than a natural person, that establishes a business relationship or enters into a single transaction, with an accountable institution and includes a person incorporated as a company, close corporation, foreign company or any other form of corporate arrangement or association, but excludes a trust, partnership or sole proprietor;

"money laundering" or "money laundering activity" means an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds, and includes any activity which constitutes an offence in terms of section 64 of the FIC Act or section 4, 5 or 6 of POCA;

"offence relating to the financing of terrorist and related activities" means an offence under section 4 of the POCDATARA;

"POCDATARA Act" means the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004;

"property" has the meaning assigned to it in section 1 of POCDATARA;

"single transaction" means a transaction other than a transaction concluded in the course of a business relationship and where the value of the transaction is not less than R5000, except in the case of section 20A (where no threshold applies);

"terrorist and related activities" has the meaning assigned to it in section 1 of POCDATARA;

"trust" means a trust defined in section 1 of the Trust Property Control Act, 1988, other than a trust established by virtue of a testamentary disposition; by virtue of a court order; in respect of persons under curatorship or by the trustees of a retirement fund in respect of benefits payable to the beneficiaries of that retirement fund, and includes a similar arrangement established outside the Republic.

CONTROL MEASURES FOR MONEY LAUNDERING AND FINANCING OF TERRORIST AND RELATED ACTIVITIES

Customer due diligence

Anonymous clients and clients acting under false or fictitious names (section 20A)

RGSA may not establish a business relationship or conclude a single transaction with an anonymous client or a client with an apparent false or fictitious name and therefore the following process is followed

When RGSA establishes a business relationship:

The institution will obtain the full name and identity number or passport number of the potential client along with physical address and contact numbers

When RGSA concludes a single transaction:

The threshold for single transactions does not apply to the obligations set out in section 20A. This means that, despite a single transaction being below the threshold (currently R5000), Raise Global SA is still prohibited from concluding a single transaction with an anonymous client or a client with an apparent false or fictitious name.

Identification of clients and other persons (section 21)

When engaging with a prospective client to enter into a single transaction or to establish a business relationship, RGSA must, in the course of concluding that single transaction or establishing that business relationship, establish and verify the identity of the client in the following manner:

South African citizens:

The full name, date of birth and identity numbers of South African citizens may be verified by an identity document. If an identity document is not available, a South African passport or South African driver's licence may be used for verification purposes.

The residential address of a South African citizen may be verified by current documentation (good practice that it is less than three months old) reflecting the name and residential address of the person. Examples are utility bills, bank statements, recent lease or rental agreements, municipal rates and taxes invoices, mortgage statements, telephone or cellular accounts, television licence documentation, motor vehicle licence documentation, recent long-term or short-term insurance

documentation, recent SARS tax returns, recent correspondence from a body corporate or share-block association or a payslip or salary advice.

Documents that may be accepted to confirm the authority of a person to act on behalf of another person and confirm the particulars of the person authorizing the 3rd party to establish the relationship may include a power of attorney, mandate, resolution duly executed by authorised signatures or a court order authorising the 3rd party to conduct business on behalf of another person.

Foreign nationals:

The full name, date of birth, nationality and passport number of foreign nationals may be verified by a passport.

In instances in which an accountable institution deems it reasonably necessary to obtain, in addition to a person's identity document (foreign passport), further information or documentation verifying the identity of such a person, Raise Global SA may obtain a letter of confirmation from a person in authority (for example, from the relevant embassy) which confirms authenticity of that person's identity document (passport).

Decisions concerning when further confirmation of the identity of a foreign national may be required and the nature of such information should be based on an RGSA's risk framework.

The fact that privacy and protection of data legislation exists in the country where the client resides or conducts business, does not excuse the client from providing Raise Global SA with the necessary client identification and verification information when establishing a business relationship or transacting with an accountable institution in South Africa.

Raise Global SA may therefore not establish a business relationship or conclude a single transaction with a foreign national if the foreign national refuses to provide the required information and documentation that is necessary for identification and verification purposes.

Additional due diligence relating to legal persons, trusts and partnerships (section 21B)

This section applies in respect of a legal person, partnership or trust or a similar arrangement between natural persons, whether it is incorporated or originated in the Republic or elsewhere.

A pension and a provident fund will fall into the category of "legal person".

South African companies:

The registered name, registered number and registered address may be verified by obtaining a registration certificate and notice of incorporation as issued in terms of the Companies Act from the representative of the company, or alternatively electronic verification processes as provided for by the CIPC.

The trade name, business address (and if operating from multiple addresses – the address of office seeking to establish the relationship and the head office) may be verified by obtaining a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return, original company letterhead or official company documentation issued by CIPC.

The full names, date of birth and identity number (SA citizen or resident) or nationality (if foreigner) of the manager, each natural person who purports to be authorised to establish a business relationship and each natural person holding voting rights may be verified, in the case of a South African citizen and resident, by an identity document or if an identity document is not available, South African passport or South African driver's licence. In the case of a foreign national it may be verified by a passport.

The registered name, registration number and registered address of each company may be verified by obtaining the registration certificate and notice of incorporation as issued in terms of the Companies Act from the representative of the company, or alternatively electronic verification processes as provided for by the CIPC.

The trade name and business address of each company that holds voting rights, may be verified by a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return, original letterhead or official CIPC company documentation.

The registered name, registration number and registered address of each close corporation that holds voting rights may be verified by the most recent version of founding statement and certificate of incorporation, bearing the stamp of the Registrar of Close Corporations and signed by an authorised member or employee of the close corporation, or alternatively electronic verification processes as provided for by the CIPC.

The trade name and business address of each close corporation that holds voting rights may be verified by a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return, original letterhead or official CIPC close corporation documentation.

The name, number of incorporation and address where situated for incorporation of each foreign company that holds voting rights may be verified by an official document by an authority for recording the incorporation of companies of the country of incorporation of the foreign company.

The name of the legal person, address from where it operates and legal form of each other legal person that holds voting rights may be verified by the Constitution or other founding document in terms of which the legal person is created, a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return, original company letterhead or official CIPC company documentation.

The name of the partnership holding voting rights may be verified by the partnership agreement.

The identifying name and number of the trust that holds voting rights may be verified by the trust deed and if trust is created in South Africa, authorisation by the Master of the High Court to each trustee to act in that capacity or if trust is created outside South Africa, an official document which reflects these particulars, by the authority in the country where the trust is created.

The residential address/business address and contact particulars of the manager, each natural person who purports to be authorised to establish a business relationship and each natural person or legal person, partnership or trust holding voting rights may be verified if required by the accountable institution.

Authorisation of a person acting on behalf of the company to establish the relationship, may be verified by written instruction from the authorising party, a power of attorney, mandate, resolution or court order.

(South African) close corporations:

The registered name, registration number and registered address may be verified by the most recent version of the founding statement and certificate of incorporation, bearing the stamp of the Registrar of Close Corporations and signed by an authorised member or employee of the close corporation, or alternatively electronic verification processes as provided for by the CIPC.

The trade name and business address and if it operates from multiple addresses, the address of office seeking to establish the relationship and the address of the head office, may be verified by a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return, original letterhead or official CIPC close corporation documentation.

The full names, date of birth, Identity number (SA citizen or resident) or nationality (if foreigner) of each member and each natural person who purports to be authorised to establish a business relationship may be verified, in the case of a South African citizen and resident, an identity document and if an identity document is not available, a South African passport or South African driver's licence. If it is a foreign national, it may be verified by a passport.

The residential address and contact particulars of each member and each natural person who purports to be authorised to establish the relationship may be verified as required RGSA

Authorisation of a person acting on behalf of the close corporation, to establish the relationship may be verified by written instruction from the authorising party, a power of attorney, mandate, resolution or court order.

Foreign companies:

The name, number of incorporation and address where situated for incorporation may be verified by an official document by an authority for recording the incorporation of companies of the country of incorporation of the foreign company.

The business name in the country of incorporation and the address from where it operates in the country of incorporation, or if from multiple addresses, the address of its head office may be verified by a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice or original company letterhead.

The trade name in South Africa, the business address in South Africa and if it operates from multiple addresses, the address of office seeking to establish the relationship, may be verified by a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return, original letterhead or official CIPC company documentation.

The full names, date of birth, identity number (SA citizen or resident) or nationality (if foreigner) of manager of affairs in South Africa, each natural person who purports to be authorised to establish the relationship and each natural person holding voting rights, may be verified, in the case of a South African citizen and resident, the identity document or if the identity document is not available, a South African passport or South African driver's licence. In the case of a foreign national, it may be verified by a passport.

The registered name, registration number and registered address of each South African company that holds voting rights may be verified by obtaining a registration certificate and notice of incorporation

as issued in terms of the Companies Act from the representative of the company, or alternatively electronic verification processes as provided for by the CIPC.

The trade name and business address of each South African company that holds voting rights may be verified by a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return, original letterhead or official CIPC company documentation.

The registered name, registration number and registered address of each close corporation that holds voting rights may be verified by the most recent version of the founding statement and certificate of incorporation, bearing the stamp of the Registrar of Close Corporations and signed by an authorised member or employee of the close corporation, or alternatively electronic verification processes as provided for by the CIPC.

The trade name and business address of each close corporation that holds voting rights may be verified by a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return, original letterhead or official CIPC close corporation documentation.

The name, number of incorporation and address where situated for incorporation of each foreign company that holds voting rights may be verified by an official document by an authority for recording the incorporation of companies of the country of incorporation of the foreign company.

The name of the legal person, address from where it operates and legal form of each other legal person that holds voting rights may be verified by a Constitution or other founding document in terms of which the legal person is created, a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return or original company letterhead.

The name of a partnership holding voting rights may be verified by the partnership agreement.

The identifying name and number of a trust that holds voting rights may be verified by the trust deed or other founding document in terms of which the trust is created.

The residential/business address and contact particulars of the manager of affairs in South Africa, each natural person who purports to be authorised to establish a business relationship and each natural

person or legal person, partnership or trust holding voting rights, may be verified if required by the accountable institution.

Authorisation of persons acting on behalf of the foreign company to establish the relationship, may be verified by written instruction from the authorising party, a power of attorney, mandate, resolution or court order.

Other legal persons:

The name of the legal person, address from where it operates and legal form may be verified by a Constitution or other founding document in terms of which the legal person is created, a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return or original company letterhead.

The full names, date of birth, identity number (South Africa citizen or resident) or nationality (if foreigner) of each natural person who purports to be authorised to establish the relationship may be verified, in the case of a South African citizen and resident, by an identity document or if an identity document is not available, a South African passport or South African driver's licence. In the case of a foreign national, verification may be done by a passport.

The residential address and contact particulars of each natural person who purports to be authorised to establish the relationship may be verified if required by the accountable institution.

Authorisation of persons acting on behalf of the other legal person to establish the relationship, may be verified by written instruction from the authorising party, a power of attorney, mandate, resolution or court order.

Partnerships:

The partnership agreement may be used to establish the identifying name of the partnership.

If partner is natural person and SA citizen or resident, the full names, date of birth and identity number may be verified by means of an identity document (if identity document is not available, South African passport or South African driver's licence).

If partner is natural person and foreigner, the full names, date of birth and nationality may be verified by a passport.

If partner is a South African company or close corporation, the registered name, registration number and registered address may be verified by obtaining the registration certificate and notice of incorporation as issued in terms of the Companies Act from the representative of the company, or

alternatively electronic verification processes as provided for by the CIPC. The trade name and business address may be verified by a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return, original company letterhead or Official CIPC company documentation.

If the partner is a foreign company, the name, number of incorporation and address where situated for Incorporation may be verified by an official document by an authority for recording the incorporation of companies of the country of incorporation of the foreign company.

If the partner is another legal person, the name, address and legal form may be verified by the Constitution or other founding document in terms of which the legal person is created, a Utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return or original company letterhead.

If the partner is a trust, the identifying name and number may be verified by the trust deed and if trust is created in South Africa, authorisation by the Master of the High Court to each trustee to act in that capacity. If trust is created outside South Africa, an official document which reflects these particulars, by the authority in the country where the trust is created, may be used to verify the identifying name and number of the trust.

The full names, date of birth and identity number (SA citizen or resident) or nationality (if foreigner) of the person who exercises executive control over the partnership and each natural person who purports to be authorised to establish the relationship may be verified, in the case of a South African citizen and resident, by an identity document or if an identity document is not available, a South African passport or South African driver's licence. In the case of a foreign national, verification may be done by a passport.

Authorisation of persons acting on behalf of the partnership, to establish the relationship may be verified by written instruction from the authorising party, a power of attorney, mandate, resolution or court order.

Trusts:

The identifying name and number of the trust may be verified by the trust deed and if the trust is created in South Africa, authorisation by the Master of the High Court to each trustee to act in that capacity. If the trust is created outside South Africa, an official document which reflects these particulars, by the authority in the country where the trust is created may be used as verification.

The Address of Master of the High Court where the trust is registered (if applicable), may be verified by authorisation given by Master of the High Court to each trustee to act in that capacity

Natural person: The full names, date of birth, identity number (if SA citizen or resident) or nationality (if foreigner) of each trustee, each natural person who purports to be authorised to establish a relationship, the beneficiaries referred to by name in the trust deed or other founding instrument and the founder of the trust may be verified, in the case of a South African citizen and resident, by an identity document and if an identity document is not available, a South African passport or South African driver's licence. In the case of a foreign national, verification may be done by a passport. In addition, authorisation by the Master of the High Court to each trustee to act in that capacity, an official document which reflects these particulars, by the authority in the country where the trust is created and other documentation required where founder has died may be used for verification purposes.

SA Company or Close Corporation: The registered name, registration number, registered address and trade name may be verified by obtaining the registration certificate and notice of incorporation as issued in terms of the Companies Act from the representative of the company, or alternatively electronic verification processes as provided for by the CIPC

The business address of each trustee, beneficiaries referred to by name in the trust deed or other founding instrument and the founder may be verified by the most recent version of founding statement and certificate of incorporation, bearing the stamp of the Registrar of Close Corporations and signed by an authorised member or employee of the close corporation, or alternatively electronic verification processes as provided for by the CIPC.

The trade name and business address may be verified by a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return, original letterhead or official CIPC close corporation documentation. In addition, authorisation by the Master of the High Court to each trustee to act in that capacity, an official document which reflects these particulars, by the authority in the country where the trust is created, other documentation required where founder has died or no longer exists may be used for verification purposes.

Foreign Company: The name, number of incorporation and address where situated for incorporation of each trustee, beneficiaries referred to by name in the trust deed or other founding instrument and the founder may be verified by an official document by an authority for recording the incorporation of companies of the country of incorporation of the foreign company. In addition, authorisation by

the Master of the High Court to each trustee to act in that capacity, an official document which reflects these particulars, by the authority in the country where the trust is created and may be used for verification purposes.

Other legal person: The name of the legal person, address from where it operates and legal form of each trustee, beneficiaries referred to by name in the trust deed or other founding instrument and founder may be verified by a Constitution or other founding document in terms of which the legal person is created, a utility bill, bank statement, recent lease or rental agreement, municipal rates and taxes invoice, mortgage statement, Telkom account, recent SARS tax return or original company letterhead. In addition, authorisation by the Master of the High Court to each trustee to act in that capacity, an official document which reflects these particulars, by the authority in the country where the trust is created and other documentation required where founder has died or no longer exists may be used for verification purposes.

Partnership: The name of the partnership, each trustee, beneficiaries referred to by name in the trust deed or other founding instrument and founder may be verified by a partnership agreement. In addition, authorisation by the Master of the High Court to each trustee to act in that capacity, an official document which reflects these particulars, by the authority in the country where the trust is created and other documentation required where founder has died or no longer exists may be used for verification purposes.

Trust: The identifying name and number of trust of each trustee, beneficiaries referred to in the trust deed or other founding instrument and founder may be verified by the trust deed. In addition, where the founder has died or no longer exists, other documentation may be used for verification purposes. The residential address and contact particulars of each trustee, each natural person who purports to be authorised to establish a business relationship, each beneficiary of the trust referred to by name in the trust deed or other founding instrument and the founder may also be verified if required by the institution.

Authorisation of persons acting on behalf of the trust, to establish the relationship may be verified by written instruction from the authorising party, a power of attorney, mandate, resolution or court order.

Understanding and obtaining information on a business relationship (section 21A)

When the institution engages with a prospective client to establish a business relationship as contemplated in section 21, the institution must, in addition to the steps required under section 21, obtain information to reasonably enable it to determine whether future transactions that will be

performed in the course of the business relationship concerned are consistent with its knowledge of that prospective client. This will be done in the following manner:

Raise Global SA will review KYC requirements on an annual basis and request new documentation were applicable

- the nature of the business relationship concerned:

Will require appropriate documentation if there is a change in the business relationship or parties involved.

- the intended purpose of the business relationship concerned:

Raise Global SA will require evidence as to the purpose of the change in business and supporting documentation.

- and the source of the funds which that prospective client expects to use in concluding transactions in the course of the business relationship concerned:

Raise Global SA will require proof of source of funds if they differ from the existing transactions.

Ongoing due diligence (section 21C)

Raise Global SA must conduct ongoing due diligence in respect of a business relationship which includes

- monitoring of transactions undertaken throughout the course of the relationship, including, where necessary-

- o the source of funds, to ensure that the transactions are consistent with the institution's knowledge of the client and the client's business and risk profile.

The institution will monitor the transactions in the following manner:

- o the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent business or lawful purpose.

The Raise Global SA will examine complex or unusually large transactions and unusual patterns of transactions which have no apparent business or lawful purpose in the following manner:

All transaction of a unusual manner will be dealt with by the board of directors of Raise Global SA.

.....

- o Raise Global SA will keep written findings thereof in the following manner:

Raise Global SA has an obligation in terms of Section 22 of FICA to hold copies of all the records that it is required to obtain during the CDD process.

These records must –

- Include copies of, or reference to, information provided to or obtained by Sanne to verify a person's identity; and
- In the case of a business relationship, reflect the information obtained by Sanne concerning
- The nature of the business relationship;
- The intended purpose of the business relationship;
- The source of funds and source of wealth which the prospective client is expected to use in concluding transactions in the course of the business relationship
- Raise Global SA is additionally obligated in terms of Section 22A of FICA to keep a record of every transaction, whether a single transaction or a transaction concluded in the course of a business relationship.
- The records must reflect the following information –
- The amount involved and the currency in which it was denominated;
- The date on which the transaction was concluded;
- The parties to the transaction;
- The nature of the transaction;
- Business correspondence; and
- If Raise Global SA provides account facilities to its clients, the identifying particulars of all accounts and the account files at Raise Global SA that are related to the transaction.

These records may be kept in electronic form. All records which relate to the establishment of a business relationship have to be kept for at least five years from the date on which the business relationship is terminated. Those records which relate to a transaction which is concluded must be kept for at least five years from the date on which the transaction is concluded. Records which relate to a transaction or activity that gave rise to a report contemplated in section 29, must be kept for at least five years from the date on which the report was submitted to the Centre.

- The duties imposed by Sections 22 and 22A on Sanne to keep records may be performed by a third party on behalf of Sanne as long as there is free and easy access

to the records. Raise Global SA is responsible for supplying the FIC with the prescribed particulars of the relevant third party.

- keeping information obtained for the purpose of establishing and verifying the identities of clients pursuant to sections 21, 21A and 21B of the FIC Act, up to date.

Doubts about veracity of previously obtained information (section 21D)

When RGSA, subsequent to entering into a single transaction or establishing a business relationship, doubts the veracity or adequacy of previously obtained information which it is required to verify as contemplated in sections 21 and 21B, it must repeat the steps contemplated in sections 21 and 21B to the extent that is necessary to confirm the information in question.

Inability to conduct customer due diligence (section 21 E)

If Raise Global SA is unable to establish and verify the identity of a client or other relevant person in accordance with section 21 or 21B, obtain the information contemplated in section 21A or conduct ongoing due diligence as contemplated in section 21C, it

- may not establish a business relationship or conclude a single transaction with a client;
- may not conclude a transaction in the course of a business relationship, or perform any act to give effect to a single transaction; or
- must terminate an existing business relationship with a client

as the case may be, and consider making a report under section 29 of the FIC Act.

Foreign prominent public official (section 21F)

If the institution determines that a prospective client with whom it engages to establish a business relationship, or the beneficial owner of that prospective client, is a foreign prominent public official, it must

- obtain director approval for establishing the business relationship, following the same measures taken for a foreign person. The directors will evaluate as per their risk framework (See annex for risk rating framework).

- take reasonable measures to establish the source of wealth and source of funds of the client,

and

- conduct enhanced ongoing monitoring of the business relationship, in the following manner:
Constant monitoring of all transactions.

Sections 21F applies to immediate family members (refer definition in definition clause above) and known close associates of a person in a foreign prominent position.

Domestic prominent influential person (section 21G)

If the institution determines that a prospective client with whom it engages to establish a business relationship, or the beneficial owner of that prospective client, is a domestic prominent influential person and that the prospective business relationship entails higher risk, it must-

- obtain director approval for establishing the business relationship,
- take reasonable measures to establish the source of wealth and source of funds of the client,
- conduct enhanced ongoing monitoring of the business relationship,

Section 21G applies to immediate family members (refer definition in definition clause above) and known close associates of a person in a domestic prominent position.

The institution must utilise the risk-based approach when assessing the risks posed by domestic prominent influential persons, their family members and their known close associates. This should be done on a case-by-case basis. Being a domestic prominent person does not create a presumption of being guilty of any crime and does not mean that an accountable institution cannot transact with such a person.

In order for the institution to identify a public sector domestic prominent influential person and to establish the source of wealth and funds, it may require screening technological solutions which are often acquired from commercial PEP database providers.

The definition of foreign prominent public official is similar and a similar process is followed, except that the measures are taken for every foreign prominent person and not based on higher risk.

Reliance on customer due diligence performed by another accountable institution

Exemption 4 (b) under the FIC Act previously exempted accountable institutions from compliance with the identification of clients by allowing for reliance on written confirmation from a primary accountable institution as to the identity of the client. The exemption was intended to avoid a duplication of customer due diligence obligations where one accountable institution referred a client to another. Exemption 4 (b) has been withdrawn, but the concept is now included implicitly in the provisions of the FIC Act.

The institution relies on the customer due diligence performed by another accountable institution which has referred a client, subject to the following processes and procedures being followed:
Raise Global SA requires a full KYC pack for the referring client and the accountable institution.

Duty to keep records

Obligation to keep customer due diligence records (section 22)

When the institution is required to obtain information pertaining to a client or prospective client pursuant to sections 21 to 21H, it must keep a record of that information.

The records must include copies of, or references to, information provided to or obtained by it to verify a person's identity and in the case of a business relationship, reflect the information obtained by it under section 21A concerning the nature of the business relationship, the intended purpose of the business relationship and the source of the funds which the prospective client is expected to use in concluding transactions in the course of the business relationship.

Obligation to keep transaction records (section 22A)

The institution must keep a record of every transaction, whether the transaction is a single transaction or concluded in the course of a business relationship which it has with the client, that are reasonably necessary to enable that transaction to be readily reconstructed.

The records must reflect the following information:

- the amount involved and the currency in which it was denominated;
- the date on which the transaction was concluded;
- the parties to the transaction;
- the nature of the transaction;
- business correspondence; and
- if it provides account facilities to its clients, the identifying particulars of all accounts and the account files at the institution that are related to the transaction.

Period for which records must be kept (section 23)

The institution must keep the records which relate to the establishment of a business relationship referred to in section 22 for at least 5 years from the date on which the business relationship is terminated.

The institution must keep the records which relate to a transaction referred to in section 22A which is concluded for at least 5 years from the date on which that transaction is concluded.

The institution must keep the records which relate to a transaction or activity which gave rise to a report contemplated in section 29, for at least 5 years from the date on which the report was submitted to the Centre.

Records may be kept in electronic form and by third parties (section 24)

The recordkeeping duties may be performed by a third party on behalf of the institution, provided it has free and easy access to the records and the records are readily available to the Centre and the relevant supervisory body for the purposes of performing its functions in terms of the FIC Act.

If a third party referred to above fails to properly comply with the requirements of sections 22 and 22A on behalf of the institution, the institution is liable for that failure.

If the institution appoints a third party to perform the duties imposed on it by sections 22 and 22A, it must forthwith provide the Centre and the supervisory body concerned with the prescribed particulars of the third party.

Records kept in terms of sections 22 and 22A may be kept in electronic form and must be capable of being reproduced in a legible format.

Reporting duties and access to information

Reporting obligations to advise Centre of clients (section 27)

If the Centre requests an accountable institution, a reporting institution or a person that is required to make a report in terms of section 29 of the FIC Act to advise

- whether a specified person is or has been a client
- whether a specified person is acting or has acted on behalf of any client
- whether a client is acting or has acted for a specified person
- whether a number specified by the Centre was allocated to a person with whom the accountable institution, reporting institution or person has or has had a business relationship or
- on the type and status of a business relationship with a client

the accountable institution, reporting institution or person must inform the Centre accordingly.

Powers of access by authorised representative to records (section 27 A)

An authorised representative of the Centre has access during ordinary working hours to any records kept by or on behalf of the institution in terms of section 22, 22A or 24, and may examine, make extracts from or copies of, any such records for the purposes of obtaining further information in respect of a report made or ought to be made in terms of section 28, 28A, 29, 30 (1) or 31.

The authorised representative of the Centre may, except in the case of records which the public is entitled to have access to, exercise these powers only by virtue of a warrant.

The institution must without delay give to an authorised representative of the Centre all reasonable assistance necessary to enable that representative to exercise the abovementioned powers.

Cash transactions above prescribed limit (section 28)

An accountable institution and a reporting institution must, within the prescribed period, report to the Centre the prescribed particulars concerning a transaction concluded with a client if in terms of the transaction an amount of cash in excess of the prescribed amount

- is paid by the accountable institution or reporting institution to the client, or to a person acting on behalf of the client, or to a person on whose behalf the client is acting; or
- is received by the accountable institution or reporting institution from the client, or from a person acting on behalf of the client, or from a person on whose behalf the client is acting.

The prescribed amount of cash above which a transaction must be reported to the Centre under section 28 of the Act is R24 999,99 or an aggregate of smaller amounts which combine to come to this amount, if it appears to the institution that the transactions involving those smaller amounts are linked to be considered fractions of one transaction. The obligation to report in terms of Section 28 therefore arises when a transaction is concluded with a client by means of which cash of R25 000 or more is received by or paid by the institution. This includes receiving or paying cash in person as well as receiving or paying it via a third party (e.g. cash deposits made via a bank).

Section 28 reports must be sent to the Centre as soon as possible but not later than 2 working days after becoming aware of a fact of a cash transaction or series of cash transactions that have exceeded R24999.

In respect of the transaction or aggregated transactions for which a report under section 28 is made, the report must contain as much of the following information as is readily available:

- the date and time of the transaction, or in the case of a series of transactions, the time of the transactions in the 24-hour period;
- the description of the transaction or series of transactions;
- the amount of the funds per transaction or series of transactions;
- the currency in which the funds were disposed of; and
- the purpose of the transaction or series of transactions.

Section 64 of the FIC Act provides that “any person who conducts, or causes to be conducted, two or more transactions with the purpose in whole or in part of avoiding giving rise to a report duty under this Act is guilty of an offence”.

If a person files a report with the Centre in terms of section 28, the institution may elect to continue with the transaction as provided for in section 33 of the FIC Act. The Centre may under certain circumstances, direct the institution not to proceed with the carrying out of that transaction or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period not longer than 10 working days as determined by the Centre.

Property associated with terrorist and related activities (section 28A)

A report under section 28A must be sent to the Centre at <http://www.fic.gov.za> as soon as possible, but not later than 5 working days after an accountable institution had established that it has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of

- any entity which has committed, or attempted to commit, or facilitated the commission of a specified offence as defined in the POCDATARA Act.
- a specific entity identified in a notice issued by the President, under section 25 of the POCDATARA Act.

A report filed in terms of section 28A is based on the knowledge of an accountable institution that it has property related to the financing of terrorism in its possession or under its control. The knowledge about the origin and ownership of the property in question should be based on fact and should be acquired with reference to an objective set of circumstances or fact. Section 28A therefore applies to a purely factual situation. The fact that an accountable institution has certain property in its possession or under its control is sufficient to prompt a report and no activity relating to that property is required to trigger the reporting obligation.

The failure to file a report in terms of section 28A with the prescribed information and within the prescribed period constitutes an offence in terms of section 51A of the FIC Act.

The Director may direct the institution which has made such a report to report at intervals determined in the direction, that it is still in possession or control of the property in respect of which the report had been made and any change in the circumstances concerning its possession or control of that property. An accountable institution that fails to comply with a direction by the Director in accordance with section, is guilty of an offence.

When filing a report with the Centre in terms of section 28A, it is an offence to continue dealing with that property in any way (section 4 of POCDATARA).

The Centre may under certain circumstances, direct the institution not to proceed with the carrying out of that transaction or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period not longer than 10 working days as determined by the Centre.

Suspicious and unusual transactions (section 29)

A suspicious transaction report (STR) must be made to the Centre at <http://www.fic.gov.za> by

- a person who carries on a business
- a person who is in charge of a business
- a person who manages a business or
- a person who is employed by a business

and who knows or ought reasonably to have known or suspected that or who knows or suspects that a transaction or a series of transactions about which enquiries are made, may, if that transaction or those transactions had been concluded, have caused any of the following consequences:

- the business has received or is about to receive the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;
- a transaction or series of transactions to which the business is a party-
 - facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;
 - has no apparent business or lawful purpose;
 - is conducted for the purpose of avoiding giving rise to a reporting duty under this Act;
 - may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Service;
 - relates to an offence relating to the financing of terrorist and related activities; or

- the business has been used or is about to be used in any way for money laundering purposes or to facilitate the commission of an offence relating to the financing of terrorist and related activities.

A report under section 29 of must be filed with the Centre within 15 working days after the knowledge was acquired or the suspicion arose.

The report must set out the grounds for the knowledge or suspicion and the prescribed particulars concerning the suspicious or unusual transaction or series of transactions.

The state of mind that is necessary to create a reporting obligation in terms of section 29 is subjective and merely one of suspicion.

The institution must perform the customer due diligence requirements in accordance with sections 21, 21A, 21B and 21C when, during the course of a business relationship, it suspects that a transaction or activity is suspicious or unusual as contemplated in section 29.

Examples of conduct and transactions that may give rise to a suspicion:

- A client who provides vague or contradictory information or references
- A client who is reluctant to disclose other bank or business relationships
- A client who uses a financial institution which is located far from his home or work
- A corporate client who makes deposits or withdrawals mainly in cash
- A client who has no record of past or present employment or involvement in a business but who engages frequently in large transactions

No person who made or must make a report in terms of this section may, subject to subsection 45B (2A), disclose that fact or any information regarding the contents of any such report to any other person, including the person in respect of whom the report is or must be made, otherwise than

- within the scope of the powers and duties of that person in terms of any legislation
- for the purpose of carrying out the provisions of the FIC Act
- for the purpose of legal proceedings, including any proceedings before a judge in chambers or
- in terms of an order of court.

In terms of section 45B (2A) an inspector of the Centre or prescribed supervisory body may order from an accountable institution or reporting institution under inspection, the production of a copy

of a report, or the furnishing of a fact or information related to the report, contemplated in section 29.

If a person files a report with the Centre in terms of section 29, they may elect to continue with the transaction as provided for in section 33 of the FIC Act. The Centre may under certain circumstances, direct the institution not to proceed with the carrying out of that transaction or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period not longer than 10 working days as determined by the Centre.

Conveyance of cash to or from Republic (section 30)

A person who intends conveying or who has conveyed or who is conveying an amount of cash or a bearer negotiable instrument in excess of the prescribed amount to or from the Republic must, on demand, report the prescribed particulars concerning that conveyance to a person authorised by the Minister for this purpose.

Electronic transfers of money to or from Republic (section 31)

If the institution through electronic transfer sends money in excess of a prescribed amount out of the Republic or receives money in excess of a prescribed amount from outside the Republic on behalf, or on the instruction, of another person, it must, within the prescribed period after the money was transferred, report the transfer, together with the prescribed particulars concerning the transfer, to the Centre.

The date of commencement of section 31 must still be proclaimed.

Reporting procedures and furnishing of additional information (section 32)

A report in terms of section 28, 28A, 29 or 31 to the Centre and a report in terms of section 30 (1) to a person authorised by the Minister must be made in the prescribed manner.

The institution has appointed a Money Laundering Reporting Officer (MLRO), a person other than the section 42A Compliance Officer), with the responsibility and authority to submit the reports to the Centre on behalf of the institution. The appointment of a MLRO is voluntary and is mostly applicable in the case of large organisations where the institution is required to submit a large amount of reports to the Centre.

All reports must be submitted on goAML after successful registration and updating of information.

The institution may be requested to furnish the Centre or the investigating authority additional information concerning the report and the grounds for the report.

Continuation of transactions (section 33)

If the institution is required to make a report to the Centre in terms of section 28 or 29, it may continue with and carry out the transaction in respect of which the report is required to be made unless the Centre directs the institution in terms of section 34 not to proceed with the transaction.

Intervention by Centre (section 34)

The Centre may under certain circumstances, direct the institution not to proceed with the carrying out of that transaction or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period not longer than 10 working days as determined by the Centre.

Monitoring orders (section 35)

A judge may, under certain circumstances, order the institution to report to the Centre all transactions concluded by a specified person with the institution or all transactions conducted in respect of a specified account or facility at the institution.

Reporting duty, obligation to provide information not affected by confidentiality rules (section 37)

No duty of secrecy or confidentiality or any other restriction on the disclosure of information, whether imposed by legislation or arising from the common law or agreements, affects compliance by the institution with the provisions relating to reporting duties, access to information, measures to promote compliance and compliance and enforcement.

This does not apply to the common law right to legal professional privilege as between an attorney and the attorney's client in respect of certain communications made in confidentiality.

Protection of persons making reports (section 38)

No action, whether criminal or civil, lies against an accountable institution, reporting institution, supervisory body, the South African Revenue Service or any other person complying in good faith with the FIC Act provisions relating to reporting duties, access to information, measures to promote compliance and compliance and enforcement, including any director, employee or other person acting on behalf of such institution.

Measures to promote compliance

Risk Management and Compliance Programme (section 42)

The institution has developed, documented and implemented a programme for anti-money laundering and counter-terrorist financing risk management and compliance.

The requirements as set out in section 42 of the FIC Act are dealt with under the relevant sections in this document and provides for the processes to implement this Risk Management Compliance Programme.

Review of Risk Management and Compliance Programme (section 42)

This Risk Management and Compliance Programme is maintained by the RGSA.

Raise Global SA will review this Risk Management and Compliance Programme at the annually to ensure that it remains relevant to the RGSA's operations and the achievement of the legislative requirements:

Availability of Risk Management and Compliance Programme to employees (section 42)

This Risk Management and Compliance Programme is made available in the following manner to each employee of Raise Global SA involved in transactions to which the FIC Act applies:

Available as an electronic copy on internal servers which are backed up off site.

Availability of Risk Management and Compliance Programme to Centre (section 42)

Raise Global SA will, on request, make a copy of the documentation describing this Risk Management and Compliance Programme available to the Centre or a supervisory body which performs regulatory or supervisory functions in respect of the institution.

Governance of compliance (section 42A)

The board of directors are responsible for compliance by Raise Global SA and its employees with the FIC Act and this Risk Management Compliance Programme.

The institution has the following compliance officer to assist the board of directors Leonardo D'Onofrio from Oracle Compliance in discharging their obligations in terms of the FIC Act:

The compliance officer has been formally appointed by the board of directors of RGSA.

There is an SLA in place with a outlining all FIC Act compliance functions that he/she is required to perform.

The person appointed as a compliance officer is a person who has the authority to make, or participate in making decisions that affect the business from a FIC Act compliance perspective.

Raise Global SA remains responsible for any compliance failures.

Raise Global SA has assigned the following person/s with sufficient competence and seniority to ensure the effectiveness of the compliance function contemplated above:

Dany Mawas

Training of employees (section 43)

Raise Global SA provides the following ongoing training to its employees to enable them to comply with the provisions of the FIC Act and this Risk Management Compliance Programme:

Registration with the Centre (section 43B)

Any person or category of persons who, on commencing a new business, fall within the list of accountable institutions (or reporting institutions) in Schedule 1 (or Schedule 3 for reporting

institutions) must, within 90 days of the day the business is opened (authorised as financial services provider), register with the Centre.

Registration is done via the www.fic.gov.za website.

Raise Global SA is aware of its obligation to notify the Centre, in writing, of any changes to the particulars furnished in terms of this section within 90 days after such a change.

COMPLIANCE AND ENFORCEMENT

The FIC Act distinguishes between administrative sanctions and criminal offences.

The Centre or a supervisory body may impose an administrative sanction on the institution when satisfied that the institution has failed to comply with a provision of the FIC Act or any order, determination or directive made in terms of the FIC Act. It may also impose an administrative sanction if the institution has failed to comply with a condition of a licence, registration, approval or authorisation issued or amended. It may furthermore impose an administrative sanction if the institution has failed to comply with a directive or has failed to comply with a non-financial administrative sanction.

Administrative sanctions may include a financial penalty not exceeding R10 million in respect of natural persons and R50 million in respect of any legal person (Section 45C(3)(e)). The Centre or supervisory body may direct that a financial penalty must be paid by a natural person or persons for whose actions the relevant institution is accountable in law, if that person or persons was or were personally responsible for the non-compliance.

A person convicted of an offence in terms of the FIC Act, other than an offence mentioned hereafter, is liable to imprisonment for a period not exceeding 15 years or to a fine not exceeding R100 million. A person convicted of an offence mentioned in section 55 62A, 62B, 62C or 62D, is liable to imprisonment for a period not exceeding 5 years or to a fine not exceeding R10 million.

Regulations issued under the FIC Act may (for a contravention of or failure to comply with any specific regulation) prescribe imprisonment for a period not exceeding 3 years or a fine not exceeding R1 000 000 or such administrative sanction as may apply.

Failure to submit suspicious and unusual transaction reports in terms of section 29 of the FIC Act may lead to further offences under section 2(1)(a) or (b), 4, 5 or 6 of POCA and/or section 4(1), (2) and (3) of POCDATARA.

POCA penalties for committing a section 2(1) offence equals a fine not exceeding R1000 million or to imprisonment for a period up to imprisonment for life.

POCA penalties for committing a section 4, 5 or 6 offence equals a fine not exceeding R100 million or to imprisonment for a period not exceeding 30 years.

POCDATARA penalties for committing an offence under section 4 equals a fine not exceeding R100 million or to imprisonment for a period not exceeding 15 years.

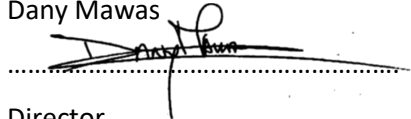
APPROVAL OF RISK MANAGEMENT COMPLIANCE PROGRAMME

The board of directors, exercising the highest level of authority of Raise Global SA hereby approves this Risk Management Compliance Programme and binds itself to create a culture of compliance within the institution, ensuring that the institution's policies, procedures and processes are designed to limit and control risks of money laundering and terrorist financing.

Full name: Dany Mawas

Signature:

Designation: Director

A handwritten signature in black ink, appearing to read 'Dany Mawas', is written over a horizontal dotted line. The signature is stylized and extends slightly above and below the line.

Signed on August 28th in 2023



RAISE GLOBAL SA (Pty) Ltd

2018/616118/07

INTERNAL REPORTING POLICY

An authorised Financial Services Provider FSP No: 50506

AUGUST 2023

**Purpose:**

The purpose of this Internal Report Policy is to establish a framework for reporting any internal concerns or potential violations of laws, regulations, or company policies related to our online trading activities. This policy aims to create an environment where employees feel comfortable coming forward with such concerns without fear of retaliation.

Scope:

This policy applies to all employees, contractors, and third-party associates engaged in activities related to the online trading services offered by RaiseFX. This includes individuals at all levels of the organization, emphasizing that everyone has a shared responsibility to uphold the ethical standards and compliance measures.

Reporting Mechanisms:**a. Internal Reporting Channel**

Employees are encouraged to report any concerns or potential violations to their immediate supervisor or, if they prefer, through our dedicated email address: compliance.sa@raisefx.com.

b. Whistleblower Protection

RaiseFX is committed to protecting employees who make good faith reports. Retaliation against any employee for reporting concerns is strictly prohibited and will be subject to disciplinary action, up to and including termination. This commitment should be clearly communicated to all employees to ensure confidence in the reporting process.

Investigation Process:**a. Designated Investigator**

Upon receiving a report, RaiseFX will assign a designated investigator, often from the compliance or legal team, to conduct a thorough and impartial investigation. This investigator should have the necessary expertise to handle the specific type of concern being reported.

b. Confidentiality

To the extent permitted by law, the identity of the individual making the report will be kept confidential. However, the company may need to disclose information during the investigation process. It's crucial to strike a balance between maintaining confidentiality and ensuring a thorough investigation.

c. Reporting Periodic Updates:

The designated investigator will provide periodic updates to the reporting individual, and the firm's management, as appropriate, regarding the progress of the investigation. Clear communication during the investigation process helps in maintaining transparency and building trust among employees.

**Non-Retaliation:**

Employees who make good faith reports will be protected against retaliation. Any employee found to be engaging in retaliation will be subject to disciplinary action. It's essential to emphasize that the company takes retaliation seriously and is committed to creating a safe environment for employees to report concerns without fear of reprisal.

Disciplinary Actions:

Employees found to have engaged in misconduct following the conclusion of an investigation may be subject to disciplinary action, including but not limited to verbal or written warnings, suspension, or termination. The severity of the disciplinary action should be proportionate to the seriousness of the violation.

Training and Awareness:

RaiseFX will conduct periodic training sessions to educate employees on this Internal Reporting Policy, emphasizing the importance of reporting concerns and the protections in place for whistleblowers. These training sessions can be conducted through workshops, online modules, or in-person seminars to ensure that all employees are well-informed about the policy and its implementation.

Review and Update:

This policy will be reviewed periodically and updated as necessary to ensure its effectiveness and relevance to the evolving regulatory landscape. Regular reviews should be conducted in collaboration with legal and compliance teams to incorporate any changes in regulations and to address any shortcomings identified in the reporting and investigation process.



Document METADATA

Document number:	#1
Document version:	V1.1
Document approval authority:	Dany Mawas
Document approval date:	August 2023
Document owner:	Kevin Wides
Document author(s):	Kevin Wides
Last updated:	August 2023
Next review date:	December 2023