



SIYAVIKA

risk solutions

An Authorised Financial Services Provider
FSP 44999

FICA

Risk and Compliance

Management Framework Programme

**In terms of Section 42 of the Financial Intelligence Centre
Act, No 38 of 2001**

Table of Contents

1. Overview	2
a. Document History	
b. Operational Approvals	
c. Governance Approvals	
2. Definitions	3
3. Siyavika Risk Solutions Background, Responsibilities and Obligations	4
4. Risk Indicators	5
5. Risk Rating (Matrix)	8
6. Risk Mitigation	9
7. Customers Due Diligence measures	10
8. Record Keeping	15
9. Risk Management & Compliance Programme	16
10. Declaration by Staff Members	19

1. Overview

1.1 Document History

Revision Date	Document Version	Summary of Changes	Author/Reviewer
30 October 2018	1	Initial drafting	Alet de Kock Tanya Jurriaanse (compliance)
11 March 2019	2	Amendments to align with new requirements	Alet de Kock / Tanya Jurriaanse
26 March 2019	3	Last revision of changes	Alet de Kock / Germa Beukes




1.2 Operational Approvals

This document has obtained the following approvals:

Name	Nature	Document Version	Approval Signature	Date of Approval
Admin Manager & Compliance Officer	Approval and Recommendation	1	Refer to Minutes	5 Nov 2018
Admin Manager Actuarial (Legal)	Approval and Recommendation	2	Refer to Minutes	13 March 2018
Admin & Operations Manager Compliance officer	Approval and Recommendation	3	Refer to on-site visit by Compliance Officer	26 March 2019

1.3 Governance Approvals

This document has obtained the following approvals:

Name	Nature	Document Version	Approval Signature	Date of Approval	Signature
Risk & Compliance Officer	Approval and Recommendation	2	Refer to Board Meeting	26 March 2019	
Board of Director: HCW RIX	Approval	3	Board meeting:	29 March 2019	
B ROBERTS					

1.4 Review process

The Risk & Compliance Officer are responsible for reviewing all aspects on a yearly basis to keep in line with the legislation or when legislation undergoes a drastic change. Board of Trustees and staff must always be kept informed of any changes .

2. DEFINITIONS

FICA

“	AML: anti-money laundering
	ML: money laundering
	CFT: combating the financing of terrorism
	TF: terrorist financing
	CRMP: Compliance and Risk Management Program that forms the basis of combating money laundering and terrorist financing.
	KYC: know your client (client identification & verification – requirement under 2002 Act and replaced by CDD)
	CDD: customer due diligence customer due diligence is aimed at understanding customers and not merely verifying identities (broader KYC approach)
	Beneficial ownership: requires knowledge of and understanding who ultimately controls corporations (the natural persons that benefit from ownership or actual control of a business)
	UN prohibition List: List of persons and organisations involved in terrorism and terrorist financing, such as Al Queda, ISIS, ISIL, etc.
	PEPs: Politically exposed persons (concept under 2002 Act and replaced by Domestic/Foreign Persons of Influence)
	DPIs: Prominent domestic (local) persons that has significant influence, such as politicians, high-ranking military officers, municipal managers, etc.
	FPIs: Foreign nationals of significant influence such as high-ranking diplomats, military attaché's, etc.
	POPI: The Protection of Personal Information Act of 2013 that regulates the collection and processing of personal data of, amongst others, clients or data subjects.
SOE: State-owned enterprises [Telkom, Eskom, Sasol, etc.]	
EME: Exempted micro enterprise [for B-BBEE purposes < R10 million turnover]	
NGO: Non-government organisation [activist groups, etc.]	
NPO: Non-profit organisation [charities, churches, etc.]	

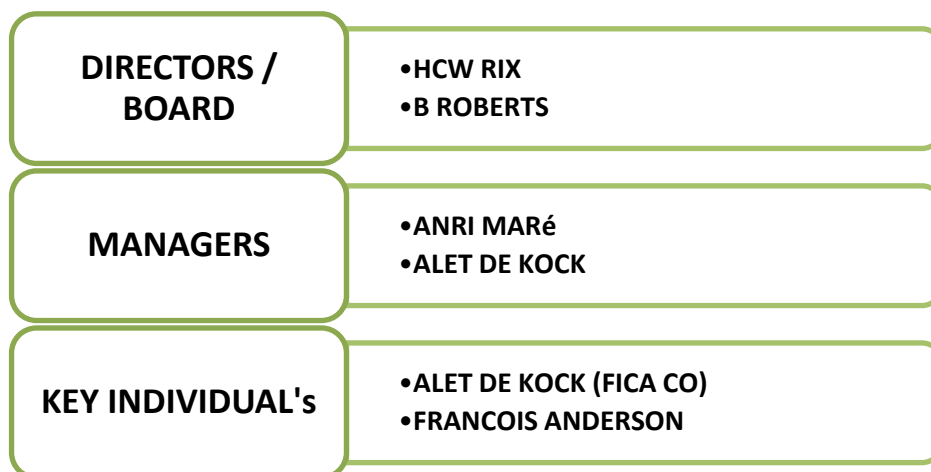
OTHER

“EFT”	means Electronic Fund Transfers.
“FICA”	means the Financial Intelligence Centre Act, Number 38 of 2001, as amended from time to time.
“FIC”	means the Financial Intelligence Centre, a juristic person created under chapter 2 of FICA.
“INSURER”	means the Insurer, GUARDRISK LIFE who offer its clients custom designed cover and is registered in South Africa for all statutory classes of non-life and life insurance.
“RMCP”	means the Risk Management and Compliance Programme contained in this document, which has been designed in response to section 42 of FICA.
“SERVICES PROVIDERS”	means providers of non-risk benefits.
“SIYAVIKA”	means Siyavika Risk Solutions (Pty) Ltd an Authorised Financial Services Provider and FICA registered.

3. SIYAVIKA RISK SOLUTIONS BACKGROUND, RESPONSIBILITIES AND OBLIGATIONS TO ELIMINATE MONEY LAUNDERING(ML) AND TERRORIST FINANCING(TF).

- a. Siyavika is a Cell Captive of GUARDRISK LIFE and an Underwriting Manager for GUARDRISK LIFE and other Services Providers.
- b. Siyavika is an accountable institution and subject to the provisions of FICA.
- c. As per Section 21A of the FIC Act requires Siyavika Risk Solutions to ascertain the nature intended purpose of the business relationship of current and prospective clients. Acceptance of a business relationship is subject to complete Due Diligence checks and approval by Siyavika and the Insurer, Guardrisk Life.
- d. Siyavika offers life insurance products under the Cell Captive with Guardrisk Life and value-added benefits for other Services Providers to our target market. We specialize in packaging thereof according to the need and affordability of the entity members.
- e. Our clients, the approved and authorised Broker (FSP) serves as the intermediary that may sell authorized products on a group basis.
- f. The premiums received for these products are received directly in the Insurer's or Siyavika's premium bank account.
- g. Siyavika's main objective is managing "Client's the Broker" Groups contribution on Group level. The Client/Broker is not allowed to be involved in any premium or contribution transactions.
- h. Therefore, the likelihood of Siyavika being used for money laundering and or terrorist financing activities is low.
 - a. No cash transactions are applicable and allowed.
 - b. All payments made on a monthly must be in Siyavika or Guardrisk's bank account.
 - c. Siyavika's business relationship is based on a monthly group level contribution and not on a single transaction.
 - d. Any unknown amount receive over R24 999 must be investigated and reported.
- i. The purpose of the RMCP is to identify and assess the risk to Siyavika Risk Solutions of policy owners seeking to launder money or to finance terrorism.
- j. Siyavika is obliged to be on the lookout for such illegal practices and to report any instances of such activity or any other suspicious activities.
- k. Siyavika obligations are to monitor their clients with inception and annually.
- l. Siyavika obligations also extend to monitor, mitigate and manage the risk of its products and services being utilized for these illegal practices.
- m. Siyavika also obligated to control and monitor any possibility of Conflict of Interest.
- n. Siyavika intends to comply with these obligations, and other related matters.

The following management is responsible for FICA monitoring powers & decision-making



4. RISK INDICATORS

4.1 PRODUCTS APPROVED AND SERVICES

- Siyavika only handles products approved under our FSP license which are Insured under Risk Policies.
- All risk products are market related and must go through Pricing Management Committee at Guardrisk Life, the Insurer.
- Value added benefits / products and Services with other Services Providers are subject to quote application and approval.

4.2 WHO ARE OUR CLIENTS?

- Siyavika's nature of business is concentrated on groups and not on individual marketing.
- The marketing of products is done by selected BROKERS who are actual our "CLIENTS" according to products authorized for (check FSCA website).
- The Broker who must comply with the Due Diligence checks and necessary agreements are in place. (Refer to **ANNEXURE A**)
- Brokers is responsible for marketing on group level and must complete a quote application (**ANNEXURE D**) to indicate products and services required.
- Group/Entity approval is subject to completion of a Siyavika standard quote application, followed by a formal quotation from Siyavika .
- Acceptance of quote must be signed by group owner / entity.
- Siyavika have a process in place to identify and evaluate the group business nature per background and dignity, OR
- If the client has previously observed suspicious or unusual activities or transactions.

Summary of Siyavika Clients who act as Brokers on behalf of GUARDRISK, Siyavika Risk Solutions and other Services Providers.

Entity	FSP number	Business relation	Registration Number	Agreements
Leap Brokers Intl (Pty) Ltd- (Vuka Risk Solutions)	29091	Broker	2006/029537/07	Intermediary - GUARDRISK Service Level Agreement with Siyavika
Maxi Employee Consultant	24377	Broker	2005/009591/07	Intermediary – GUARDRISK Service Level Agreement with Siyavika
Spectre Wealth (Pty) Ltd	40845	Broker	2006/001122/07	Intermediary – GUARDRISK Service Level Agreement with Siyavika
Multinet Life (Pty) Ltd	11091	Broker	1995/009982/07	Intermediary – GUARDRISK Service Level Agreement with Siyavika
Umcebo Financial Services (Pty) Ltd	28698	Broker	2005/026332/07	Intermediary – GUARDRISK Service Level Agreement with Siyavika
Central Lake Trading 377 (Pty) Ltd	45517	Broker	2008/025860/07	Intermediary – GUARDRISK Intermediary(premium collection) – INSURER. Service Level Agreement with Siyavika
Conecting Points (Pty) Ltd	46130	Broker	2013/056978/07	Intermediary – GUARDRISK Service Level Agreement with Siyavika

- ML/TF is unlikely with above clients, because all current and prospective clients are verified by INSURER and Siyavika and must comply with all Due Diligence requirements.

4.2.1 Process to check dignity of clients on different levels

Level	FSP on FSCA website	ID of owner / responsible or policy holder	Residential address	Copy – COR.15	LR number	Copy – FICA registration	Verify info on internet
Broker	√	√	√	√		√	√
Intermediary	√	√	√	√		√	√
Company		√	√	√		√	√
Group Owner		√	√			√	√
Union		√	√		√	√	√
Individual / Beneficiary under GROUP		√ (w/a)	√	√		√	√

Note: Siyavika decides whether the group members' IDs are required upon entry, taking into account the background of the group. In example of FUND members like AGRICULTURE SECTOR FUND as a compulsory scheme it is impossible to obtain the farm workers' ID's and residential addresses with inception. ID's are verified before a claim is paid and part of assessment process.

** Intermediaries/companies/Unions are subject to an annual review.

4.3 Risk Indicator Objectives

1	Product Type (as explain above) and Services (as per quote application with relevant information required)
2	Business Activity / Associated delivery channels – only adopted on quotation and Due Diligence checks approved by INSURER and Siyavika = <i>low</i>
3	Type of Entity (Authorised FSP - low / Union – legal union with LR number - low / EB business through payroll - low)
4	Jurisdiction of Client (Local-low / Foreign - High) – refer to new client verification as High Risk (ANNEXURE C)
5	Source of Funds / Payment methods (client's/brokers cannot receive any money. Payments of contributions to Guardrik / Siyavika premium bank account - Low

1. PRODUCTS	LOW	MEDIUM	HIGH	EXPLANATION
Funeral Cover – Assistance Bus	x			Max cover R30 000 – Tariff per R1000
Accidental Death – Life	x	x		Cover amount is fixed – Tariff per R1000 – double payment with commuter coverage.
Accidental Disability – Life	x			Cover amount is fixed – Tariff per R1000
Death benefit – Life	x	x		Cover amount is fixed – Tariff per R1000. Members may have funeral and Death benefit.
Repatriation	x			Premium is paid for a service. Claims are approved as per Siyavika's database.
Assist Products: Legal / Tutor on line Trauma / Debt & Credit	x			Premium is paid for a service. . Claims are approved as per Siyavika's database.
Vouchers: Groceries / Airtime / Electricity	x			Premium is paid for a service. . Claims are approved as per Siyavika's database.

4.4 Delivery Channels

- The delivery channel refers to how institutions and clients interact with each other in the offering of products and services, on-boarding of clients and the usage of products and services.
- Clients/Brokers are selling the approved products in 4.1 on group base and are not allowed to receive any cash premiums.
- Payments are done directly to:

Compliance-Management-Framework of Siyavika

- Siyavika Premium Account (EFT)
- INSURER Life Account (Persal / Persol / Debit Orders)
- Due diligence checks must be signed off by INSURER & Siyavika before any new business can be concluded – refer to point 7.
- Training by Siyavika will apply when a new product is market and before business can be concluded
- Siyavika handles all 5 (five) binder functions.
- Marketing through call center is monitored by script (signed off by Insurer) and voice recordings linked to client’s profile. No internal call center functions within Siyavika.
- Marketing material must be approved and signed off by Siyavika/Insurer/Service Provider.
- Individual clients will be issued with inception the following documents named as WELCOME PACK:
 - Welcome letter
 - Policy schedule (includes the option taken, cover amounts and dependents)
 - Policy wording
 - FAIS disclosure
- Groups as FUND clients will be issued with a group certificate and copy of the Master Policy and products approved as an Addendum.

4.5 Indicators relating to geographic locations

- Siyavika is not allowed to deal directly with any client not situated in South Africa.
- All our clients are domiciled in South Africa but may operate in another country subject to approval by Insurer and Siyavika.
- Do clients who are domiciled outside of South Africa or operate outside South Africa engage with the institution in South Africa or through branches, subsidiaries or intermediaries outside South Africa? **N/A**
- Have credible sources identified geographic locations from where clients engage with an institution as high-risk jurisdictions? **N/A**
- Are the geographic locations from where clients engage with an institution subject to sanctions regimes? **NO**, because it’s subject to Due Diligence checks by Insurer and Siyavika.
- Has an international body, a domestic regulator or supervisory body or other credible source expressed concern with weak regulatory measures against money laundering and terrorist financing, weak transparency requirements for beneficial ownership of corporate structures or weak institutional frameworks such as supervisory, law enforcement and prosecuting agencies in relation to a geographic location from where clients engage with an institution? **NO**

5. RISK RATING (MATRIX)

5.1 General remarks

- Risk rating implies assigning different categories to different levels of risk according to a risk scale and classifying the ML/TF risks pertaining to different relationships or client engagements in

terms of the assigned categories

- An FSP offering a relatively homogenous range of products and services, using a limited range of delivery channels, operating in one or a few geographic location(s) or engaging with a homogenous range of clients require relatively simple risk scales distinguishing only between two or three risk categories. If the FSP’s offerings become more diverse in the range of products and services, using a wider range of delivery channels, operating in a larger number of geographic locations or engaging with a more diverse range of clients, it will require more finely calibrated risk scales distinguishing between a larger number of risk categories.

5.2 The role of a Risk Matrix

- The assessment of ML/TF risk ultimately draws together all the factors that are relevant to an engagement with a client by completion of a Risk Questionnaire **(ANNEXURE B)**.
- **Current Risk Matrix of Clients/Brokers**

Entity	FSP number	1	2	3	4	5
Leap Brokers Intl (Pty) Ltd- (Vuka Risk Solutions) - SA	29091	Low	Low	Low	Low	Low
Maxi Employee Consultants - SA	24377	Low/Med	Low	Low	Low	Low
Spectre Wealth (Pty) Ltd - SA	40845	Low/Med	Low	Low	Low	Low
Multinet Life (Pty) Ltd - SA	11091	Low	Low	Low	Low	Low
Umcebo Financial Services (Pty) Ltd - SA	28698	Low	Low	Low	Low	Low
Central Lake Trading 377 (Pty) Ltd - SA	45517	Low / Med	Low	Low	Low	Low
Conecting Points (Pty) Ltd	46130	Low	Low	Low	Low	Low

6. RISK MITIGATION

6.1 General introduction

- Risk mitigation in the context of ML/TF refers to the activities and methods used to control and minimise the ML/TF risks it has identified.
- Siyavika Risk Solutions has established and implemented systems and controls in response to the assessed risks. These controls are designed to detect money laundering and terrorist financing and respond appropriately when risks materialise.

6.2 Implementation of systems and controls for management of ML/TF risk

- Siyavika Risk Solutions 's systems and controls provide for more information to be obtained about clients, more secure confirmation of clients' information to be applied and closer scrutiny to be conducted to clients' transaction activities where the risk of abuse is assessed to be higher. This is referred to as enhanced due diligence.
- Simplified due diligence is applied where the assessed risk of abuse is determined to be lower.
- Mechanisms to manage risk include, but are not limited to:
 - Systems, policies and procedures – refer to;
 - Conflict of Interest policy
 - Complaint Management Policy and Procedures
 - Awareness training of staff;
 - Reporting channels (any transaction above the amount off R24 999);
 - Client analytics;
 - Process to exit from high risk relationships;
 - Approval procedures for higher risk transactions and relationships;
 - Adequate supervision over higher risk activities; and
 - Screening tools.

7. CUSTOMER DUE DILIGENCE MEASURES (REFER TO CLIENT/FSP DD - ANNEXURE A)

7.1 Introduction

- Customer due diligence (CDD) refers to the knowledge that Siyavika Risk Solutions has about its client and the institution's understanding of the business that the client is conducting with it.
- CDD measures, enable Siyavika to manage their relationships with clients and to better identify possible attempts by clients to exploit our products and services for illicit purposes. Applying CDD is essential in our framework to combat ML and TF effectively.
- This, combined with the obligation to apply a risk-based approach, gives Siyavika Risk Solutions greater discretion to determine the appropriate compliance steps to be taken in given instances. This means that Siyavika Risk Solutions has the flexibility to choose the type of information by means of which it will establish clients' identities and also the means of verification of clients' identities.

7.2 Establishing and verifying clients' identities

- A natural person's identity can be determined by reference to a number of attributes. At the basic level these attributes are the person full names, date of birth, and in most cases, a unique identifying number issued by a government source (e.g. in case of a SA citizen or resident, his/her identity number or, in case of other natural persons, a passport number or numbers contained asylum seeker or refugee permits, work permits etc.). It is expected that these basic attributes will always be used in accountable institutions' process to establish a natural person's identity.
- Siyavika Risk Solutions will, in the course of establishing a business relationship, establish and verify the identity of the client and,
- if applicable, the person representing the client as well as any other person on whose behalf the client is acting.

7.3 Impact of POPI on the identification and verification requirements of the FIC Act

- The processing of personal information of clients for the purposes of the FIC Act compliance may only be done within the confines of POPI.
- While the processing and further processing of personal information of a client for purposes of FIC Act requirements is allowed in terms of the POPI, Siyavika Risk Solutions will be cautious of verifying clients' identities using third party data sources which may have obtained personal information about a client without the client's consent or knowledge.
- This information can also be verified through Guardrisk, the Insurer scanning tool.

7.4 Obtaining information on the business relationship (How and when Siyavika obtain DD information)

- According Section 21A of the FIC Act, Siyavika Risk Solutions is obliged to ascertain from a prospective client what the nature and intended purpose of the business relationship will be on approval that relates to long-term relationship.
- By complying with this provision, Siyavika Risk Solutions will be able to form a view of the frequency and the nature of transactions that could be expected to be conducted in the normal course of the ensuing business relationship.
- The manner and type of information obtained in terms of section 21A of the Act is recorded in Siyavika Risk Solutions 's RMCP as per information that may be relevant include-
 - 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; and
 - The anticipated level and nature of the activity that is to be undertaken during the business relationship.
- The information which Siyavika Risk Solutions obtains from a prospective client will be sufficient for Siyavika Risk Solutions to understand the client's profile and to establish the business relationship.

7.5 Establishing the identity of legal persons, trusts and partnerships

- Siyavika do not have any clients that's been related to legal persons, trust and partnerships, but have special measures in place to identify such an entity.
- Siyavika must make sure that applicable steps are in line regard to all the requirements in respect of Section 21B and 21D as set out below.
- Section 21 of the FIC Act (the requirement to establish and verify a client's identity) also applies to clients who are not natural persons acting in their personal capacity. Clients of this nature are referred to as corporate vehicles and include legal, trust and partnerships. In addition to the obligation to establish and verify the identities of corporate vehicles section 21B of the FIC Act also require accountable institutions to apply additional due diligence measures namely to establish –
 - the nature of the client's business
 - the ownerships and control structure of the client; and
 - the beneficial ownership of clients, andto take reasonable steps to verify the identity of the beneficial owners. The requirements to establish and verify the identities of corporate vehicles and to apply the additional due diligence

measures are discussed separately in respect of legal persons, partnership and trusts or similar arrangements in the sections that's applicable to the identity.

- The requirements set out in section 21 and 21B of the FIC Act apply whether the legal person partnership or trust or similar arrangement between natural persons is incorporated or originated in South Africa or elsewhere.
- A **Legal person** is defined in the FIC Act as 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.
- 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.
- In addition, section 21B(2) of the FIC Act provides for a process of elimination which accountable institutions must follow to determine who the *beneficial ownership* of a legal person is:
 - The process starts with determining who the natural person is who, independently or together with another person, has a controlling ownership interest in the legal person. The percentage of shareholding with voting rights is a good indicator of control over a legal person as a shareholder with a significant percentage of shareholding, in most cases, exercises control. In this context ownership of 25 per cent or more of the shares with voting rights in a legal person is usually sufficient to exercise control of the legal person.
 - If the ownership interests do not indicate a beneficial owner, or if there is doubt as to whether the person with the controlling ownership interest is the beneficial owner, the accountable institution must establish who the natural person is who exercises control of the legal person through other means, for example, persons exercising control through voting rights attaching to different classes of shares or through shareholders agreements.
 - If no natural person can be identified who exercises control through other means, the accountable institution must determine who the natural person is who exercises control over the management of the legal person, including in the capacity of an executive officer, non-executive director, independent non-executive director, director or manager.
- **Partnership** are not incorporated entities and do not have legal personality. However, accountable institutions must establish the identities of partnerships who are their client's, nonetheless. This means that the starting point to the identification of a partnership is to determine how the partnership is generally known.
- Accountable institutions must therefore establish whether a partnership is identified by a unique name or description. In addition to establishing this information, accountable institutions must take reasonable steps to verify it. This means that accountable institutions must apply measures that are commensurate with the assessed ML/TF risk relating to a partnership in a given case.
- The concept of a beneficial owner in the context of a partnership encompasses all the partners in the partnership. Hence, section 21B(3) of the FIC Act requires accountable institutions, over and above the requirements of sections 21 and 21A of the FIC Act, to establish the identity of every
- partner in a partnership. This includes every member of a partnership (a partnership where the

liability of certain partners who contribute a fixed amount and who remain undisclosed as partners are limited according to the partnership agreement establishing and governing the partnership), an anonymous partnership (a partnership where the partners' names are not disclosed to persons who are not partners in the partnership) or any similar partnership.

- The express references to partnerships and anonymous partnerships indicates clearly the intention that accountable institutions must establish the identity of every person who contributes to a partnership or may benefit from a partnership when they do business with a partnership. The most reliable source document indicating who the members of the partnership are is the partnership agreement which establishes the partnership and governs its membership and functioning.
- Section 21B(3) of the FIC Act also requires accountable institutions to establish the identity of the person who exercises executive control over the partnership, if there is such a person, indicating that accountable institutions should determine the notion of control over (in addition to benefit from) a partnership. Moreover, the provision requires accountable institutions to establish the identity of each natural person who is authorized to enter into a single transaction or establish a business relationship with the accountable institution on behalf of a partnership.
- Accountable institutions are required to take reasonable steps to verify the names of the natural persons covered by section 21B(3) FIC Act. The remarks made above about the verification of a natural person's identity also apply in this instance.

- **Trusts** are also not incorporated entities and do not have legal personality. All trusts in South Africa are "express trusts" – either trusts *inter vivos* (trusts created during the lifetime of a person) or *mortis causa* trusts (trusts created in terms of the will of a person and comes into effect after their death). The administration of trusts in South Africa is regulated by the Trust Property Control Act, 1988.
- The FIC Act defines a 'trust' as any trust as contemplated in the Trust Property Control Act, 1988 but excludes trusts 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.
- The identification and verification requirements set out in section 21B(4) of the FIC Act apply in respect of a trust which is *inter vivos*. The existence of a trust must be registered at an office of the Master of the High Court before legal effect can be given to the trust and the trustee(s) can obtain authority from the Master of the High Court to perform their functions. Therefore, accountable institutions must establish the unique reference number identifying the trust in the Master's Office and the address of the Master of the High Court where the trust is registered as part of the elements describing the identity of the trust.
- In respect of foreign trusts, accountable institutions should obtain a letter of authority or other official document from a competent trust registering authority in a foreign jurisdiction.
- The concept of a **beneficial owner** in the context of a trust encompasses all the natural persons who may benefit from a trust arrangement or may control decisions in relation to the

management of trust property or are otherwise associated with the trust. Hence, section 21B(4) of the FIC Act requires accountable institutions, over and above the requirements of sections 21 and 21A of the FIC Act, to establish:

- The identity of the founder;
- The identities of each trustee and each natural person who purports to be authorised to enter into a single transaction or establish a business relationship with the accountable institution on behalf of the trust, and
- The identities of each beneficiary referred to by name in the trust deed or other founding instrument in terms of which the trust is created; or
- If beneficiaries are not referred to by name in the trust deed or other founding instrument in terms of which the trust is created, the particulars of how the beneficiaries of the trust are determined.

7.6 Ongoing due diligence (Step to verify background of FSP/entities on an ongoing base)

- Siyavika Risk Solutions will in respect of Section 21C of the Act make provision for ongoing due diligence measures. These measures follow on from the obligation to understand the purpose and intended nature of a business relationship.
- They include the scrutiny of transactions undertaken throughout the course of a relationship, to ensure that the transactions being conducted of a business relationship are consistent with Siyavika Risk Solutions 's knowledge of the client,
- and the client's business and risk profile, including, where necessary, the source of funds.
- Siyavika Risk Solutions will ensure that the information about a client is, and at all times remain, accurate and relevant and will be verified on an annual base.
- The intensity and frequency of ongoing due diligence in respect of a given business relationship must be determined based on Siyavika Risk Solutions 's understanding of ML/TF risks associated with that relationship.

7.7 Doubts about veracity of previous obtained information

- Section 21D FIC Act provides for measures that accountable institutions are required to take if doubts about the veracity or adequacy of previously obtained customer due diligence information arise later on in the relationship, or where a suspicion of money laundering or terrorism financing is formed at a later stage.
- An accountable institution is required to repeat the steps set out in sections 21 and 21B of the FIC Act in accordance with its RMCP and to the extent that is necessary to confirm the information that is required to be verified.
- An accountable institution must provide, in its RMCP, for the manner in which and the processes by which the institution will confirm information relating to a client when it has doubts about the veracity of previously obtained information.

7.8 Inability to conduct due diligence

- With reference to Section 21E of the FIC Act, is Siyavika Risk Solutions not authorised from

entering or maintaining business relationships if the required CDD cannot be performed in accordance with the provisions of the Act (such as with anonymous clients or clients with fictitious names).

7.9 Foreign prominent public officials and domestic prominent influential persons

- Sections 21F, 21G and 21H of the FIC Act refer to deal with persons in prominent positions.
- Siyavika Risk Solutions do not have any business related to Foreigners, prominent public officials and or domestic prominent influential persons.
- Siyavika Risk Solutions will consider future business relationships 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.
- Siyavika Risk Solutions will apply the same requirements as for foreign prominent public officials and will refer to Schedule 3A to the FIC Act that contains a list of positions that will be considered.
- Siyavika Risk Solutions must comply with the Due Diligence requirement of the Insurer and approval before any business can be taken on or concluded.
- Siyavika Risk Solutions will also 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. This procedure also applies to immediate family members and known close associates of such prominent public officials.
- When considering whether to approve a business relationship with a prominent person, senior management will base the decision on the level of ML/TF risk the company would be exposed to if it entered that business relationship and whether the risk can effectively be managed.
- When determining the source of wealth, Siyavika Risk Solutions will consider the activities that generated the total net worth of the client (that is, the activities that produced the client's funds and property).
- Siyavika Risk Solutions will therefore as far as reasonably practicable be alert to public information relating to possible changes in the status of the clients of the business AND conduct additional due diligence measures when dealing with legal persons, trusts and partnerships.

8. RECORD-KEEPING

8.1 Obligation to keep customer due diligence records

- Section 22 of the FIC Act provides for an obligation on Siyavika Risk Solutions to keep customer due diligence records.
- Due Diligence records are filed electronically and is subject to acceptance and signature of the Insurer.
- This means that Siyavika Risk Solutions will keep record of all information pertaining to a client obtained in the course of its processes to comply with sections 21 to 21H of the FIC Act.
- Such records will include copies of, or references to, information provided to or obtained by Siyavika Risk Solutions to verify the person's identity.

8.2 Obligation to keep transaction records

- Siyavika Risk Solutions will keep transaction records of single transactions and transactions concluded in the course of the business relationship with the client in terms of Section 22A of the FIC Act.
- This means that Siyavika Risk Solutions will keep records of every transaction which Siyavika Risk Solutions conducts with a client.
- Transaction records must be sufficiently detailed to enable the transaction to be reconstructed and include the amount, currency, date of transaction, parties to the transaction, the nature of the transaction, pertinent or relevant business correspondence and also the identifying particulars of all accounts and account files related to the transaction.
Example : Hard Copies / Electronic information / Voice recordings
- Security protection = Fire Walls / Fire Fox and Back-ups;
 - Daily
 - Weekly
 - Monthly (stored off-site)

8.3 Manner in which records must be kept

- Siyavika Risk Solutions 's standard procedures for the capture of information and the retention of records will apply to records maintained in terms of FICA. Records will be kept by way of storing original documents, photocopies of original documents, scanned versions of original documents or otherwise in computerized or electronic form.
- Siyavika Risk Solutions will attempt to reduce the volume and density of records by storing these on:
 - Internal networks;
 - Physical storage devices e.g. Hard drives, Metro filing and
 - Cloud storage.
- All computers and electronic devices are password protected and changed every month.
- Siyavika Risk Solutions will ensure that the following principles are met:
 - Free and easy access to the relevant records;
 - Records will be readily available to the FIC and the relevant supervisory body when required;
 - The records will be capable of being reproduced in a legible format; and
 - If the records are stored off-site the FIC and the relevant supervisory body will be provided with the details of the third party storing the records.
- Records include details that will assist in the identification of the records such as:
 - Reference numbers on documents or letters;
 - Relevant dates, such as issue or expiry; and
 - Details of the issuer or writer.
- Siyavika Risk Solutions information and documentation are tamperproof and there are safeguards in place to prevent unauthorised access to electronic information.

8.4 Period for which records must be kept

- Records in relation to establishment of a business relationship referred to in section 22 of the FIC Act must be kept for at least five years from the date on which the business relationship is terminated.
- Siyavika Risk Solutions will furthermore retain records which relate to ongoing investigations

until the relevant law enforcement agency has confirmed that the case was closed.

9. RISK MANAGEMENT AND COMPLIANCE PROGRAMME

9.1 Implementation of the this RMCP

- Section 42 of the FIC Act places an obligation on Siyavika Risk Solutions to develop, document, maintain and implement a RMCP.
- Siyavika Risk Solutions notes that the board of directors, senior management or the person with the highest level of authority is ultimately responsible for ensuring that it maintains an effective internal AML/CFT control structure through a RMCP.
- The board of directors, senior management and KI's created a culture of compliance within Siyavika Risk Solutions , ensuring that all policies, procedures and processes are designed to limit and control ML and TF risks and are fully consistent with the law. The board will ensure that staff adhere to all policies and procedures.
- The board and senior management are fully engaged in decision-making processes and take ownership of the risk-based measures adopted, as they will be held accountable if the content of the RMCP is found to be inadequate.
- Siyavika's board of directors and senior management and KI's accountability and the appointment of a person with an adequate seniority with experience to assist with ensuring compliance with the FIC Act , by implementing:
 - Appropriate training on money laundering and terrorist financing to ensure that employees are aware of, and understand, their legal and regulatory responsibilities and their role in handling criminal property and money laundering/terrorist financing risk management;
 - And to be connected to report properly on differences related to the finance of terrorist and related activities;
 - Appropriate provision of regular and timely information to the board of directors or senior management relevant to the management of Siyavika Risk Solutions 's ML and TF risks;
 - Appropriate documenting of Siyavika Risk Solutions 's risk management policies and risk profile in relation to ML and TF risks, including documentation of Siyavika Risk Solutions 's application of those policies;
 - Appropriate descriptions of decision-making processes in respect of the application of different categories of CDD and other risk management measures, including escalation of decision-making to higher levels of seniority in Siyavika Risk Solutions where necessary; and
 - Appropriate measures to ensure that money laundering risks are considered in the day-to-day operation of the institution, including in relation to:
 - The development of new products;
 - The taking-on of new clients; and
 - Changes in the business profile.
- Appropriate measures to ensure that the day-to-day operation functions of reconciliation process is followed;
 - Responsible personal of Siyavika reconcile a transaction on bank statement according to the bordereaux received from the entity(group);

- Verify premium payer according the approval documentation signed off by management
 - Verify the products & pricing approved
 - Verify the dignity of the client on the bordereaux if it is a new client
 - Report any unknown or suspicious transaction to senior management or Compliance Officer.
- Siyavika Risk Solutions 's RMCP will always be commensurate with the size and complexity of operations and the nature of its business.
 - The content of Siyavika Risk Solutions 's RMCP is communicated widely throughout the business and is electronical available on the companies share drive and also on the website.
 - Siyavika Risk Solutions will review its RMCP at regular intervals to ensure that it remains relevant to the effective operation of the company as well as the identified risks.

9.2 FICA TRAINING

- The FICA awareness training is aimed at employees of accountable institutions and covers basic money-laundering and terrorist financing concepts, anti-money-laundering legislation in South Africa, the risk-based approach, and looks at the requirements for customer due diligence, reporting of certain transactions and record-keeping requirements.
- The Compliance Officer is responsible to ensure that all members of the companies are constantly aware of the legislation and appropriate use in their own environments.
- The Compliance Officer will ensure that such training sessions are applied at least on an annual basis for all the employees and board of directors.
- Last FICA training register attached.

9.3 Reporting process in Siyavika Risk Solutions

- Siyavika Risk Solutions and all staff member are obligated to report any suspicious transaction and or activities as set out per Section 29 of the FIC Act that may exposed ML/TF,
- The table below indicates the reporting structure in Siyavika

Role player	Report to	Time frame
Junior staff	Team Leader	Immediately
Team leaders	Senior Management	Immediately
Senior Management	Board / Directors	Immediately
Board / Directors	FIC Compliance Officer	Immediately
FIC Compliance Officer	Financial Intelligence Centre via GOAML	As soon as possible but not longer than within 15 days

RISK MANAGEMENT AND COMPLIANCE PROGRAMME

AWARENESS DECLARATION BY SIYAVIKA EMPLOYEES

I _____ (full names and surname) with
ID _____ declare that I am fully aware of the contents and obligations
related to me as _____ (Job description) and will adhere to
obligations and requirements to support any suspicious transaction or activity as it
occurs.

Date: / /

Signature