attooh!
HEALTH | WEALTH | LIFE

RISK MANAGEMENT AND COMPLIANCE PROGRAMME (RMCP)

FINANCIAL INTELLIGENCE CENTRE ACT, 2001

as amended by the

FINANCIAL INTELLIGENCE CENTRE AMENDMENT ACT, 2017

ACCOUNTABLE INSITUTION: ORG2421

CONTENTS

Acronyms	Definition
AI	Accountable institution as defined by the FIC Act
AML	Anti-money laundering
Amendment Act	Financial Intelligence Centre Amendment Act 1 of 2017
CDD	Customer due diligence
CFT	Countering the financing of terrorism
CTR	Cash Threshold Report
EDD	Enhanced due diligence
FATF	Financial Action Task Force (an international body of countries tasked with setting best practices to combat money laundering and terrorism financing. SA has been a member of FATF since 2003 and is also a signatory to the United Nations Convention against Corruption in 2004)
FSP	Financial services provider
FIC	Financial Intelligence Centre
FIC Act	Financial Intelligence Centre Act 38 of 2001
FSCA	Financial Sector Conduct Authority **(FSCA)** (previously the Financial Services Board (FSB))
MLO	Money Laundering Officer
NCCT	Non-cooperative countries and territories
ODD	Ongoing due diligence
PEP	Politically Exposed Person (persons with prominent public functions)
RMCP	Risk Management Compliance Programme
STR	Suspicious Transaction Report
TFS	Targeted financial sanctions
TPR	Terrorist Property Report
UNSC	United Nations Security Council

1. INTRODUCTION

1.1 Purpose of the FIC Act and the Risk Management Compliance Program

The Financial Intelligence Centre Act **(FICA)** was enacted to combat money laundering activities and later, this included the countering of financing of terrorist and related activities. This is part of the fight against crime and terror financing in order for South Africa to protect the integrity and stability of its financial system.

The FIC Act provides the legal framework that supports the administration of the criminal justice system together with legislation such as the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 33 of 2004 **(POCDATARA)** and Prevention of Organized Crime Act, No 121 of 1998 **(POCA)**.

The purpose of the FIC Act is to:

- assist in the identification of the proceeds of unlawful activities
- combat money laundering
- combat the financing of terrorist and related activities.

The objectives of the Financial Intelligence Centre **(FIC)** are to:

- assist in identifying proceeds of unlawful activities and the combating of money laundering and terrorist financing;
- implement financial sanctions pursuant to resolutions adopted by the United Nations Security Council **(UNSC)**;
- make information available to various authorities and bodies within South Africa;
- administer measures requiring accountable institutions **(AI's)** to freeze property and transactions pursuant to financial sanctions that may arise from resolutions adopted by the UNSC;
- exchange information with bodies in other countries regarding money laundering;
- supervise and enforce compliance with the FIC Act.

The FIC Act requires accountable institutions **(AI's)** (as defined in the FIC Act) to:

- apply a risk-based approach to customer due diligence **(CDD)** to ensure that AI's are compliant with the regulatory requirements of the FIC Act. The Company therefore has to develop, document, maintain and implement a Risk Management Compliance Program **(RMCP)** which will enable the Company to identify; assess; monitor; mitigate; and manage the risk which the Company faces as we provide products and services which could involve or facilitate money laundering activities or the financing of terrorist and related activities. This contributes to:
  - making it more difficult for criminals to hide their illicit proceeds in the formal financial sector and profit from their criminal activities
  - cutting of the resources available to terrorists
- follow certain procedures and report suspicious activities or unusual transactions in the combating of money laundering.

EXAMPLES of accountable institutions* (see Schedule 1 to the FIC Act)*:

A financial services provider **(FSP)** authorised in terms of the Financial Advisory and Intermediary Services Act, 2002 **(FAIS Act)**, to provide advice and intermediary services in respect of any financial product

This excludes:

- a short -term insurance contract/policy referred to in the Short-Term Insurance Act, 1998
- a health service benefit provided by a medical scheme as defined in section 1(1) of the Medical Schemes Act, 1998.

A person who carries on long-term insurance business as defined in the Long-Term Insurance Act, 1998, including an insurance broker and an agent of an insurer.

An estate agent as defined in the Estate Agents Act, 1976.

An attorney as defined in the Attorneys Act, 1979.

The FIC Act empowers various supervisory bodies to supervise compliance with the FIC Act by AI's which are under their control.

EXAMPLES of supervisory bodies:

The Financial Sector Conduct Authority **(FSCA)**.

The Estate Agency Affairs Board.

Law societies.

As an AI, if the Company fails to comply with its obligations, it may be subjected to corrective action by the FSCA as its supervisory body **in addition to** being prosecuted for the offences linked to non-compliance. More on this below.

1.2 What is Money Laundering?

Money laundering is the process of disguising the proceeds of crime and integrating it into the legitimate financial system. Before proceeds of crime are laundered, it is problematic for criminals to use the illicit money because they cannot explain where it came from and it is easier to trace it back to the crime.

1.3 Stages of Money Laundering

Three stages are generally distinguished in the money laundering process:

- Placement: In this stage funds derived directly from a criminal activity are introduced into the financial system.

- Layering: In this stage, the aim is to separate the illicit proceeds from their criminal source, usually by a succession of complex financial transactions designed to obscure the audit trail of the money.

- Integration: In this stage, the illicit funds (minus the costs of laundering) are brought back into the economy, under the control of the criminal, in such a way that they appear as legitimate funds ("clean" money).

Depending on the sophistication of the criminal and the amounts of illicit funds involved, not all money laundering schemes will involve all three stages and the stages may overlap. Usually the best chance of detecting money laundering is in the placement stage when criminal proceeds are first introduced into the financial system.

2. THE CURRENT LEGAL POSITION AND PENALTIES

2.1 Current South African Legislation

There are three important pieces of legislation that have been enacted to drive Anti-Money Laundering **(AML)** and Countering the Financing of Terrorism **(CFT)** in SA:

2.1.1 Prevention of Organized Crime Act, No 121 of 1998 (POCA)

This Act contains the offences directly relating to money laundering and defines the money laundering offences. It criminalizes any act in respect of the proceeds of crime which is likely to have the effect of concealing or disguising the nature, source, location or movement of the proceeds of unlawful activities or which is likely to assist a criminal to avoid prosecution or to remove or diminish such proceeds. It also criminalizes the rendering of assistance to another person to enable him to benefit from crime and makes it an offence to acquire, use or possess the proceeds of the crime of another person. Although the FIC Act introduces mechanisms aimed at preventing money laundering and creates a regulatory regime which applies to institutions and entities that might otherwise be exploited for money laundering purposes, specific offences relating to organized crime, racketeering, participation in gang activities and money laundering are still governed by POCA.

People engaging in money laundering transactions can be charged under POCA.

2.1.2 Financial Intelligence Centre Act, No 38 of 2001 (the FIC Act) as amended by the Financial Intelligence Centre Amendment Act, No 1 of 2017 (Amendment Act)

This introduces a general money laundering control framework as it co-opts the financial sector (and certain other sectors) in the prevention and detection of money laundering by imposing compliance obligations on certain types of institutions (called accountable institutions) to assist in the fight against money laundering. It also establishes the FIC to assist in the identification of the proceeds of unlawful activities and the combating of money laundering activities. It creates a number of offences relating to non-compliance with the money laundering control obligations it imposes on certain types of institutions and in some cases on all businesses. Such obligations include the duty to identify and

verify the identity of clients, record keeping requirements, the duty to report suspicious or unusual transactions to the FIC, implement internal rules, appoint a compliance officer and train their employees to recognize and deal with suspected money laundering.

2.1.3 **Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 33 of 2004 (POCDATARA)**

This Act provides measures for the prevention of terrorist related activities and to further provide measures to prevent the financing of these activities. It further stipulates that any person who has reason to suspect that any other person intends to commit an offence as stipulated above must as soon as possible report such suspicion to a police official.

EXAMPLE: Mr van Rensburg is a licensed FSP and he is also a silent partner in a local night club. His partner in this business, Mr Jones, has been earning extra money in drug trafficking in the club. He always uses the proceeds of these activities to purchase insurance policies with Mr van Rensburg, who then earns commission on the large cash transactions. Mr van Rensburg is well aware of the origins of the money invested, but since he is earning a good living off this scheme, he has no intention of ever reporting any of these deals.
If caught, both Mr van Rensburg and Mr Jones will be charged under POCA. Mr Jones has knowingly laundered the proceeds of unlawful activities. Mr van Rensburg has contravened the same section of POCA in that he proceeded with selling a client an insurance policy with the knowledge that the money for such policy has been derived from the proceeds of a crime. Mr van Rensburg has also contravened the provisions of the FIC Act, since he did not report his suspicions.

2.2 **Offences and Penalties**

2.2.1 The money laundering offences under POCA carry penalties of fines of up to R100 million or imprisonment of up to 30 years. Both employees in their personal capacity, and/or the Company, may be liable if found guilty of an offence.

2.2.2 The main offences under the FIC Act (as amended) and the applicable penalties are as follows:

Administrative Sanction (section 45C): Fine of up to R50 million for a legal person or R10 million for natural person:

Contravention resulting in non-compliance with the FIC Act (as amended):	Section
Failure to identify clients (section 21)	46
Failure to comply with duty in regard to customer due diligence (sections 21A to 21H)	46A
Failure to keep records (sections 22, 22A, 23, 24)	47
Failure to comply with duty in respect of RMCP (section 42)	61
Failure to register with the FIC (section 43B)	61A
Failure to comply with duty in regard to governance (section 42A)	61B
Failure to provide training (section 43)	62
Failure to comply with directives of the FIC or supervisory body (section 43A(3) or 45C(3)(c)	62E

Fine of up to R100 million or imprisonment of up to 15 years (section 68(1)):

Contravention of the FIC Act (as amended) resulting in offence:	**Section**
Tampering with records kept in terms of section 22 or 24(1), or wilfully destroying such records (otherwise than in accordance with section 23)	48
Failure to give assistance to a FIC representative (section 27A(5))	49
Contravention of prohibitions relating to persons and entities identified by the UNSC (section 26B)	49A
Failure to advise FIC of client (section 27)	50
Failure to report cash transactions (section 28)	51
Failure to report property associated with terrorist and related activities and financial sanctions pursuant to Resolutions of the UNSC (section 28A)	51A
Failure to report suspicious or unusual transactions (section 29(1) or (2))	52
Unauthorised disclosure (section 29(3) or (4))	53
Failure to report conveyance of cash or bearer negotiable instruments into or out of the Republic (section 30)	54 & 55
Failure to report electronic transfers (section 31)	56
Failure to comply with a request (section 32(2) or 45(1B)(d))	57
Failure to comply with direction of FIC (section 34(1))	58

Misuse of information (other than in accordance with section 40)) or disclosing a fact / information (as contemplated in section 45B(2A)) or using such information (otherwise than as permitted by section 45B(5))	60
Obstructing of official in performance of functions	63
Conducting transactions to avoid reporting duties	64
Unauthorised access to computer system or application or data	65
Unauthorised modification of contents of computer system	66

Fine of up to R10 million or imprisonment of up to 5 years (section 68(2)):

Contravention of the FIC Act (as amended) resulting in offence:	**Section**
Offences relating to inspection	62A
Hindering or obstructing the appeal board	62B
Failure to attend when summoned	62C
Failure to answer fully or truthfully	62D

2.2.3 There are also offences that are specific to an FSP, i.e. the Company, specified in section 4 of the POCDATARA. These include the following:

Fine of up to R100 million or imprisonment of up to 15 years (High or Regional Court) OR fine of up to R250k or imprisonment of up to 5 years (Magistrate's Court):

- Acquire, collect, use, possess or own property ***(note – the definition of "property" includes money)***, with the intention that the property may be used, or knows or ought reasonably to know that the property may be used to commit an offence

- Provide or make available, or invite a person to provide or make available property, ***any financial service***, economic support and who knows or suspects that the property, financial service and economic support may be used for the commission of an offence relating to terrorist activity, either in whole or in part

- Deal with, enter into or facilitate transactions in connection with property, when he knows or ought reasonably to have known that the property has been acquired, collected, used, owned or provided to commit an offence, or who provides ***financial or other services*** in respect of this property

- Enter into an arrangement which has the effect of facilitating the retention of property by an entity which commits or attempts to commit an offence by either converting, concealing or disguising the nature of such property, removing such property from a jurisdiction or transferring such property to a nominee.

- In terms of **Section 42 (2A**) of the FIC Act, the following provisions are not applicable to the Company and this RMCP, for reasons as indicated:

  - Section 42(2)(q) – The Company has no branches, subsidiaries or other operations in foreign countries. All branches, subsidiaries and operations of the Company as an accountable institution are situated locally within the borders of South Africa.

3. THE COMPANY POLICY

- The Company will not be associated with money laundering and terrorist or related activities and has introduced policies and procedures to comply with all statutory and regulatory obligations. The Company will ensure that these policies are adhered to at all times.

- The Company may decline or terminate business relationships where there appears to be a risk of its services being abused for the purposes of laundering funds associated with unlawful activities.

- The Company will report any knowledge or suspicion of unlawful activities to the FIC as required and will co-operate with the FIC and law enforcement agencies as required in terms of its legal obligations.

- The Company will undertake appropriate AML and CTF employee training.

- This RMCP will be regularly reviewed to ensure that it remains relevant to the Company's operations, specifically any further money laundering and terrorist financing risks it may identify, to ensure that it continually mitigates and manages such risk.

- **The Company has appointed:**
  Riana Kleynhans
  Contact no: (012) 368 9900 or +27834578085
  e-mail address: rianak@attooh.co.za

  as the FICA Compliance and Money Laundering Officer **(MLO)** (in terms of section 42A(2)(b)) (**MLO)** to assist the Board of Directors (or Senior Management if there is no Board) in discharging their obligations to ensure compliance by the Company and its employees with the FIC Act and its RMCP.

- The Company has registered with the FIC as an AI and has employees dedicated to the necessary reporting duties who have their own separate log in credentials.

- The Company shall in terms of Part 2 of Chapter 3 of the FICA Act, ensure that all FICA and/or related records of the Company as a whole, including any of its local branches are maintained in a compliant, safe, and easily accessible electronic format, for immediate and direct access from the Company's registered Head office address situated at Unit 1B, Menlyn Woods Office Park, Faerie Glen, Pretoria. **(Section 42(2)(n))**

- The FIC Act creates various money laundering and terrorist financing **control obligations** for the Company as an AI, which include:
  - To establish and verify clients' identities *(responsibility of employees)*

- To retain records concerning client identification and transaction activity *(responsibility of employees)*
- To report certain transactions to the FIC *(responsibility of the MLO)*
- To prevent unauthorized access to information *(responsibility of employees)*
- To formulate and implement a RMCP *(responsibility of management)*
- To train our employees *(responsibility of the FICA CO & MLO)*
- To appoint a person with adequate seniority and experience to assist with ensuring compliance with the FIC Act *(responsibility of management).*

3.1 Responsibilities of Management:

Management is responsible for:

- the development, documentation, maintenance and implementation of this RMCP;
- the review of this RMCP at regular intervals to ensure that it remains relevant to the Company's operations and the achievement of the requirements required by the FIC Act **(section 42(2C));**
- the day-to-day compliance with the Company's AML and CTF obligations and RMCP within the areas of the Company for which they are responsible;
- ensuring that the documentation describing the RMCP is made available to each of its employees who may be involved in transactions to which the FIC Act applies and, on request, to the FIC or the FSCA **(sections 42(3) and (4)**;
- ensuring that the Company has a compliance function to assist the Board of Directors (or the Senior Management if there is no Board) to discharge its obligations (which are to ensure compliance by the Company and its employees with the provisions of the FIC Act and this RMCP) **(section 42A(2)(a)**;
- ensuring that a person with sufficient competence and authority is assigned to ensure the effectiveness of the compliance function referred to above **(section 42A(2)(b).**

3.2 Responsibilities of Board of Directors or Senior Management:

Board of Directors (or Senior Management if there is no Board) is responsible for:

- ensuring compliance by the Company and its employees with the provisions of the FIC Act and this RMCP **(section 42A(1)**;
- the formal approval of this RMCP **(section 42(2B).**

Senior Management is responsible for:

- where applicable, giving approval for establishing a business relationship with a prospective client who is a foreign prominent public official or a domestic prominent influential person **(sections 21F(a) and 21G(a))**.

3.3 Responsibilities of the CO/ MLO:

The fica Compliance Officer/MLO, is responsible for:

- supporting management and employees in achieving compliance with all applicable AML and CTF legislation;
- facilitating the ongoing training of employees in terms of the provisions of Section 43 of the FIC Act, to enable the employees to comply with the provisions of the FIC Act and the RMCP;
- developing and implementing a risk framework to accurately assess the risks involved;
- assisting with the development of necessary policies and procedures in line with AML and CFT legislation;
- representing the Company when dealing with external agencies such as the FIC or law enforcement agencies, in respect of money laundering and terrorist related matters;
- maintaining a register of suspicious or unusual transaction reports;
- carrying out monitoring activities as required, checking that all parts of the Company are complying with this RMCP and the Company's policies;
- online registration and approval of employees handling FIC related activities;
- where applicable, conduct enhanced ongoing monitoring of the business relationship established with a client who is a foreign prominent public official, a domestic prominent influential person and/or a family member of close known associate of the a foregoing **(sections 21F(c) and 21G(c) and 21H)**.

3.4 <u>Responsibilities of Employees (who are involved in the Company's relationship with its clients):</u>

All such employees are responsible for:

- remaining vigilant to the possibility of money laundering and terrorist financing;
- reporting to the MLO all suspicious or unusual transactions as set out in this RMCP;
- complying in full with all AML procedures and the RMCP in respect of client identification, record keeping and reporting of suspicious transactions;
- not tipping off clients where a suspicious transactions report has been made and not making unauthorized disclosures of information relating to any such reports;

- staying up to date with their obligations in terms of this RMCP and attending training sessions when required.

Note: Failure to comply with the Company's AML and CFT procedures and RMCP will be considered to be a serious breach of responsibilities and may lead to disciplinary action against the individual.

3.5 Client Confidentiality:

- Ordinarily, client confidentiality is very important. However, the Company's duty to report knowledge or suspicion of unlawful activities in terms of the FIC Act, **overrides the duty of client confidentiality**.

- The legislation protects both the Company and individual employees from being sued for breach of client confidentiality.

4. CUSTOMER DUE DILIGENCE (Sections 20A, 21 and 21A to 21H) (see *Annexures A* and *B* hereto)

4.1 Introduction:

4.1.1 The Company may not establish a business relationship / conclude a single transaction with an anonymous client or a client with an apparent false of fictitious name **(section 20A)**.

4.1.1.1 In terms of this RMCP adopted, implemented and prescribed by the Company, any reference to "business relationship", shall mean the arrangement for financial and advisory services between the Client and the Company or any of its persons (including but not limited to management, authorised representatives and/or employees), resulting in the Client's acceptance of a new business quotation and/or instruction for the submission of an application for purposes of the issuing of any long term insurance product, as defined in terms of the long- term insurance act 52 of 1998, and shall include any ongoing financial and advisory services provided to the Client, in maintaining and servicing any existing long-term insurance policies held by the client. **(Section 42(2)(b)(i) &(ii);**

4.1.1.2 A single transaction shall for the purposes of this RMCP be defined as a transaction–

a) other than a transaction concluded in the course of a business relation; and
b) where the value of the transaction is not less then the amount as prescribed from time to time (Section 1A), except in the case of a such single transaction being concluded with an anonymous client or a client with an apparent false or fictitious name.

4.1.2 When the Company engages with a prospective client, the Company must, in the course of concluding that single transaction / establishing that business relationship:

(a) establish and verify the identity of that client;

(b) if the client is acting on behalf of another person, establish and verify—
(i) the identity of that other person; and
(ii) the client's authority to establish the business relationship / to conclude the single transaction on behalf of that other person; and

(c) if another person is acting on behalf of the client, establish and verify—
(i) the identity of that other person; and
(ii) that other person's authority to act on behalf of the client **(section 21)**.

4.1.3 The Company must establish and verify the identity of <u>any person</u> who provides funds, gives instructions or is involved in the operation of a structure. For example, in addition to the actual client, the details of a person who is a joint signatory, trustees of a trust, directors of a company or an agent who is acting on behalf of a client, or in terms of a Power of Attorney, will need to be verified.

4.1.4 The Company needs to know the <u>true identity</u> of the person who is using the Company's services, in all the Company's business relationships.
Are they really who they say they are (Identity document/Passport**)?**
Where can they be found if needed during an enquiry (Proof of physical address**)?**
Do they have authority to make the investment (Resolutions**)?**

4.2 <u>Requirements:</u>

4.2.1 The documents required for the verification of clients ("FICA documents") are contained in ***Annexure A*** and are to be obtained by the mandated and authorized representative concluding the business relationship with the client.

4.2.2 The representative of the Company shall ensure that such FICA documents are as soon as possible and within 24(twenty four) working hours, uploaded electronically onto the Company's current CRM management system under such Client's file, so as to enable the Company's head office situated at the Company's registered address, Pretoria, to conduct and commence the verification and/or due diligence processes, prior to the entering of any business relationship with the client. The representative shall furthermore (where applicable), ensure the necessary control and safekeeping processes are implemented within their offices, for the safekeeping of such documents, despite being electronically uploaded on the Company's CRM system. (Section 42(2)(n)).

4.2.3 The documents required for the verification of clients ("FICA documents") are contained in ***Annexure A*** and are to be submitted to the relevant product provider together with the client's completed application form.

4.2.4 Employees must also:

- understand and obtain information on the <u>business relationships with clients</u>, which is the arrangement between the client and the Company for concluding transactions on a regular basis

over time. These documents are also listed in ***Annexure A****;*

- comply with additional due diligence measures relating to legal persons, trust, partnerships,

- attend to ongoing due diligence,

- know what to do if they doubt the veracity of previously obtained information and if they are unable to conduct customer due diligence,

- conduct enhanced ongoing monitoring of the business relationship when clients are foreign prominent public officials, domestic prominent influential persons and/or family members and close known associates of the a foregoing **(Sections 21A to 21H) (See *Annexure B*** for the process guide**)**

4.3 Responsibilities of Employees:

4.3.1 General responsibilities applicable to all the Company employees:

4.3.1.1 the Company is not allowed to enter into a business relationship / to transact with a client unless the relevant identification information (as per ***Annexure A – FICA documents***), has been received and verified. These documents must be certified copies where required and filed in hard copy or electronically. Client information must be updated as and when changes occur and must be maintained for a period of at least five years after termination of the Company's relationship with the client;

4.3.1.2 the Company is **prohibited** from transacting with existing clients without identifying and verifying the details of these clients, and the employees are obliged to obtain the required verification documentation;

4.3.1.3 **the Company will not be able to start trading for or with the client, accept funds or assets from the client, until the relevant information has been received and verified**;

4.3.1.4 it is the responsibility of **all the Company employees** to comply with the requirements of the FIC Act **regarding client identification** and **verification**, and with this RMCP. **Disciplinary action may be taken against staff members who do not comply with the FIC Act, or this RMCP**;

4.3.1.5 employees must lodge all suspicious transactions, including relevant attachments with the MLO as soon as any suspicion arises **(within 24 hours of such suspicion arising)**. This must be done in hardcopy or electronically via email or by hand to the MLO as per the details provided above.

4.4 Responsibilities of the MLO:

4.4.1 General responsibilities:

4.4.1.1 the MLO must ensure that the responsible persons in the various business units are complying with the FIC Act client identification and verification requirements. Compliance monitoring is performed on an ongoing and regular basis;

4.4.1.2 the MLO must provide ongoing FICA awareness training, as required.

5. KEEPING OF RECORDS (Sections 22, 22A, 23, and 24):

5.1 Introduction:

The FIC Act obliges the Company to keep both customer due diligence records and transaction records.

5.2 Responsibilities of Company Employees:

5.2.1 To Keep Customer Due Diligence Records:

5.2.1.1 employees must keep a record of the information obtained in compliance with sections 21 to 21H **(see *Annexures A* and *B)***. The records must -

(a) include copies of, or references to, information obtained by the employee to verify a person's identity; and

(b) in the case of a business relationship, reflect the information obtained by the employee under section 21A concerning—
(i) the nature of the business relationship;
(ii) the intended purpose of the business relationship; and
(iii) the *source of the funds which the prospective client is expected to use in concluding transactions in the course of the business relationship (section 22);

(* 'Source of funds' means the origin of the funds involved in a business relationship or single transaction. It includes both the activity that generated the funds used in the business relationship (for example the client's salary, occupation, business activities, proceeds of sale, corporate dividends, etc.), as well as the means through which the client's funds were transferred)

5.2.1.2 these records must be kept for a **minimum of five (5) years from the date of termination of the business relationship with the client** (section 23(a))**.**

5.2.2 To Keep Transaction Records:

5.2.2.1 employees must keep a record of all transactions that are reasonably necessary to enable the reconstruction of such transaction. Records must show -

(a) the amount and currency involved;
(b) the date on which the transaction was concluded;
(c) the parties to the transaction;

(d) the nature of the transaction;
(e) business correspondence; and
(f) any identifying particulars of the client's accounts with the Company that are related to the transaction (section 22A);

5.2.2.2 these records must be kept for a **minimum of five (5) years** from the **date of the transaction** (section 23(b))**.**

5.2.3 To Keep Records Which Give Rise to a Section 29 Report:

5.2.3.1 employees must keep records of suspicious and unusual transactions which give rise to a report contemplated in section 29 for a **minimum of five (5) years** from the **date that the report was submitted to the FIC** (section 23(c)).

5.2.4 Record Keeping Procedures (section 24):

The Company's record keeping procedures are also detailed in the Company's Risk Management Programme and Business Continuity Plan:

5.2.4.1 records kept in terms of sections 22 and 22A may be kept in electronic form, must be kept safe from destruction and must be capable of being reproduced in a legible format;

5.2.4.2 records kept in terms of sections 22 and 22A may be kept by a third party on behalf of the Company, but the particulars of the third party have to be provided to the FIC and the supervisory body concerned. The Company must also be able to request those records from the third party within a reasonable period of time if ever requested to do so by the FIC or the relevant supervisory body;

5.2.4.3 employees must take cognizance of the fact that **authorized representatives from the FIC** are allowed access to the records during working hours, and should provide assistance where possible, after informing the MLO of the request and getting the approval of the MLO to provide assistance (Section 27A);

5.2.4.4 employees must be fully aware of the records that they are required to keep (as per ***Annexure A- FICA documents***), and they should approach the MLO for guidance in situations when they are uncertain;

5.2.4.5 it is the responsibility of **all the Company's employees** (including the Key Individuals, MLO and Management) to comply with the requirements of the FIC Act regarding **record keeping** (Sections 22 and 22A) and with the Company's internal procedures in this regard. **Disciplinary action may be taken against employees who do not comply.**

6. REPORTING DUTIES (Sections 27, 28 and 29)

The Company's appointed Money Laundering Officer shall be appointed as the responsible reporting individual for all reporting in terms of the FIC and related legislation. Where the appointed Moany Laundering Offer is unable to report in terms of the accountable institutions'

obligations for any reason whatsoever, such reporting obligation shall be the responsibility of the Key Individual of the accountable institution, with the necessary reporting abilities to the FIC.

Reporting by the appointed money launder officer and/or Key Individual shall where applicable, take place within the prescribed and legislated time periods.

Internal reporting and/or investigations shall take place within the necessary internal periods prescribed below, so as to ensure sufficient reporting compliance within the prescribed time periods to the FIC, where necessary.

Internal investigations and reporting shall be made in accordance with the processes below, and shall require the completion of the appendices 1, 2 and 3 to the RMCP, where applicable.

All reporting by the appointed Money Laundering Officer and/or Key Individual of the Company to the FIC shall be made by completing the FIC standard reporting form/s and submitting the report/s using the internet-based reporting portal provided by the FIC at http://www.fic.gov.za. If for some reason the reporting cannot be submitted electronically, the required form will be faxed, or hand delivered to the FIC.

6.1 Company to advise the FIC of clients (Section 27):

a) Respond to reported requests on entities or individuals within given time deadlines on whether the Company has any business dealings currently or in the past;

b) Retain proof of submission of reported responses.

6.2 Cash Transactions above prescribed limit R24,999.99 (Section 28):

a) All transactions to be reported to the FIC (online) within 48 hours after the Company or any of its employees have become aware (have *knowledge) of a cash transaction or a series of cash transactions that has exceeded the prescribed limit;

b) The aggregate of transactions from the same client per day must also be reported if above the prescribed limit;

c) Proof of the submission of Cash Threshold Reports **(CTR's)** AND Suspicious Transaction Reports **(STR's)**. Also Terrorist Property Reports **(TPRs)** (if appropriate).

Cash is defined as any coins, notes or legal tender of any country and includes traveller's cheques. Cash does not include EFT's; electronic wires or transactions falling outside of the definition of Cash.

The obligation to report extends to cash in excess of the prescribed amount being **paid out** or **received by** the Company.

(* knowledge will normally be acquired when the Company:

- physically received or pays out cash exceeding R24,999.99
- examines the client's bank statement or a bank deposit slip from the client reflecting the transaction that exceeds R24,999.99.

6.3 Property associated with terrorist and related activities and financial sanctions pursuant to Resolutions of the UNSC (Section 28A):

a) Report a transaction (online) involving the property in the Company's possession or under its control which is owned or controlled by or on behalf of a person or an entity identified in the sanctions list (as per detail below and ***Annexure B***).

b) Sanctions impose restrictions on activities that relate to particular countries, goods and services, or persons and entities. Targeted financial sanctions **(TFS)** measures restrict sanctioned persons and entities from having access to funds and property under their control and from receiving financial services in relation to such funds and property. In order for these sanctions to be given effect, the FIC Act requires AI's to freeze property and transactions pursuant to financial sanctions imposed in the UNSC Resolutions;

c) Mechanisms for implementation of the UNSC Resolutions

- the publication in the Government Gazette by the Minister of Finance of a Notice of the adoption of the UNSC Resolution, and
- the publication of a Notice by the Director of the Centre of persons who are subject to the sanction measures (the sanctions list).

These Notices:

- may be revoked if it is considered that they are no longer necessary to give effect to the applicable UNSC Resolutions. Otherwise the sanctions announced in these Notices remain in effect indefinitely;
- are public statements and are meant to advise both sanctioned persons and entities and AI's who may have them as clients or prospective clients of the relevant sanctions. If an AI has a sanctioned person or entity as a client it is allowed to draw the attention of the person or entity to the relevant sanctions notices.

d) The acquisition, collection or use of the property of persons or an entity whose names appear in the sanctions is **prohibited**. This includes the provision of financial services and products to those persons or entities. The Company is not allowed to transact with a sanctioned person or entity or to process transactions for such a person or entity. The status quo as at the time of the imposition of the sanction in relation property or funds of the sanctioned person or entity must be maintained and no financial services may be provided to the person or entity.

e) Clients must be screened during the client-take-on process as well as subsequently as and when the UNSC adopts new TFS measures or expand existing ones.

f) FIC will maintain an updated sanctions list which will be available on its website and which will reflect available identity particulars of persons and entities contained in notices published by the Director.

A copy of the UNSC consolidated sanction list is viewable on the UNSC website at: https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list

6.4 Suspicious and unusual transactions (Section 29):

6.4.1 What is Suspicion?

As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is personal and subjective and falls far short of proof based on firm evidence. However, the suspicion must at least have some foundation and not just be based on mere speculation.

A suspicious transaction will often be:

- any transaction where the amount, duration, or other specific feature is inconsistent with the client's professional or business activities, standard of living, or normal movements on the account; or
- reluctance by the client to furnish the Company with the required FICA documents (as per ***Annexure A***); or
- a transaction that is not logical from an economic, financial or commercial point of view;
- a party to a transaction does not wish to record his/her own name in an agreement but uses the name of a business associate or of a distant relative.

The key to recognizing a suspicious transaction is based on having enough knowledge about a client to be able to recognize the abnormal or unusual from the normal. **All suspicions must be reported to the MLO**.

6.4.2 Examples of Suspicious Transactions in the context of the Company's business:

a) A new or existing client who is reluctant or unable to supply information or documentation required in terms of the FIC Act and/or the Regulations for client identification and verification purposes.

b) A new or existing client who is reluctant to provide normal information when giving account details, providing minimal or fictitious information or providing information that is difficult or expensive for the Company to verify.

c) Where the client keeps changing their bank account.

d) Surrendering of policies shortly after they have been purchased.

e) A client providing doubtful or vague identification documentation.

f) A client refusing to produce personal identification documents.

g) A client changing a transaction after learning that he must provide a form of identification.

h) Any transaction in which the nature, size or frequency appears unusual.

6.5 Reporting Suspicious Transactions:

There are two stages to the suspicious and/or unusual transaction reporting procedure:

a) in the first stage, it is the unusual nature of the transaction that must alert an employee or management to report it. This could occur within various areas of the business,

b) in the second stage, the MLO decides, on the basis of all available information and additional enquiries, whether or not the transactions should remain unusual or suspicious and should be reported, or whether there is some additional information that removes the suspicion.

c) Retain proof of the submission of STRs.

It is the duty of every employee of the Company to report any suspicious or unusual transactions to the following people:

- the MLO, or in his/her absence, to
- any senior manager.

Note: Employees who fail to report such transactions as set out herein will not meet their obligations in terms of the FIC Act and can be subject to the penalties (including criminal sanction) prescribed in the FIC Act and to internal disciplinary action.

It is the responsibility of all the Company employees (including management), who have interaction with clients and potential clients to comply with the relevant sections of the

FIC Act, the Regulations, and the RMCP with regard to the reporting of suspicious transactions.

6.5.1 Responsibilities of Employees and Senior Management:

a) All employees must be alert to the possibility of suspicious or unusual transactions and must be aware of the possible examples of suspicious or unusual transactions listed in the Customer Due Diligence Process Guide (***Annexure B***).

b) All employees with any suspicion must **immediately (within 24 hours from such suspicion arising) report the suspicious or unusual transaction to the MLO** without delay. It is important that the reason for the suspicion is explained fully. This must be done via e-mail to your MLO as per the MLO details above. If an employee has a suspicion but feels that more information should be gathered to be sure, reporting should not be delayed while attempting to gather further information. Reporting should happen if there is a suspicion and any additional information required can be gathered afterwards.

c) **It is vital that no mention of the suspicion is made to the client as this would risk tipping off the client and is prohibited in terms of the FIC Act.** Any employee who intentionally tips off a client or any other person commits an offence and may be liable to disciplinary action. It is thus important that the suspicion is not discussed with anyone, except the Key Individual, the MLO or a director, who will decide whether any other employees should be involved in the investigation as to whether there is a suspicious or unusual transaction. Discussions with the abovementioned persons must only occur for the purposes of carrying out the requirements of the FIC Act, and not for any other purposes.

d) A copy of the report supplied to the MLO should be given to the MLO and Key Individual(s) for his/her information. The employee may discuss the report with such person, who should review the report and also sign the report to acknowledge that they also regard the transaction as suspicious.

e) If an employee believes that his/her supervisor, manager, a Key Individual or director is involved in the client's scheme to launder funds they should contact the MLO immediately. If the employee believes that the MLO is involved they should speak to a Key Individual or director.

f) The MLO will examine all internal reports and make additional enquiries as deemed appropriate. Employees are required to assist the MLO with any additional enquiries if required to do so.

g) This procedure must be followed and repeated every time there is a suspicious or unusual transaction, even if the Company has already notified the FIC of previous suspicious or unusual transactions relating to that particular client.

h) All employees should note that once the reporting process has commenced it must be followed through and completed, even if the original suspicion no longer exists (in other words, the MLO must investigate and properly document his findings as to whether the transaction is suspicious or not and should be reported to the FIC or not).

i) By reporting as required above, employees will discharge their obligations in terms of the FIC Act and avoid the possibility of criminal sanction in terms of the FIC Act. It is important that all employees, Key Individuals and MLO's involved in the reporting chain sign the report as evidence of their suspicions, so that everyone fulfils their duties in terms of the FIC Act.

j) If the FIC or a law enforcement agency approaches the Company for additional information or explanations following a report to the FIC, no employee may provide any explanation or information. The enquirer should be referred to the MLO.

6.5.2 <u>How to behave when faced with a Suspicious or Unusual Transaction:</u>

a) An employee who is faced with a client, transaction or situation that he/she feels is suspicious or unusual, must:

- not make any comment to other employees except the MLO, the, Key Individual or a director/ senior management official if required;
- immediately complete the Company **Internal Suspicious Transactions Report (see Appendix 1)** and report the details to the MLO to enable him/her to make a decision;
- take note of all information available on the proposed transaction. Make copies of documents submitted if possible;
- at no time either confirm or deny to a client or any other third party that a report to the FIC has or may be made;
- ensure that any correspondence that may indicate that a report has been made is **<u>not</u>** placed on the client's file;
- continue with the execution of the transaction after consulting with the MLO and obtaining permission, unless:
    - the transaction involves a withdrawal of a client's funds from or into a bank account of an unrelated or unknown person.

- the FIC, after a report has been made to them by the Company, directs that the Company may not proceed with the transaction in terms of section 34 of the FIC Act (this period may not be longer than 10 days (excluding Saturdays, Sundays and public holidays).

b) As soon as a report is made, whether internally or externally, any subsequent contact with the reported client must be conducted with caution. If the client asks why certain questions are being asked or information requested, employees should reply that it is required as a result of the Company's internal procedures.

c) After making an internal report, employees must obtain guidance from the MLO to establish procedures for further contact with the client. Generally, employees should not contact the client again except to protect the interests of the Company. The MLO must be kept informed of any subsequent contact with the client concerned. In particular, if the client demands that any subsequent transactions are executed; employees should contact the MLO to discuss the situation before completing the transaction.

Note: Where the Company has actual knowledge, as opposed to just a suspicion about a transaction, it is very likely that the transaction will not be continued, in order to protect the Company's reputation (reporting will take place, but the transaction will not be continued).

6.5.3 Responsibilities of the MLO:

a) The MLO will, on receipt of the internal report from an employee, undertake sufficient enquiries to determine whether or not, in his or her judgment, there are grounds for suspicion.

b) The MLO may:

- discuss the report with the employee;
- discuss the report with management within the Company, as may be appropriate and reasonable;
- review copies of documentation relating to the transaction or proposed transaction.

c) The MLO will document his/ her enquiries and complete the Company **Evaluation Record for Suspicious/Unusual Transactions (see Appendix 2)**.

d) The MLO will supply every employee who makes a hard copy report with an **acknowledgement of receipt signed by the MLO** so that such employee has evidence to show that his/her obligations in terms of this RMCP for reporting have been met.

e) All internal reports received by the MLO will be recorded in a **Suspicious Transactions Report Register (see Appendix 3)** and retained for reference and audit purposes, whether or not the transaction is reported to the FIC.

f) The MLO will **not** disclose the identity of the reporting employee to the FIC or report back on the outcome of the report, unless deemed appropriate.

g) The MLO will ensure that any reporting to the FIC is done timeously in terms of the FICA. In terms of Regulation 24 of the FIC Act Regulations, a report must be sent to the FIC **as soon as possible, but not later than 15 (fifteen) days (excluding weekends and public holidays)** after any of the employees or officers of the Company have become aware of a fact concerning a transaction on the basis of which knowledge or a suspicion concerning the transaction must be reported, unless the FIC has approved that the report can be sent after this period has expired.

6.6 Additional duty to Report Terrorist Activities:

- POCDATARA further stipulates that any person who has reason to suspect that any other person intends to commit a terrorist activity related offence as stipulated in 2.2.3 above must as soon as possible report such suspicion to a police official.
- The person reporting the offence may continue with the suspicious transaction unless directed not to proceed by a police official authorized by the National Commissioner. The period within which the person is not authorized to proceed with the suspicious transaction cannot exceed 5 (five) days.
- A person who fails to report suspicious transactions in terms of this provision in terms of POCDATARA is guilty of an offence.

6.6.1 Responsibilities of employees and management:

a) employees must report suspected terrorist related activities to the MLO in exactly the same manner as indicated above for suspicious money laundering related activities;

b) employees must report to the MLO using the same document as indicated in 6.4.2 above (**Internal Suspicious Transactions Report (Appendix 1)**);

c) proof of the submission of TPR's must be retained.

6.6.2 Responsibilities of MLO:

a) The MLO must report suspected terrorist related activities to the FIC in exactly the same manner as indicated above (the reporting form on the FIC website has been amended to facilitate this inclusion).

7 <u>Politically Exposed Persons (PEP's) : Foreign Prominent Public Officials and Domestic Prominent Influential Persons</u> (Sections 21F, 21G and 21H)

1.1 A PEP is an individual who is or has in the past been entrusted with prominent public or private sector position. Schedules 3A and 3B to the FIC Act contains a list of positions that will be considered domestic prominent influential persons (see ***Annexure B***)

1.2 **Business relationships with domestic prominent influential persons are not inherently high-risk**. The Company must consider each such relationship on its own merits in order to determine whether there is any reason to conclude that it brings higher risk of abuse for money laundering and terrorist financing purposes. If so, the Company must apply the same requirements as for foreign prominent public officials.

1.3 **Business relationships with foreign prominent public officials must always be considered high-risk** and senior management approval must be obtained to establish the business relationship.

1.4 <u>Treatment of PEP's in relation to other high-risk clients</u>

a) Senior Management approval should be obtained for establishing business relationships with a PEP. When the client has been accepted, the Company should be required to obtain Senior Management approval to continue the business relationship;

b) the Company should take reasonable measures to establish the source of wealth and the source of funds of customers and the beneficial owners identified as PEP's; and

c) the Company should conduct enhanced ongoing monitoring of a relationship with a PEP.

ANNEXURE A

MINIMUM DOCUMENTS REQUIRED FOR THE IDENTIFICATION AND VERIFICATION OF CLIENTS (FICA documents)

If client is a <u>natural person</u>:

- Certified copy of client's ID
- Proof of client's residential and/or employment/business address
- Proof of client's banking details
- Tax number

If client is a juristic entity (legal person) (e.g (Pty) Ltd / CC / Trust / Partnership):

- Certified copy of client's registration documents
- Proof of client's address
- Proof of client's banking details
- Certified copy of *beneficial owner of legal person's ID

  (*"beneficial owner" in respect of a legal person is the natural person who, independently or together with another person, owns the legal person or exercises effective control of the legal person)

Person acting on behalf of client (regardless of whether client is a natural person or a legal person):

- Certified copy of person acting on behalf of client's ID
- Resolutions/ Power of Attorney
- Proof of person acting on behalf of client's address
- Tax number

Information required for the business relationship:

- The nature and details of the client's business/occupation/employment
- The expected source and origin of the funds to be used in the business relationship
- The anticipated level and nature of the activity that is to be undertaken during the business relationship

The process when identifying and verifying the identity of a client relates to the documents they submit at on-boarding stage. These requirements must be met regardless of whether the client is a natural person or a juristic entity (legal person) (e.g (Pty) Ltd / CC / Trust / Partnership).

These requirements also include identifying and verifying the identity of any person acting on behalf of another person or vice versa.

If client or beneficial owner of client is a:
Foreign prominent public official OR an immediate family member of a foreign prominent public official
(business relationship must always be considered as high-risk)

OR

Domestic prominent influential person OR an immediate family member of a domestic prominent influential person **(business relationship not inherently high-risk):**

- Certified copy of client's ID / passport
- Proof of client's residential and/or employment/business address
- Proof of client's banking details
- Tax number
- Take reasonable measures to establish the source of wealth and funds of client
- Obtain senior management approval to establish the business relationship.

Keep Records

The Company must keep:

Nature of records	**Types of records**	**Records to be kept for:**
Customer due diligence records	1. Verify client's identity 2. Business relationship: 2.1 nature of the business relationship 2.2 intended purpose of the business relationship and 2.3 source of the funds	five (5) years from the date of termination of the business relationship with the client
Transaction records	Be able to reconstruct the transaction, showing: 1. amount and currency involved 2. date of conclusion of transaction was concluded 3. parties 4. nature of the transaction 5. business correspondence 6. identifying particulars of client's accounts with the Company that are related to the transaction	five (5) years from the date of the transaction
Records which give rise to a Section 29 Report	suspicious and unusual transactions	five (5) years from the date that the report was submitted to the FIC

Customer Due Diligence (CDD)

Before a potential client is signed on / on-boarded, a customer due diligence should be conducted.

This requirement entails the following:

- ✓ Verification and identification of the client;
- ✓ Risk rating and source of fund verification;
- ✓ Screening;
- ✓ Enhanced due diligence;
- ✓ Ongoing due diligence.

All requirements mentioned above, except the ongoing due diligence **(ODD)**, must be met prior to the establishment of a relationship, or the conclusion of a single transaction with a new client.

a) Verification and identification of the client

The process when identifying and verifying the identity of a client relates to the documents they submit at on-boarding stage (FICA documents) **(**see ***Annexure A*****)**. These requirements must be met regardless of whether the client is a natural person or a juristic entity (legal person) (e.g (Pty) Ltd / CC / Trust / Partnership).

These requirements also include identifying and verifying the identity of any person acting on behalf of another person or vice versa.

Section 21A of FIC Act further stipulates that the Company is required to:

- Obtain information to reasonably enable the Company to determine whether future transactions performed in the course of the relationship are consistent with the Company's knowledge of that prospective client;
- Obtain information that describes the nature of the business relationship concerned;
- Obtain information on the intended purpose of the business relationship concerned;
- Obtain information on the source of the funds the prospective client expects to use in concluding transactions in the course of the business relationship concerned.

b) Additional measures relating to partnerships (Section 21B)

The Company must establish:

- The nature of the client's business;
- The ownership and control structure of the client;
- If a natural person is acting on behalf of a partnership, the Company must:

❖ Establish the identifying name of the partnership (if applicable);

❖ Establish the identity of every partner, including every member of a partnership *en commandite*, an anonymous partnership or similar partnership;

❖ Establish the identity of the person who exercises executive control over the partnership;

❖ Establish the identity of each natural person who claims to be authorised to enter into a single transaction or business relationship with the Company on behalf of the partnership;

❖ Take reasonable steps to verify the particulars mentioned above; and

❖ Take reasonable steps to verify the identity of these natural persons so that the Company is satisfied that it knows the identities of the natural persons concerned.

These provisions apply whether the partnership is incorporated in South Africa or not.

c) <u>Additional measures relating to legal persons (Section 21B)</u>

The Company must establish:

- The nature of the client's business;
- The ownership and control structure of the client;
- Establish the *beneficial owner where the client is a legal person, of the client by –

    ❖ Determining the identity of each natural person who has a controlling ownership interest in the legal person;

    ❖ Where the above is not applicable, determining the identity of each natural person who exercises control of that legal person through other means; or

    ❖ If no natural person is identified, determining the identity of each natural person who exercises control over the management of the legal person - this could include the CEO, non-executive Directors; independent non-executive Directors, Director or Manager; and

- ❖ Take reasonable steps to verify the identity of the beneficial owner so that the Company is satisfied that it knows who the beneficial owner is.

(*The FIC Act defines a "beneficial owner" in respect of a legal person as the natural person who, independently or together with another person, owns the legal person or exercises effective control of the legal person).

Elimination process to establish the beneficial owner of a legal person:

Step 1: Who is the main shareholder/voter?

- The percentage of shareholding with voting rights = good indicator
- Ownership of 25% or more of shares/voting rights = good indicator

Step 2: Who is natural person who exercises control through other means?

- e.g. through voting rights attaching to classes of shares or through shareholder

Step 3: If no natural person can be identified - management

- Determine who = natural person who exercises control over the management of the legal person (this could include the CEO, non-executive Directors; independent non-executive Directors, Director or Manager).

These provisions apply whether the legal person is incorporated in South Africa or not.

d) Additional measures relating to trusts (Section 21B)

The Company must establish:

- The nature of the client's business;
- The ownership and control structure of the client;
- If a natural person is acting on behalf of a trust in terms of a trust agreement, the Company must:

❖ Establish the identifying name and number of the trust (if applicable);

❖ Establish the address of the Master of the High Court where the trust is registered (if applicable);

❖ Establish the identity of the founder;

❖ Establish the identity of each trustee and any natural person claiming to be authorised to enter into a single transaction or business relationship with the Company on behalf of the trust;

- ❖ Establish the identity of each beneficiary referred to by name in the trust deed or founding document; or

- ❖ If no beneficiaries are named, the particulars of how the beneficiaries of the trust are determined;

- ❖ Take reasonable steps to verify the particulars mentioned above; and

- ❖ Take reasonable steps to verify the identity of these natural persons so that the Company is satisfied that it knows the identities of the natural persons concerned.

These provisions apply whether the trust is incorporated in South Africa or not.

Doubts about the veracity of previously obtained information (Section 21D)

In the case where the Company, after entering into a single transaction / establishing a business relationship, doubts the veracity of adequacy of the previously obtained information, in other words, where the documents submitted as part of the identification process do not correspond with the verification documents, or there are inconsistencies with the original copies of the documents, the Company must redo the CDD processes (as outlined above) to confirm the information.

> ***EXAMPLE:***
>
> The business relationship is underway. Whilst preparing a client's application, a support staff member sees that the client's date of birth does not match his ID number. The support staff member now doubts the authenticity of the existing information originally provided by the client to the broker.

Unusually Large Transactions, Unusual Patters and/or No apparent business purpose (Section 42(2)(h))

In terms of Section 42(2)(h), where the Company in its customer due diligence and ongoing monitoring of the business relationship and/or single transactions concluded with clients, the company, at any time, deems any transaction unusually large, presents an irregular pattern and/or of no apparent business purpose, the Company will continue to follow the adopted processes in terms of this RMCP, however, the further processes listed below will be conducted:

- Irrespective of the client's risk rating, should a transaction be deemed unusually large, present unusual or irregular patterns and/or of no apparent purpose, the client will automatically be graded as a high-risk client, irrespective of the outcome of the risk rating of such client;

- At such point of identification of such transaction in terms of Section 42(2)(h), the EDD process will be conducted on the client, to verify the legitimacy of the transaction, the nature of the transaction and the risks such transactions may pose.

- Management of the Company will sign off each such transaction and approve the furtherance of the business relationship and/or single transaction established or to be established, upon receipt of the outcome of the EDD process conducted in terms of the RMCP.

- All accepted and active clients identified as conducting transactions in terms of Section 42(2)(h), shall require ongoing monitoring as to the purpose of the transaction and the nature of any further such transactions during the existence of the business relationship with the client, and until such high risk client is re- risk rated on a yearly basis

- Should such client monitoring present further and regular transacting in terms of Section 42(2)(h) transactions during such monitoring period and until such further risk rating take place, the Money Laundering Officer shall conduct further investigation into such client's business relationship established.

- Pending the outcome of such further investigations, the management of the Company will make a decision whether to proceed with the business relationship conducted with the client and shall proceed to ensure the necessary reporting is followed where required.

For purposes of this RMCP, an unusually large transaction shall be defined as any single transaction or transaction concluded in the course of the business relationship with the client, where the ongoing premium of the client amounts to more then R30 000p.m, a single investment contribution amounting to more then R2 000 000 or where more then R500 000 ad hoc contributions have been made to an investment in the past 3 months, excluding any approved transfers from a pension product to another pension product as defined in terms of the Pensions Fund Act

Unusual patters and/or no apparent business purpose may include, but is not be limited to, regular changes (more then 3 times) within a period of 12 months of beneficiary nominations on policies, regular changes(more then 3 times) within a period of 12 months to banking details of client, regular cancellation and/or re-issuing of policies within a period of 12 months for no apparent reason, regular issuing and /or requests for further policies not in accordance with the regular business relationship and purpose of such business relationship.

Inability to conduct a Customer Due Diligence (Section 21E)

If the Company is unable to:

- Establish and verify the identity of a client or other relevant person OR
- Obtain the required information in terms of Section 21 of FIC Act OR
- Conduct ODD in terms of Section 21C;
- The Company:

❖ May NOT establish a business relationship or conclude a single transaction with the 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 the client.

So, in any of the above circumstances, the employee must escalate the problem to the MLO for a decision on:

- whether the required information is indeed if not available, and/or
- whether the Company is not able to conduct appropriate CDD / ODD as the case may be, and/or
- how an existing business relationship will be terminated if the CDD requirements cannot be completed, and/or
- whether to report this as suspicious in terms of Section 29 of FIC Act, to the FIC.

If during the CDD stage, notwithstanding the insufficiency of the received verification documents, it is determined that the client is:

- high risk, then it is recommended that the client be given no further time in which to submit the requested verification documentation;

- medium risk, then it is recommended that the client be given an additional 7 calendar days in which to submit the requested verification documentation;

- low risk, then it is recommended that the client be given an additional 14 calendar days in which to submit the requested verification documentation.

If the Company is still unable to finalize the CDD process, it is recommended that the procedure detailed under "Enhanced Due Diligence" (below) be followed, commencing with the submission of all the information which was obtained on the client to the MLO in order to conduct an EDD. Ultimately, the Company's Principal/ Senior Managment and/or Key Individual will determine whether to proceed with the tranaction in question.

Enhanced Due Diligence (EDD)

The level of CDD will depend on the risk ratings that the Company has set in place (see the risk matrix below).

Enhanced Due Diligences **(EDD)** are conducted on clients deemed to be high risk. For example, in the case of every Politically Exposed Person **(PEP)**, an EDD must be conducted. This means that the range, degree, frequency or intensity of preventative measures and controls conducted will be more stringent or tougher in higher risk scenarios.

This entails the following:

- For each new business relationship / single transaction, FICA documents must be obtained at pre-approval stage and correcteness and validity of such documents at servicing servicing stage to ascertain the identity of the client that we are dealing with (see ***Annexure A***).

- When a PEP, family member or associate of the PEP, has been discovered during the CDD stage, the information regarding the PEP is to be sent to the MLO in order to conduct an EDD.

- The MLO to conduct the following additional checks:

  - Desktop research using the internet in the form of social media searches and any other available media sources;
  - Use of the Company's internal systems to determine if the Company has any additional information on the PEP;
  - ITC and Government Department websites.

- The MLO should then perform a risk assessment on the PEP, taking into account the following factors:

  - Customer risk factors;
  - Kind of facility;
  - Nature of prominent public function that the PEP has – in other words, what is the level of the PEP's involvement (is he/she the decision maker), the PEP's access to or control over public funds, the history / profile of the PEP (taking into account any adverse media reports or criminal records) and the nature of his/her position held.

- If the MLO finds that the above establishes the PEP as high risk, continuous monitoring of that PEP will have to implemented.

- The MLO will then complete a report to be submitted to the Company's principal/ Senior Management and/or Key Individuals with all relevant known information regarding the PEP.

Foreign prominent public official (Section 21F)

The definition of a foreign prominent public official incudes a person who holds the relevant position or has held the position in a foreign country for a period of at least 12 months after the date on which that person ceased to hold that position.

Schedule 3B to the FIC Act contains a list of positions that will be considered foreign prominent public officials which includes:

- 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.

If the Company determines that a prospective client, or the beneficial owner of that prospective client is a foreign prominent public official, the Company must:

❖ Obtain senior management approval before establishing the business relationship;

❖ 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.

To establish the source of wealth, the Company should look at the activities that have generated the total net worth of the client (i.e. the activities that produced the client's funds) in as far as possible.

To establish the source of funds, the Company should consider the origin and means of transfer for funds that are involved in the transaction (e.g. occupation, business activities, proceeds of sale and corporate dividends) in as far as possible.

Domestic prominent influential person (Section 21G)

A person is considered to be a domestic prominent influential person if he/she holds the position for a period exceeding 6 months or has held the position at any time in the preceding 12 months.

Schedule 3A to the FIC Act contains a list of positions that will be considered domestic prominent influential persons which includes:

- President or Deputy President: https://www.gov.za/
- Government minister or deputy minister: https://www.gov.za/
- Premier of a province: http://www.gov.za/links/provincial-government
- Member of the Executive Council of a province: http://www.gov.za/links/provincial-government
- Executive mayor of a municipality elected in terms of the Local Government Municipal Structures Act, 1998 http://www.salga.org.za/Municipalities%20MCD.html
- Leader of a political party registered in terms of the Electoral Commission Act, 1996 http://www.elections.org.za/content/Parties/Political-party-list/

  (Note: The leader of a political party is the person identified by the party to occupy the position of the highest level of authority in the party)

- Member of the royal family or senior traditional leader as defined in the Traditional Leadership and Governance Framework Act, 2003 http://www.cogta.gov.za/?p=938

  (Note: The description of a "senior" traditional leader, therefore, applies to such traditional leaders who exercise authority over a number of headmen or headwomen in accordance with customary law, or within whose area of jurisdiction a number of headmen or headwomen exercise authority)

- 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: https://www.gcis.gov.za/
- 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, 1999: http://www.salga.org.za/Municipalities%20MCD.html
- 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: http://www.gcis.gov.za/content/resourcecentre/contactdirectory/government-structures-and-parastatals

- 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: http://www.govpage.co.za/municipal-entities.html

- Constitutional court judge or any other judge as defined in section 1 of the Judges' Remuneration and Conditions of Employment Act, 2001: https://www.judiciary.org.za/

- Ambassador or high commissioner or other senior representative of a foreign government based in the Republic of South Africa: http://www.dirco.gov.za/foreign/forrep/index.htm

- Officer of the South African National Defence Force above the rank of major-general http://www.dod.mil.za/leaders/leaders.htm

  (Note: This will include persons holding the position of General and Lieutenant General in the South African National Defence Force)

- The position of—
  - Chairperson of the board of directors; Chairperson of the audit committee; Executive officer; or
  - Chief financial officer 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 of Finance by notice in the Gazette.

  (Note: It is envisaged that the Minister of Finance will delay the operational date of this paragraph in the legislation, given that information about persons who may fall in this category is not publicly available currently. The National Treasury will explore ways to make such information readily available to enable easier compliance by accountable institutions)

- Position of head, or another executive directly accountable to that head, of an international organisation based in South Africa http://www.dirco.gov.za/foreign/forrep/intorg.htm

The links to websites above are merely to assist the Company to obtain further information relating to a particular group of prominent persons.

The client remains the most valuable source of information in order to determine whether he/she occupies a prominent position. The Company may augment the information obtained from its client by making use of commercially available information sources which specialise in providing information on PEPs if there is a need to conduct more thorough checks.

If the Company determines that a prospective client or the beneficial owner of that prospective client is a domestic prominent influential person, and that the business relationship entails higher risk as a result of this fact, the Company must:

- Obtain senior management approval before establishing the business relationship;
- 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.

Family members and close known associates (section 21H)

Sections 21F and 21G (as discussed above) apply to immediate family members and close known associates of a person in a foreign or domestic prominent position.

An immediate family member includes:

- The spouse, civil partner or life partner;
- The previous spouse, civil partner or life partner, if applicable;
- Children and step children and their spouse, civil partner or life partner;
- Parents; and
- Siblings, step siblings and their spouse, civil partner or life partner.

Close associates include:

- Known sexual partners (girlfriends, boyfriends, mistresses etc);
- Prominent members of the same political party, civil organization, Labour or employee union;
- Business partners or associates;
- An individual who has sole beneficial ownership of a legal entity set up for the actual benefit of the prominent person.

In each of the above cases, the Company need only have regard to the information within its possession, or to credible information which is publicly known.

Ongoing Due Diligence (ODD) (Section 21C)

Ongoing due diligence **(ODD)** measures follow on from the obligation to understand the purpose and intended nature of the business relationship.

- Scrutiny of all transactions during the business relationship:
  - ❖ Are the transactions consistent with the Company's knowledge of the client?
  - ❖ Are the transactions consistent with the client's business and risk profile?
  - ❖ The source of funds may need to be verified
  - ❖ Is the client information on the Company's system still accurate and relevant?

- Pay particular attention to complex or unusually large transactions, and all unusual transaction patterns which have no apparent business or lawful purpose.

Duration of ODD:

- **High risk client conduct ODD annually**
- **Medium risk client conduct ODD every two years**
- **Low risk client conduct ODD every three years.**

Keep track of potential change in risk status:

- Advise clients, before entering into a single transaction / establishing a business relationship, that should any factor that is investigated during the Company's CDD process, associated with its business, change during the period of such single transaction / business relationship, the client is obliged to bring such change to the Company's immediate attention.

- This will assist the Company to keep record of any change in the client's risk status, enabling the Company to perform a revised CDD at such time. Existing clients must also be made aware of this obligation.

- Examples of factors which would influence the client's risk status would include, but are not limited to, a change in the client's shareholding, beneficial ownership, nature of business, an unlisted company becoming a listed company (and vice versa), change in directorship etc.

Risk Matrix :

Client / beneficial owner of client	0k <R50k investment amount / transaction	R50-150k investment amount / transaction	R150-300k investment amount / transaction	>R300k investment amount / transaction
SA citizen	10	20	30	40
SA listed company	10	10	20	20
Wholly owned subsidiary of SA listed company	10	10	20	20
SA (Pty) Ltd's & CC's	10	20	30	30
SA PEP (incl domestic prominent influential persons; Schedule 3A to Amendment Act)	60	60	60	60
SA trust, partnership & other	20	30	40	50
Foreign national (incl foreign prominent public officials; Schedule 3B to Amendment Act): *A country	20	30	40	50
Foreign listed company: *A country	20	30	30	40
Foreign national (incl foreign prominent public officials; Schedule 3B to Amendment Act): *B country	30	30	40	50
Foreign listed company: *B country	20	30	30	30
Foreign company: *A country	20	30	40	40
Foreign company: *B country	30	30	40	50
Foreign trust, partnership & other	50	50	50	50
Foreign national (incl foreign prominent public officials (Schedule 3B to Amendment Act): *C country	50	50	50	50

Additional weighting based on client attributes:

Client on the TFS or UNSC List	+50
< 1 year relationship	+20
1 – 5 year relationship	+15
Intermediary acting on behalf of client	+30

Additional weighting based on source of funds:

Dealer in high value goods	+30
Import / export	+30
High cash generating	+30

Additional weighting based on client conduct:

Unusual concern for secrecy	+40
Refuses / fails to indicate / vague as to source of funds / nature of business	+40

Country classification:

*A: Members of the Financial Action Task Force **(FATF)**, *except USA and UK*

*B: FATF Associate Members (members of the 9 Regional Bodies which use the FATF's 40 Recommendations as their principle guidelines for the implementation of effective AML/CFT standards and measures) *+ USA and UK*

*C: High-risk and Non-Cooperative Countries and Territories **(NCCT)** listed

***A Countries: Members of FATF**

The FATF (Financial Action Task Force) currently comprises 38-member jurisdictions. Please note that this list may change over time. For further information, please regularly visit the website for an update on these members, see: http://www.fatf-gafi.org/about/membersandobservers/

Argentina	France	Japan	Russian Federation
Australia	Germany	Republic of Korea	Singapore
Austria	Greece	Luxembourg	South Africa

Belgium	Hong Kong, China	Malaysia	Spain
Brazil	Gulf Co-operation Council	Mexico	Sweden
Canada	Iceland	Netherlands, Kingdom of	Switzerland
China	India	New Zealand	Turkey
Denmark	Ireland	Norway	*United Kingdom (but to be classified under B Country)*
European Commission	Isreal	Portugal	*United States (but to be classified under B Country)*
Finland	Italy		

***B Countries: FATF Associate Members** (members of the 9 regional bodies which use the FATF's 40 Recommendations as their principle guidelines for the implementation of effective AML/CFT standards and measures). Please note that this list may change over time. For further information, please see**:** http://www.fatf-gafi.org/countries/

See Appendix 4 – FATF Members, Associate Members and Observers, for a list of the countries comprising each of the 9 regional bodies, as taken from the FATF Annual Report 2015 - 2016.

The 9 regional bodies are as follows:

- Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)
- Eurasian Group (EAG)
- Eastern & Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Central Africa Anti-Money Laundering Group (GABAC)
- Latin America Anti-Money Laundering Group (GAFILAT)
- West Africa Money Laundering Group (GIABA)
- Middle East and North Africa Financial Action Task Force (MENAFATF)
- Council of Europe Anti-Money Laundering Group (MONEYVAL).

***C Countries: High-risk and Non-Cooperative Countries and Territories**.

Please note that this list may change over time. For further information and to view changes, please constantly see**:** http://www.fatf-gafi.org/countries/#high-risk

Bosnia and Herzegovina	Iran	Uganda
Democratic people's Republic of Korea (DPRK)	Iraq	Vanuatu
Ethiopia	Syria	Yemen

Risk Classification:

1 – 50: Low

51 – 69: Medium

70 & higher: High

Annexure C

Indicators / Guidelines of Suspicious and Unusual transactions/activities:

- The client makes deposits of funds with a request for their immediate transfer elsewhere;
- Unwarranted and unexplained international transfers;
- The payment of commission or fees that appear excessive in relation to those normally payable;
- Lack of concern about high commissions, fees, penalties etc. incurred as a result of a particular type or method of transaction;
- Transactions do not appear to be in keeping with normal industry practices;
- Purchase of commodities at prices significantly above or below market prices;
- Unnecessarily complex transactions;
- Unwarranted involvement of structures such as trusts and corporate vehicles in transactions;
- A transaction seems to be unusually large or otherwise inconsistent with the customer's financial standing or usual pattern of activities;
- Buying or selling securities with no apparent concern for making profit or avoiding loss;
- Unwarranted desire to involve entities in foreign jurisdictions in transactions;
- A client attempts to convince employee not to complete any documentation required for the transaction;
- A client makes inquiries that would indicate a desire to avoid reporting;
- A client has unusual knowledge of the law in relation to suspicious transaction reporting;
- A client seems very conversant with money laundering or terrorist activity financing issues;
- A client is quick to volunteer that funds are clean or not being laundered.

Indicators in terms of Client Identification:

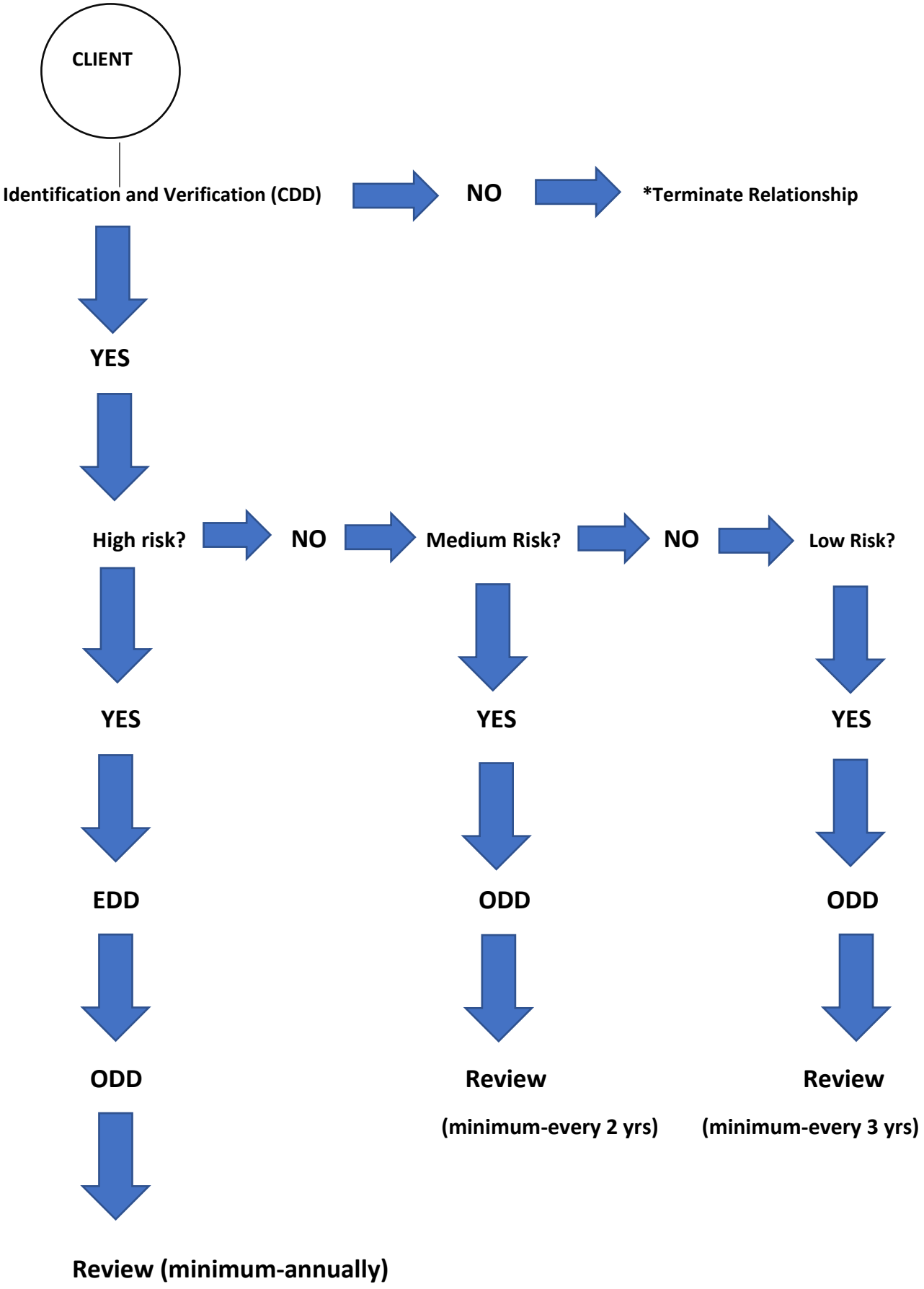
- The use of seemingly false identity in connection with any transaction, including the use of aliases and a variety of similar but different addresses and, in particular, the opening or operating of a false name account;
- Opening accounts using false of fictitious documents;
- A client provides doubtful or vague identification information;
- A client refuses to produce personal identification documents;
- A client changes a transaction after learning that he must provide a form of identification;
- A client only submits copies of personal identification documents;
- A client wants to establish identity using something other than his or her personal identification documents;
- A client's supporting documentation lacks important details such as contact particulars;
- Client does not want correspondence sent to his/her home address.
- A client inordinately delays presenting corporate documents; or

- All identification presented by the client is foreign or cannot be checked for some reason.

General Indicators of Suspicious Behaviour:

- A client provides insufficient, vague or suspicious information concerning a transaction;
- Accounts that show unexpectedly large cash deposits and immediate withdrawals;
- Frequent changing of bank accounts;
- A frequent exchange of small denomination notes for large denomination notes;
- Client appears to have accounts with several financial institutions without no apparent reason;
- Involvement of significant amounts of cash in circumstances that's difficult to explain.

Flow chart



*The Company is responsible for all compliance and, therefore, for non-compliance with the CDD, EDD and ODD principles. Where full CDD has not been or has only partially been attended to (eg. Company able to obtain some but not all required verification documents), it is incumbent upon the Company to nevertheless attend to / complete and finalize the CDD process if it does not wish to terminate the relationship with the client.

Appendix 1
Internal Suspicious Transactions Report

Appendix 2
Evaluation Record for Suspicious/Unusual Transactions

Appendix 3
Suspicious Transactions Report Register