Crypto Consult (PTY) LTD

FSP 55052 | REG: 2024/392954/07
389 Victoria Street, Waterkloof, Pretoria, 0181
L: +27 12 460 1330 | M:+27 68 607 8728

CRYPTO CONSULT
THE NEXT ERA OF INVESTING

RISK MANAGEMENT AND COMPLIANCE PROGRAMME

FOR

CRYPTO CONSULT (PTY) LTD

Authorised FSP No. 55052

Version Control	Date of Approval
1.0	12-02-26

Crypto Consult (PTY) LTD

FSP 55052 | REG: 2024/392954/07
389 Victoria Street, Waterkloof, Pretoria, 0181
L: +27 12 460 1330 | M:+27 68 607 8728

CRYPTO CONSULT
THE NEXT ERA OF INVESTING

Table of Contents

PREAMBLE

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

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

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

Crypto Consult (Pty) Ltd ("the institution") is an accountable institution as envisaged in the FIC Act. This Act requires the senior management of the institution to ensure compliance by the institution and its employees with the provisions of the FIC Act and a Risk Management and Compliance Programme.

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

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

BUSINESS OVERVIEW AND RISK ASSESSMENT

Crypto Consult (Pty) Ltd is a Category I and II financial services provider that specialises in cryptocurrency investment consultancy services offering financial planning, investment advice and fund management services to customers.

As an accountable institution, we are committed to preventing the use of our products and services for money laundering, terrorist financing or proliferation financing (ML/TF/PF) purposes. We take a risk-based approach to identifying, assessing, and mitigating our ML/TF/PF risks in line with the FIC Act and other relevant laws and regulations.

ML/TF/PF risk management is an integral part of the institution's broader strategic, operational, and management functions. The identification, assessment, and mitigation of these risks directly influence business objectives, customer engagement strategies, and governance structures. This ensures that risk mitigation measures are not only regulatory compliance exercises but also aligned with the institution's overall risk appetite, decision-making, and long-term sustainability.

This business risk assessment documents our methodology for identifying and assessing ML/TF/PF risks and the results of our inherent and residual risk assessment. It was developed with input from senior management and relevant business units, and will be regularly reviewed and updated on a 12-18 month cycle or when this RMCP is updated.

Risk Capacity and Appetite Statement

The Accountable Institution has no appetite for knowingly facilitating money laundering, terrorist financing or proliferation financing. We aim to effectively mitigate the ML/TF/PF risks identified in this assessment to within the following risk appetite:

- We will not offer products/services or take on customers that inherently pose an unacceptably high risk of ML/TF/PF that cannot be mitigated;
- We aim to bring any identified high risks down to a medium or low level through enhanced controls;
- We have a low tolerance for unidentified ML/TF/PF risks and will continuously monitor to identify emerging risks;
- We will provide adequate resources, systems and training to effectively implement our ML/TF/PF risk management framework.

Risk Assessment Methodology

Our risk assessment methodology looks at inherent risks across the key categories identified below:

- Customer risk (e.g. customer type, occupation, PEPs, sanctions)
- Geographic risk (e.g. high-risk countries, sanctions)
- Product/service risk (e.g. cash-intensive, high value, complexity)
- Delivery channel risk (e.g. non-face-to-face, third parties)
- Transaction risk (e.g. size, frequency, patterns)

Risk Assessment Results

After taking into the account the National and Sector Risk Assessment, risks in each category are rated by management per the below assessment.

- Inherent Risks may be totalled to give a LOW (0-28), MEDIUM (29-57) or High (58-85) result.
- Residual Risks may be totalled to give a LOW (0-28), MEDIUM (29-57) or High (58-85) result.
- Inherent and Residual risk scores may be totalled to give an overall LOW (0-56), MEDIUM (57-114) or HIGH (115-170) result.

RISK FACTOR	**INHERENT RISK RATING**	**INHERENT RISK**
Customer *(The FSP has the following clients)*	9	Natural Persons: Yes ☒ No ☐ If yes, a score of **2** should be added to the Inherent risk rating for Customers.
		Companies: Yes ☒ No ☐ If yes, a score of **3** should be added to the Inherent risk rating for Customers.
		Trusts: Yes ☒ No ☐ If yes, a score of **4** should be added to the Inherent risk rating for Customers.
		Funds: Yes ☐ No ☒ If yes, a score of **2** should be added to the Inherent risk rating for Customers.
		Complex Structures: Yes ☐ No ☒ If yes, a score of **4** should be added to the Inherent risk rating for Customers.
		DPEP'S, FPEP'S Yes ☐ No ☒

		If yes, a score of **5** should be added to the Inherent risk rating for Customers.
Geographic *(where are the FSP's clients located)*	2	Local Clients: Yes ☒ No ☐ If yes, a score of **2** should be added to the Inherent risk rating for Geographic.
		Foreign Clients: Yes ☐ No ☒ If yes, a score of **3** should be added to the Inherent risk rating for Geographic.
		High risk Jurisdictions i.e. Grey listed countries: Yes ☐ No ☒ If yes, a score of **5** should be added to the Inherent risk rating for Geographic.
Product/Service *(What Product services does the FSP render)*	7	Insurance Products: Yes ☐ No ☒ If yes, a score of **2** should be added to the Inherent risk rating for Product/Service.
		Investment Solutions: Yes ☒ No ☐ If yes, a score of **3** should be added to the Inherent risk rating for Product/Service.
		Retirement Products: Yes ☐ No ☒ If yes, a score of **2** should be added to the Inherent risk rating for Product/Service.
		Crypto Assets:

		Yes ☒ No ☐ If yes, a score of **4** should be added to the Inherent risk rating for Product/Service.
		Products with complex structures: Yes ☐ No ☒ If yes, a score of **5** should be added to the Inherent risk rating for Product/Service.
		Offshore Products: Yes ☐ No ☒ If yes, a score of **4** should be added to the Inherent risk rating for Product/Service.
Delivery Channel *(How are services rendered/instruction received from clients)*	8	How are clients Onboarded: ☒ Face to Face (Risk score 1) ☐ Telephonically (Risk score 4) ☒ Email (Risk score 4) ☐ Platform (Risk score 3) ☐ Via Third Parties (Risk score 5) If multiple, only use highest risk score

		How are services rendered: ☒ Face to Face (Risk score 1) ☐ Telephonically (Risk score 4) ☒ Email (Risk score 4) ☐ Platform (Risk score 3) ☐ Via Third Parties (Risk score 5) If multiple, only use highest risk score
Transaction	7	Does the FSP receive Third Party Payments: Yes ☐ No ☒ If yes, a score of **5** should be added to the Inherent risk rating for Transactions.
		Types of payments utilised: ☐ EFT's (Risk score 1) ☐ Cash (Risk score 4) ☒ Don't receive any funds directly (Risk Score 0) If multiple, only use highest risk score
		Are transactions local or cross border: ☒ Local (Risk score 1) ☐ Cross Border (Risk score 3) If multiple, only use highest risk score
		How long do clients stay with us: ☐ Short-term (Less than 12 months - risk score 3)

		☐ Medium-term (12 to 36 months - risk score 2) ☒ Long-term (36 months plus - risk score 1) If multiple, only use highest risk score	
		How often do clients Transact: ☒ Low Frequency (Risk score 1) ☐ Moderate Frequency (Risk score 2) ☐ High Frequency (Risk score 3) If multiple, only use highest risk score	
		How large are the average transaction received: ☐ Small (Less than R5000 - risk score 1) ☐ Medium (Between R5000 and R100,000 - risk score 2) ☒ Large (More than R100,000 risk score 3) If multiple, only use highest risk score	
		Where are client funds kept: ☒ No client funds held (Risk score 1) ☐ CCM Accounts (Risk score 2) ☐ FSP holds client funds in a separate bank account (Risk score 2) ☐ Both Separate and CCM Accounts (Risk score3) If multiple, only use highest risk score	
OVERALL INHERENT RISK RESULT		**33/85**	Medium

Existing preventive and detective controls are then identified to determine the level of residual risk remaining after controls are applied and risks mitigated.

RISK FACTOR	**RESIDUAL RISK RATING**	**MITGATING CONTROLS & RISK ANALYSIS AND ASSESSMENT**
Customer	8	Driven by retail clients (may include higher risk occupations that are cash intensive businesses, freelance professionals or even higher exposure to FPEP/DPEP individuals) with limited targeting of institutional/corporate clients; This is mitigated by customer due diligence performed at onboarding (as well as ongoing), including screening, that filters out higher risk individuals;
Geographic	1	Driven by retail client base that could include individuals from higher ML/TF risk countries that may be grey-listed or even be subject to sanctions; This is mitigated by initial and ongoing sanction screening and not allowing the onboarding of individuals from countries that FATF has identified as having serious strategic deficiencies in terms of ML/TF/PF, e.g., North Korea, Iran, Myanmar;
Product/Service	2	Driven mainly by the offering of complex investment structures service that could be attractive for ML/TF, with all transactions taking place electronically; This is mitigated by controls built into the service with additional limits and enhanced monitoring for higher risk clients;

Delivery Channel	4	Driven by non-face-to-face client communication, reliance on customer-supplied data to conduct customer due diligence; Mitigation: The institution tries to meet clients face to face prior to entering into a business relationship and makes use of screening and KYCDD to bolster monitoring;		
Transaction	6	Driven by lower value transactions but with high volumes. Potential to hide illicit transaction between legitimate transactions; This is mitigated by calibrated and enhanced transaction monitoring. As a rule the institution does not deal with third party payments.		
OVERALL RESIDUAL RISK RESULT			**21/85**	Low
TOTAL RISK SCORE *(INHERENT AND RESIDUAL)*			**54/170**	Low

Closing the Gap: RMCP Enhancements Driven by Risk Assessment

Based on the risk assessment results, this RMCP has been updated to ensure that the risk management framework remains aligned with our current risk profile. Key enhancements include:

- Client due diligence procedures strengthened;
- Management identified that the Directive 8 procedures must be improved;
- Management noted that the grey-list has been updated and must consider implementing enhanced due diligence for clients from e.g., Bulgaria, Burkina Faso, Cameroon, Croatia, Democratic Republic of Congo, Haiti, Kenya, Mali, Monaco, Mozambique, Namibia, Nigeria, Philippines, Senegal, South Africa, South Sudan, Syria, Tanzania, Venezuela, Vietnam, Yemen;

A RISK-BASED APPROACH

The institution follows a risk-based approach to client identification and verification regarding the type of information by means of which it will establish clients' identities and the means of verification of such information by various means.

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

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

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

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

DEFINITIONS

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

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

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

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

Address:	The Financial Intelligence Centre	
	Private Bag X177	
	Centurion	
	0046	
Tel Number:	0860 342 342 (FIC FIC)	
Compliance and Prevention:	Tel Number	0860 222 200
	Fax Number	0860 333 336
Head Office:	Tel Number	+27 12 641 6000
	Fax Number	+27 12 641 6215

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

"domestic politically exposed person" ('DPEP'), previously **"domestic prominent influential person"** ('DPIP') means an individual who,

- holds, including in an acting position for a period exceeding six months, or has held a prominent public function in the Republic, including that of-

  (i) the President or Deputy President;

  (ii) a government minister or deputy minister;

  (iii) the Premier of a province;

  (iv) a member of the Executive Council of a province;

  (v) an executive mayor of a municipality elected in terms of the Local Government: Municipal Structures Act, 1998 (Act No. 117 of 1998);

  (vi) a leader of a political party registered in terms of the Electoral Commission Act, 1996 (Act No. 51 of 1996);

  (vii) a member of a royal family or senior traditional leader as defined in the Traditional Leadership and Governance Frame work Act, 2003 (Act No. 41 of 2003);

  (viii) the head, accounting officer or chief financial officer of a national or provincial department or government component, as defined in section 1 of the Public Service Act, 1994 (Proclamation No. 103 of 1994);

  (ix) the municipal manager of a municipality appointed in terms of section 54A of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000), or a chief financial officer designated in terms of section 80(2) of the Municipal Finance Management Act, 2003 (Act No. 56 of 2003);

  (x) the chairperson of the controlling body, the chief executive officer, or a natural person who is the accounting authority, the chief financial officer or the chief investment officer of a public entity listed in Schedule 2 or 3 to the Public Finance Management Act, 1999 (Act No. 1 of 1999);

  (xi) the chairperson of the controlling body, chief executive officer, chief financial officer or chief investment officer of a municipal entity as defined in section 1 of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000);

  (xii) a constitutional court judge or any other judge as defined in section 1 of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act No. 47 of 2001);

(xiii) an ambassador or high commissioner or other senior representative of a foreign government based in the Republic; or
(xiv) an officer of the South African National Defence Force above the rank of major-general; or

- holds, including in an acting position for a period exceeding six months, or has held the position of head, or other executive directly accountable to that head, of an international organisation.

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

"foreign politically exposed person" ('FPEP'), previously **"foreign prominent public official"** ('FPPO')
is an individual who holds, or has held, in any foreign country a prominent public function including that of a-

(a) Head of State or head of a country or government;
(b) member of a foreign royal family;
(c) government minister or equivalent senior politician or leader of a political party;
(d) senior judicial official;
(e) senior executive of a state owned corporation; or
(f) high-ranking member of the military.

"immediate family member" means

- the spouse, civil partner or life partner;

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

"institution" means Crypto Consult (Pty) Ltd **;**

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

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

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

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

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

"proliferation financing" refers to the act of providing financial support or resources to individuals or groups involved in the development, acquisition, manufacture, or trade of weapons of mass destruction (WMDs) and their means of delivery. This includes providing financial support to entities involved in the proliferation of nuclear, biological, and chemical weapons, as well as ballistic missiles and other delivery systems. The financing of WMD proliferation can involve complex networks of individuals and entities, often across multiple jurisdictions, making it difficult to identify and disrupt. Proliferation financing poses a significant risk to global security, and efforts to prevent it are an important part of promoting peace and stability.

"prominent influential person" (PIP) refers to an individual who holds, or has held at any time in the preceding 12 months, the position of-

(a) chairperson of the board of directors;
(b) chairperson of the audit committee;
(c) executive officer; or
(d) chief financial officer,

of a company, as defined in the Companies Act, 2008 (Act No. 71 of 2008), if the company provides goods or services to an organ of state and the annual transactional value of the goods or services or both exceeds an amount determined by the Minister by notice in the Gazette.

"S42A Compliance Officer" for this institution is Gideon Frylinck.

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

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

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

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

Customer due diligence

Anonymous clients and clients acting under false or fictitious names (section 20A & 42(2)(c))

The institution may not establish a business relationship or conclude a single transaction with an anonymous client or a client with an apparent false or fictitious name and therefore the process under section 21 is followed at all times (single transaction and business relationship).

Identification of clients and other persons (section 21 & 42(2)(d) & 42(2)(m))

When engaging with a prospective client and / or contracted client to enter into a single transaction or to establish a business relationship, the institution must, in the course of concluding that single transaction or establishing that business relationship, establish and verify the identity of the client.

The steps the institution will follow in order to mitigate the risk of a prospective client / contracted client to launder money / finance terrorism though the institution is as follows:

The institution will apply a risk based approach in order to ascertain the level of customer due diligence to be applied by completing a risk assessment matrix for each client, same is completed automatically via KYCDD:

Category	Options	Score (1-5)

Product / Service	1 - Low complexity (SA Regulated Products) 3 - Medium complexity (offshore) 5 - High complexity / offshore / structured	
PEP Status	1 - Not a PEP 2 - Domestic PEP or Foreign PEP (automatic high-risk client)	
Source of Funds / Wealth	1 - Clear, verifiable (salary, pension, property, inheritance) 3 - Business/self-employed with proof 5 - Opaque / high-risk sources	
Geographic Risk	1 - SA/low-risk jurisdictions 3 - Grey-listed countries 5 - Sanctioned/high-risk jurisdictions	
Age of Client / Juristic Person	1 - >25 yrs or >5 yrs incorporated 2 - 18–25 yrs or <5 yrs incorporated 5 - Minor or newly incorporated <12 months	
Duration of Relationship	1 - Long-standing >3 yrs 3 - New client with long-term intent 5 - Once-off transaction	
Delivery Channel	1 - Direct, face-to-face/video 3 - Through intermediary (verifiable) 5 - Non-face-to-face, reliance on 3rd party	
Transaction Value / Activity	1 - Low (<R1m annually) 3 - Moderate (R1m–R2m annually) 5 - High/complex (>2m, offshore)	
Client's Occupation	1 - Low risk (employee) 3 - Medium (business owners) 5 - High risk (cash-intensive, NGOs, crypto)	

Business Activity	1 - Transparent, regulated industries 3 - Medium-risk industries (property, car dealer, mining etc.) 5 - High-risk (cash-intensive, gambling, offshore structures)	
Type of Client	1 - Natural person 3 - Juristic with transparent structure 5 - Complex (trusts, partnerships, offshore entities)	
Total Risk Score	Total all risk scores allocated above	
Risk Classification	Low/Medium/High	

Risk Classification	Low Risk (11-17) / Medium Risk (18-34) / High Risk (35-51)

The institution will weight all indicators equally and follow a low/simplified CDD if the majority of the risks are low, neutral/standard CDD if the majority of the risks are neutral and enhanced CDD if the majority of the risks are high. Any FPEP or DPEP will follow the enhanced CDD, no matter the risk rating score.

Based on this risk score that the institution will then collect the necessary verification documents depending on the customer due diligence level applied:

All clients and prospective clients will be screening against the TFS list prior to onboarding, on a continuous basis as part of ongoing CDD, including as and when the TFS list are updated. Noting that the institution utilizes the services of KYCDD who screen clients on a daily basis a list of all sanction list can be supplied/requested from KYCDD.

Natural Persons

Information to be obtained	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Full Name and Surname	Yes	Yes	Yes
Date of Birth	Yes	Yes	Yes
Identity/passport number*	Yes	Yes	Yes
Nationality	Yes	Yes	Yes
Residential Address**	No	Yes	Yes
Occupation	No	Yes	Yes
Source of funds	Yes	Yes	Yes
Source of income (wealth)	No	No	Yes
Verification of information obtained by means of documentation	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Identity/Passport Document*	Yes	Yes	Yes
Proof of residence**	No	Yes	Yes
Other	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Sanction list screening	Yes	Yes	Yes
Adverse media screening	No	No	Yes
Related parties screening	No	No	Yes
Senior management approval	No	No	Yes

Companies:			
Information to be obtained from natural person acting on behalf of company	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Registered name of the company	Yes	Yes	Yes
Registration number	Yes	Yes	Yes
Registered address	Yes	Yes	Yes
Operating address	Yes	Yes	Yes
Authorised person	Yes	Yes	Yes
Nature of business	Yes	Yes	Yes
Source of funds	Yes	Yes	Yes
Ownership and control structure	Yes	Yes	Yes
Beneficial owner(s)	Yes	Yes	Yes
Verification of information obtained by means of documentation	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Incorporation documentation	Yes	Yes	Yes

Register of shareholders	Yes	Yes	Yes
Proof of registered and operational address	No	Yes	Yes
Authorised signatory list	Yes	Yes	Yes
Identification document of each authorised signatory	No	No	Yes
Other	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Sanction list screening	Yes	Yes	Yes
Adverse media screening	No	No	Yes
Related parties screening	No	No	Yes
Senior management approval	No	No	Yes

Trusts:			
Information to be obtained from natural person acting on behalf of Trust	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Trust name	Yes	Yes	Yes

Trust registration number	Yes	Yes	Yes
Registered address	Yes	Yes	Yes
Authorised persons	Yes	Yes	Yes
List of Trustees/ Beneficiaries and Founder	Yes	Yes	Yes
Nature of trust	Yes	Yes	Yes
Source of trust wealth	Yes	Yes	Yes
Verification of information obtained by means of documentation	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Trust deed or other founding documentation	No	Yes	Yes
Letters of authority	Yes	Yes	Yes
Trust resolution nominating a Trustee to make investments on behalf of Trust	Yes	Yes	Yes
Identity documents of Trustees/ Beneficiaries and Founder	Yes	Yes	Yes
Other	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Sanction list screening	Yes	Yes	Yes

Adverse media screening	No	No	Yes
Related parties screening	No	No	Yes
Senior management approval	No	No	Yes

Partnerships:			
Information to be obtained from natural person acting on behalf of Partnership	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Partnership Name	Yes	Yes	Yes
List of full names, date of birth, Identity number of all partners	Yes	Yes	Yes
Authorised persons acting on the partnerships' behalf	Yes	Yes	Yes
Nature and makeup of partnership	Yes	Yes	Yes
Source of partnership wealth	Yes	Yes	Yes

Verification of information obtained by means of documentation	Simplified CDD (Low)	Standard CDD (Neutral)	Enhanced CDD (High)
Partnership agreement	No	Yes	Yes
Partnership resolution nominating a partner to make the investment on behalf of the partnership	Yes	Yes	Yes
Letter of authority of each person acting on behalf of the partnership	Yes	Yes	Yes
Identity documents of authorised person/s	Yes	Yes	Yes
Other	**Simplified CDD (Low)**	**Standard CDD (Neutral)**	**Enhanced CDD (High)**
Sanction list screening	Yes	Yes	Yes
Adverse media screening	No	No	Yes
Related parties screening	No	No	Yes
Senior management approval	No	No	Yes

*If an identity document is not available, a copy of their passport may be used for verification purposes. In instances in which it is deemed to be reasonably necessary to obtain, in addition to a person's identity document (foreign passport), further information or documentation identifying and verifying the identity of such a person, a letter of confirmation from a person in authority (for example, from the relevant embassy) which confirms authenticity of that person's identity document (passport), may be used.

**The address may be identified and verified by current documentation reflecting the name and address of the person. Examples of this include utility bills, bank statements, recent lease or rental agreements, municipal rates and taxes invoices, mortgage statements, telephone or cellular accounts, television licence documentation, motor vehicle licence documentation, recent long-term or short-term insurance documentation, recent SARS tax returns, recent correspondence from a body corporate or share-block association or a payslip or salary advice. This document should display a date that is not older than 3 months.

If the client is acting on behalf of another person, or if another person is acting on behalf of the client the institution must establish and verify:

- the identity of that client or other person, as above, and
- the client's or other person's authority to establish the business relationship, act or to conclude the single transaction on behalf of that other person or on behalf of a client.

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

If the institution had established a business relationship with a client (or if another person acted on behalf of the client) before the FIC Act took effect, it may not conclude a transaction in the course of that business relationship, unless it has taken the abovementioned steps to establish and verify the identity of the client.

Step by Step onboarding procedure:

- Step 1: The prospective client is supplied with a completion link on email via KYCDD;
- Step 2: clients are prompted to complete the automated onboarding process by selecting the client type e.g. Individual/Company/Trust;
- Step 3: all required information and verification documents per the above tables are uploaded by the client. Noting that the client cannot complete the workflow if the required information/documentation is not supplied;
- Step 4: all documents including the prospective clients identity is verified by the system and;
- Step 5: the prospective client is screened against the relevant TFS lists;
- Step 6: the information gathered is then utilised to compile the client risk matrix and identify a risk score for the client;
- Step 7: the FSP reviews all information to determine if any additional information may be required prior to accepting or declining the prospective clients application.

Understanding and obtaining information on a business relationship (section 21A & 42(2)(e))

When the institution engages with a prospective client to establish a business relationship as contemplated in section 21, the institution must, in addition to the steps required under section 21, obtain information to reasonably enable it to determine whether future transactions that will be performed in the course of the business relationship concerned are consistent with its knowledge of that prospective client.

Clients are required to sign an agreement (or the applicable mandate that governs the client interaction/product application forms). This forms the basis for the business relationship and inform the approach taken to decision making now and in the future and include information describing-

- The nature of the business relationship concerned.
- The intended purpose of the business relationship concerned.
- The source of the funds which that prospective client expects to use in concluding transactions in the course of the business relationship.

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

The institution will carry out additional due diligence measures in relation to the beneficial ownership of legal persons, trusts and partnerships. This includes identifying the nature of the client's business and establishing the ownership and control structure of the client. The primary goal is 'finding the hot body' (identifying the natural person(s) that is the beneficial owner(s)). Once identified, the institution will taking reasonable steps to verify their identity and perform the required due diligence steps on that individual, in terms of the table in section 21 above.

To achieve this, the institution will follow a process of elimination to identify the beneficial owners, in line with Section 21B of the FIC Act and the FIC's Public Compliance Communication 59:

Step 1: Controlling Ownership Interest

a. The institution will first identify any natural person who, independently or together with another person, directly or indirectly owns a controlling ownership interest of 5% or more in the legal person.

b. Ownership interest will be determined by shareholding, voting rights, or other forms of control specific to the type of legal entity.
c. If no natural person is identified with a controlling ownership interest, or if there is doubt about whether the person(s) with the controlling ownership interest are the beneficial owner(s), the institution will proceed to step 2.

Step 2: Control Through Other Means

d. The institution will identify any natural person who exercises control of the legal person through other means, including e.g., contractual arrangements, personal connections to persons in positions described in 1(a), power to appoint senior management, rights associated with invested capital, nominee shareholders acting for or on the directions of another person;
e. If no natural person is identified as exercising control through other means, the institution will proceed to step 3.

Step 3: Control Over Management - As a last resort, the institution will identify the natural person(s) who holds the position of senior managing official(s), including e.g., Chief Executive Officer, Managing Director, president, other senior executives with decision-making authority.

(For each step, the institution will take reasonable steps to verify the identity of the identified beneficial owner(s), and document the process followed, record the information obtained and the outcome/decisions made.)

The institution will use appropriate documentation to identify and verify beneficial owners for different entity types. This may include, but is not limited to:

Companies	Partnerships	Trusts
• Organogram (signed by director) • Memorandum of Incorporation/CIPC • Share register/certificates	• Partnership agreement • Partnership resolution	• Trust deed • Letters from the Master of the High Court

In cases where the ownership structure is complex or multi-layered:

- The institution will map out the entire ownership structure
- Identify all intermediate layers
- Apply the above steps at each layer until the ultimate beneficial owner(s) are identified

The institution recognises that there may be multiple beneficial owners for a single legal person. All identified beneficial owners will be recorded and verified.

If the institution is unable to identify any natural person as the beneficial owner after exhausting all reasonable means, it will not proceed with the transaction/business relationship and will consider filing a suspicious transaction report (STR) in terms of Section 29 of the Act.

Proliferation Financing

As an Accountable Institution, it is important to be aware of the risks associated with proliferation financing. Proliferation financing refers to the financing of the development, acquisition, manufacture, or trade of weapons of mass destruction (WMDs) and their means of delivery. This includes providing financial support to individuals, groups, or entities involved in WMD proliferation. Proliferation financing can pose significant risks to the integrity of the financial system and can contribute to global security threats.

As a responsible financial service provider, we must take steps to prevent our services from being used for proliferation financing and comply with relevant laws and regulations.

This involves implementing robust anti-money laundering and counter-terrorist financing controls to detect and prevent suspicious transactions related to WMD proliferation. We must also comply with relevant laws and regulations, such as the United Nations Security Council's targeted financial sanctions and South Africa's Prevention and Combating of Terrorist and Proliferation Financing Act.

Furthermore, we are proactive in combating proliferation financing by conducting due diligence on our clients and third-party relationships to ensure that they do not have any ties to WMD proliferation. By taking these steps, we can help prevent proliferation financing and contribute to global efforts to promote peace and security.

Ongoing due diligence (section 21C & 42(2)(g) & 42(2)(h))

The institution must conduct ongoing due diligence and account monitoring in respect of a business relationship which includes:

- monitoring of transactions undertaken throughout the course of the relationship, including, where necessary the source of funds, to ensure that the transactions are consistent with the institution's knowledge of the client and the client's business and risk profile.

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

  The institution will examine complex or unusually large transactions and unusual patterns of transactions which have no apparent business or lawful purpose and will then be flagged for further investigation by management.
- keeping information obtained for the purpose of establishing and verifying the identities of clients pursuant to sections 21, 21A and 21B of the FIC Act, up to date.

Doubts about veracity of previously obtained information (section 21D & 42(2)(i))

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

Inability to conduct customer due diligence (section 21E & 42(2)(k))

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

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

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

Foreign politically exposed person ('FPEP'), previously "foreign prominent public official" ('FPPO') (section 21F & 21H & 42(2)(l))

If the institution determines that a prospective client with whom it engages to establish a business relationship, or the beneficial owner of that prospective client, is a FPEP, it must obtain senior management approval for establishing the business relationship, in the following manner:

Prepare a report detailing the nature of the prospective client and what the potential risks associated with engaging in a business relationship with this client are and what impact they could have on the business, financially or otherwise. This report should be provided with a recommendation which then needs to be considered by senior management who make the final decision.

- take reasonable measures to establish the source of wealth and source of funds of the client.
  The nature and source of wealth needs to be requested from the client and supporting documents need to be supplied, in the form of a salary slip, investment statement, bank statement, or similar in order for the institution to satisfy itself that these funds are not proceeds from money laundering, terrorist financing or other illicit activities defined in the FIC Act.
  and
- conduct enhanced ongoing monitoring, as put forth in the table under section 21 above, of the business relationship, in the following manner:

Reconcile all inflows with a source of funds and continuously monitor all transactions linked to an account. Conduct enhanced screening of clients for appearance on sanctions lists.

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

In addition to the above, section 21 must be followed on each FPEP.

Domestic politically exposed person ('DPEP'), previously "domestic prominent influential person" ('DPIP') (section 21G & 21H & 42(2)(l))

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

- obtain senior management approval for establishing the business relationship, in the following manner:

Prepare a report detailing the nature of the prospective client and what the potential risks associated with engaging in a business relationship with this client are and what impact they could have on the business, financially or otherwise. This report should be provided with a recommendation which then needs to be considered by senior management who make the final decision.

- take reasonable measures to establish the source of wealth and source of funds of the client, in the following manner:

The nature and source of wealth needs to be requested from the client and supporting documents need to be supplied, in the form of a salary slip, investment statement,

statement, or similar in order for the institution to satisfy itself that these funds are not proceeds from money laundering, terrorist financing or other illicit activities defined in the FIC Act.

- conduct enhanced ongoing monitoring, as put forth in the table under section 21 above, of the business relationship, in the following manner:

Reconcile all inflows with a source of funds and continuously monitor all transactions linked to an account. Conduct enhanced screening of clients for appearance on sanctions lists.

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

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

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

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

Reliance on customer due diligence performed by another accountable institution
Exemption 4 (b) under the FIC Act previously exempted accountable institutions from compliance with the identification of clients by allowing for reliance on written confirmation from a primary accountable institution as to the identity of the client. Exemption 4 (b) has been withdrawn.

The institution does not rely on the customer due diligence performed by another accountable institution.

Duty to keep records:

Obligation to keep customer due diligence records (section 22 & 42(2)(n))

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

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

This information is kept on the institution's server.

Obligation to keep transaction records (section 22A & 42(2)(n))

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

The records must reflect the following information:

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

This information is kept on the institution's server.

Period for which records must be kept (section 23)

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

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

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

[While the FAIS Act only requires 5 years, SARS advises 7 years +]

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

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

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

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

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

The institution does not make use of a 3rd party company to store information, although it does make use of Software-as-a-service providers, like Microsoft.

Reporting duties and access to information (section 42(2(o))

Reporting obligations to advise Centre of clients (section 27 & 42(2)(p))

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

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

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

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

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

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

Cash transactions above prescribed limit (section 28)

The Institution will within the prescribed period, report to the Centre the prescribed particulars concerning a transaction concluded with a client if in terms of the transaction an amount of cash in excess of the prescribed amount is paid to or received from a client.

- The prescribed amount of cash above which a transaction must be reported was R24999.99 and changed to R49 999,99*, effective 14 November 2022.

The obligation to report in terms of Section 28 therefore arises when a transaction is concluded with a client by means of which cash of R50 000.00 or more is received by or paid by the institution. This includes receiving or paying cash in person as well as receiving or paying it via a third party. This obligation also arise with cash deposits made into the account of the accountable institution.
Section 28 reports must be sent to the Centre as soon as possible but not later than 3* working days after becoming aware of the fact of a cash transaction that have exceed R49 999,99*.

*The Minister of Finance, in terms of section 77(1)(a) of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), revised the threshold for cash transaction reporting (CTR) effective 14 November 2022. The threshold for reporting cash transactions is contained in the Money Laundering and Terrorist Financing Control (MLTFC) Regulations. The amended MLTFC Regulations were published in Government Notice No. 2638 as published in Government Gazette No. 47302 on Friday, 14 October 2022.

The CTR threshold was revised from R24999.99 to R49999.99 and the time afforded to institutions to report same was revised from two business days to three business days from the date on which the accountable/reporting institution, or any of their employees, have become aware of the transaction. Any transactions before 14 November 2022 will still be subject to these old limits.

The 24-hour aggregation requirement has also been removed. Accountable institutions should submit a suspicious transaction report (STR) if it deems that the amounts received are deliberately being kept under the threshold limit to avoid triggering a cash threshold report.

Information to be reported concerning a cash threshold report:

(1) When a reporter makes a cash threshold report, the report must contain full particulars of

(a) the name of the accountable or reporting institution making the report;

(b) the identifying particulars of the accountable or reporting institution on whose behalf the report is made including a registration or license number;

(c) the contact address of the accountable or reporting institution on whose behalf the report is made;

(d) the type of business or economic sector of the accountable or reporting institution on whose behalf the report is made;

(e) in the case of a legal person or an entity making the report, the surname, first name, date of birth and contact particulars of a contact person who may be contacted in relation to the report; and

(f) if the contact person mentioned in paragraph

(e) is—

(i) a South African citizen or resident, the identifying particulars of that person and the type of a South African citizen or resident, the identifying particulars of that person and the type of identifying document from which the particulars were obtained; or

(ii) not a South African citizen or resident, the identifying particulars of that contact person and the source of identifying information from which the particulars referred to were obtained and the issuing country thereof.

(2) In respect of the transaction for which a cash threshold report is made, the report must contain—

(a) full particulars of—

(i) the location where the transaction took place;

(ii) the date of the transaction;

(iii) the value of the transaction in local currency; and

(iv) a description of how the transaction was conducted; and

(b) as much information as is readily available concerning the currency in which the funds were disposed of.

(3) In respect of each natural person conducting the transaction or legal person or entity on whose behalf the transaction is conducted, for which a cash threshold report is made, the report must contain as much of the following information as is readily available—

(a) in the case of a natural person—

(i) the person's title, gender, names and surname;

(ii) the person's identifying number, nationality and date of birth;

(iii) the source of identifying information from which the particulars referred to in subparagraphs (i) and (ii) were obtained;

(iv) the person's contact address in the Republic;

(v) the person's contact number;

(vi) the person's occupation;

(vii) the person's country of residence;

(viii) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;

(ix) the person's alias, if any;

(x) the person's source of funds;

(xi) the person's income tax number; and

(xii) the person's employer's name, contact address and contact particulars; and (b) in the case of a legal person or other entity—

(i) the person's or entity's name;

(ii) the person's or entity's identifying number, if it has such a number;

(iii) the information referred to in paragraph (a) in respect of the natural person with authority to conduct the transaction on behalf of the person or entity; and

(iv) in the case of a company, the information referred to in paragraph (a) in respect of at least one director of that company; or

(v) in the case of another type of legal person or other entity, the information referred to in paragraph (a) in respect of at least one natural person associated with that legal person or entity and the role of such person in the legal person or entity.

(4) If any account held at the reporter was involved in the transaction for which a cash threshold report is made, the report must contain—

(a) full particulars in respect of each such account, of—

(i) the account number;

(ii) the name and identifying particulars of the branch or office of the reporter where each account is held;

(iii) the type of account;

(iv) the currency in which this account is denominated; and

(v) the date on which the account was opened; and

(b) as much of the following information as is readily available in respect of each signatory on each such account—

(i) the person's title, gender, names and surname;

(ii) the person's identifying number, nationality and date of birth;

(iii) the source of identifying information from which the particulars referred to in subparagraphs (i) and (ii) were obtained;

(iv) the person's alias, if any;

(v) he person's contact address in the Republic;

(vi) the person's country of residence;

(vii) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;

(viii) the person's contact number;

(ix) the person's occupation;

(x) the source of funds of the person;

(xi) the person's income tax number; and

(xii) the person's employer's name, contact address and contact particulars.

(5) A cash threshold report must contain an indicator or indicators in respect of the circumstances that gave rise to the submission of the report.".

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

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

The accountable institution does not collect cash directly from clients and have a policy to never pay out any cash amounts to clients.

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

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

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

A report filed in terms of section 28A is based on the knowledge of an accountable institution that it has property related to the financing of terrorism in its possession or under its control. The knowledge about the origin and ownership of the property in question should be based on fact and should be acquired with reference to an objective set of circumstances or fact. Section 28A therefore applies to a purely factual situation. The fact that an accountable institution

has certain property in its possession or under its control is sufficient to prompt a report and no activity relating to that property is required to trigger the reporting obligation.

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

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

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

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

Suspicious and unusual transactions (section 29 & 42(2)(j))

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

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

- a person who is employed by a business

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

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

A report under section 29 of must be filed with the Centre within 15 working days after the knowledge was acquired or the suspicion arose.
The report must set out the grounds for the knowledge or suspicion and the prescribed particulars concerning the suspicious or unusual transaction or series of transactions.

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

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

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

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

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

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

In terms of section 45B (2A) an inspector of the Centre or prescribed supervisory body may order from an accountable institution or reporting institution under inspection, the production of a copy of a report, or the furnishing of a fact or information related to the report, contemplated in section 29.

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

Conveyance of cash to or from Republic (section 30)

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

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

Starting from 1 February 2023, accountable institutions must report any electronic transfers of money that exceed the threshold of R19 999.99 to or from South Africa to the Financial Intelligence Centre (FIC) when they send or receive such amounts on behalf or on the instruction of another person. The relevant International Fund Transfer Report (IFTR) must be filed no later than three days after the money was transferred, along with the required details about the transfer. Failing to comply with this requirement will lead to an offence and an administrative penalty.

Please refer to Guidance note 9/ (DRAFT) Guidance note 104 that states that only certain accountable institutions that are authorized to handle cross-border electronic fund transfers must comply with section 31 of the FIC Act. These institutions include e.g.,: Authorised dealers (ADs), Authorised dealers with limited authority (ADLAs), some category of financial services providers (FSP) with direct reporting under the Exchange Control Regulations , and finally The Post Office. These institutions are authorized under the Currency and Exchanges Act, 1933 (Act 9 of 1933) regulations. Only they are legally

allowed to transfer funds into and out of South Africa.

Reporting procedures and furnishing of additional information (section 32)

A report in terms of section 28, 28A, 29 or 31 to the Centre and a report in terms of section 30 (1) to a person authorised by the Minister must be made in the prescribed manner. These reports include but are not limited to:

- Suspicious and Unusual Transaction Report (STR)
- Suspicious Activity Report (SAR)
- Terrorist Financing Transaction Report (TFTR)
- Terrorist Financing Activity Report (TFAR)
- Terrorist Property Report (TPR)
- Cash Threshold Report (CTR)

The institution has appointed the section 42A Compliance Officer, with the responsibility and authority to submit the reports to the Centre on behalf of the institution. The appointment of a MLRO is voluntary and is mostly applicable in the case of large organisations where the institution is required to submit a large amount of reports to the Centre. The Institution has not appointed a separate MLRO at this stage.

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

The step by step procedure for submission of the above reports including the requisite information required may be found via - https://www.fic.gov.za/compliance/compliance-guidance/user-guides/

These procedures outline the process for submitting reports to the Financial Intelligence Centre (FIC) via the goAML platform in compliance with sections 28, 28A and 29 of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001).

1. Registration and Access

1. Access the system at **https://goweb.fic.gov.za/goAMLWeb_PRD**.
2. Log in using your registered credentials and authenticate via **two-factor authentication** (Microsoft/Google Authenticator or fallback email code).

2. When to Submit Reports

Report Type	Trigger Event	FIC Act Section
CTR	Cash received or paid ≥ R49 999.99	s28
STR / SAR	Suspicion or unusual transaction/activity (ML/TF indicators)	s29(1)(a–c)
TFAR/TFTR	Suspicious activity/transaction relating specifically to terrorist financing	s29(1)(c)
TPR	Property owned or controlled by, or for, a UN-sanctioned or POCDATARA entity/person	s28A

All reports must be filed as soon as possible once the obligation arises; do not delay for additional information.

---

3. Capturing the Report (All Report Types)

Step 1 – Create the Report

- On the goAML menu, select **New Reports → Web Reports → [Select Report Type] → Create Report**.

Step 2 – Report Header

- Auto-populated with your entity and user details.

- If resubmitting, include the **original FIC reference number**.

Step 3 – Location

- Verify and, if necessary, edit the branch or office location where the transaction/activity/property occurred.

Step 4 – Reason for Reporting

- Mandatory free-text field describing why the report is made (suspicion, threshold, or terrorist linkage).

Step 5 – Action Taken

- Mandatory for STR, SAR, TFAR, TFTR & TPR: describe actions taken (e.g., freeze property, block transaction, notify law enforcement).

Step 6 – Attachments

- Upload supporting evidence, client files, screenshots, or correspondence (recommended for STR/SAR/TPR).

Step 7 – Indicators

- Select applicable indicators (e.g., structuring, sanctions evasion, unusual transaction pattern, TFS match).

Step 8 – Activity / Transaction Details

- **CTR:** Record each transaction above threshold.
- **STR/SAR/TFAR/TFTR:** Capture suspicious or unusual activities (attempted, abandoned, or completed).
- **TPR:** Record the property or asset linked to terrorism/TFS.

Step 9 – Report Parties (Person / Entity / Account)

- Add all relevant parties:
    - **Person:** natural person
    - **Entity:** legal person or business
    - **Account:** account involved (bank or crypto)

      Each party may include related individuals (e.g., directors, signatories).

Step 10 – Goods / Services (if applicable)

- Complete only if physical property or assets are involved (e.g., vehicle, real estate, gold, crypto).

4. Submission

1. Validate all mandatory fields (*).
2. Once all sections turn green, click Submit Report.
3. The system issues a FIC reference number. Save confirmation and message board receipt

5. Record Keeping & Follow-Up

- Retain: submission record, attachments, reference number, screenshots, and any correspondence for five years.
- Monitor the Message Board for feedback or rejections.
- For TPRs, maintain the freeze until officially lifted under the FIC's instruction.

6. Key Differences Between Report Types

Report Type	Focus Area	Mandatory Sections
CTR	Cash in/out ≥ R49,999.99	Transaction details
STR / SAR	Suspicious/unusual transaction	Reason & Action
TFAR/TFTR	Suspected terrorist financing	Indicators, Activity
TPR	Terrorist property / UN-listed entity	Reason, Action, Goods/Services

Report Type	Focus Area	Mandatory Sections
All Reports	Must complete all fields marked (*) or "not obtained"	Mandatory fields apply

7. Controls and Accountability

- **Frontline staff:** identify triggers and escalate immediately.
- **MLRO/S42A CO:** verify, complete and submit the report.
- **Senior Management:** oversee compliance and ensure remediation of rejections.

Information Required for the abovementioned goAML Reports include but are not limited to:

(CTR • STR • SAR • TFTR • TFAR • TPR)

1. General Information (All Reports)

- Report Type (CTR / STR / SAR / TFTR / TFAR / TPR) *
- Reporting Entity Name and Branch *
- Reporting Entity Reference / Internal Case Number *
- MLRO/ S42A CO / Reporting Person Name *
- Date of Submission (auto-generated) *
- Location of Event / Branch Address *
- Reason for Reporting (free text) *
- Action Taken (freeze, block, escalate, etc.) *
- Indicators (select from list) *
- Attachments (supporting docs) examples below:

Attachment Type	Examples
Identification Documents	ID, passport, registration certificate
Transaction Evidence	Deposit slips, SWIFT messages, transfer records
Communication Evidence	Emails, chat logs, or call transcripts
Account Statements	Bank or crypto statements showing flows
Screenshots	Of system entries, alerts, or TMS hits
Sanctions Match	Screening results, UNSC list hits
Internal Memo	MLRO decision or escalation notes
Law Enforcement Request	If prior engagement occurred

---

2. Parties Involved

- **Person:** full name, ID/passport, DOB, nationality, gender *
- **Entity:** legal name, registration no., country, business type *
- **Account:** number, type, institution, currency *
- My Client / Not My Client status *
- Contact info (phone, email, address) *
- Related persons (directors, signatories, beneficial owners)

The above step and information may vary, please consult the latest manual prior to submission.

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

Continuation of transactions (section 33)

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

Intervention by Centre (section 34)

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

Monitoring orders (section 35)

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

Reporting duty, obligation to provide information not affected by confidentiality rules

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

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

Protection of persons making reports (section 38)

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

Measures to promote compliance

Risk Management and Compliance Programme (section 42)

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

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

Distinguishing between prospective clients and established clients (section 42(2)(b))

The institution can determine if a person is a prospective client in the process of establishing a business relationship or entering into a single transaction with it or a client who has established a business relationship or entered into a single transaction by checking if the person/entity has any existing agreements or investments with the institution. Prospective clients have not yet signed any documentation establishing their relationship with the

institution while an established client will have such a signed agreement in place. Should this not be clear, management should be consulted together with the administrative staff.

Implementation of the RMCP in branches, subsidiaries and foreign countries (section 42(2)(q))

The institution does not have any branches in any foreign countries and therefore, this Risk Management Compliance Programme will not be implemented in branches, subsidiaries or other operations of the institution in foreign countries.

Management and employees will be notified of this RMCP face-to-face and electronically and this document will be circulated in order to uniformly implement this new programme across the entire organisation.

Review of Risk Management and Compliance Programme (section 42)

This Risk Management and Compliance Programme is maintained by the institution. The institution will review this Risk Management and Compliance Programme annually to ensure that it remains relevant to the institution's operations and the achievement of the legislative requirements.

The institution will also ensure that its ML/TF risk management controls remain effective and responsive to emerging threats, new product offerings, and changes in client risk profiles. Continuous monitoring will be conducted to adapt to evolving risks beyond the annual review cycle.

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

This Risk Management and Compliance Programme is made available electronically (accessible at any time on the institutions servers) to each employee of the institution involved in transactions to which the FIC Act applies.

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

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

Governance of compliance (section 42A)

Senior management is responsible for compliance by the institution and its employees with the FIC Act and this Risk Management Compliance Programme. The institution remains responsible for any compliance failures.

The institution has appointed an external compliance officer to assist the board of directors with their obligations in terms of the FIC Act as well as an internal s42(a) compliance officer with sufficient competence and seniority to ensure the effectiveness of the compliance function.

Training of employees (section 43)

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

Employees are required to complete an annual FIC refresher course and questionnaire which ensures that their knowledge of the FIC Act is current and accurate.

Screening of employees (directive 8)

Accountable institutions are required to periodically screen both prospective and current employees for competence and integrity, in a risk-based manner in accordance with Directive 8 issued by the Financial Intelligence Centre (FIC).

As an accountable institution under the Financial Intelligence Centre Act, we are committed to preventing the abuse of our institution for money laundering, terrorist financing or proliferation financing (ML/TF/PF) purposes. A key aspect of our ML/TF/PF risk management framework is identifying, assessing, mitigating & monitoring risks related to our employees in line with the requirements of Directive 8.

Employee Risk Assessment Methodology

Our employee risk assessment looks at inherent ML/TF/PF risks posed by different employee roles based on:

- Level of employee access to sensitive customer/transaction data
- Ability of employee to alter AML/TF/PF controls or decision-making
- Employee interactions with high-risk customers (e.g. PEPs)
- Employee connections to high-risk geographies

Taking a risk-based approach translates to applying screening that is proportionate to the level of ML/TF/PF risk that the employee might pose. Senior management positions and where employees may take decisions to alter the ML/TF/PF risk of the accountable institution are considered to pose a higher risk.

This employee risk assessment determines the frequency and depth of screening for each employee:

- High Risk (e.g., senior management, AML/CFT roles):

  Screening every 2 years including criminal record checks, credit history, employment history verification, reference checks, and sanctions list screening.

- Medium Risk (e.g., customer-facing staff):

  Screening every 5 years, including criminal record checks, employment history verification, reference checks, and sanctions list screening.

- Low Risk (e.g., back-office staff):

  Screening every 10 years, including criminal record checks and sanctions list screening.

Screening Process

All (prospective) employees will be screened upon hiring, with ongoing screening occurring with any role changes and in line with the frequency required for their risk rating.

All employees are also furthermore screened against the TFS list whenever the list is updated.

We conduct thorough checks using reputable third-party providers while adhering to all relevant labour laws and POPIA requirements.

- **Screening for Competence**

Screening for competence determines if the employee has the necessary skills, knowledge and expertise for their role. This may include reviewing previous employment history, employment references, qualifications and accreditations.

- **Screening for Integrity**

Integrity screening relates to evaluating the honesty and moral principles of the employee. At a minimum this includes:

  - Criminal record checks, especially for financial crimes, money laundering, dishonesty
  - Qualification checks
  - Evaluation against the institution's code of conduct requirements

- Enhanced screening measures will be applied for employee roles that pose a higher ML/TF/PF risk.

Outcome of screening

Directive 8 and PCC55 make it clear that no person may provide economic support, financial or other services to any person who is listed on a targeted financial sanctions list, as per section 26B of the FIC Act.

If an employee is found to be on the TFS list, the accountable institution will not employ such an individual or continue to provide financial support or services to that employee.

For any other risk, the accountable institution will attempt to mitigate & monitor the risk, such as imposing restrictions on their access rights, requiring additional approvals, etc.

Recordkeeping

The accountable institution must provide for, and record, the manner in which screening for competence and integrity, as well as the manner in which scrutinising of employee information against targeted financial sanctions lists, is conducted.

We maintain secure records of all employee screening activities and outcomes for the required retention periods.

Review and Update

This program is reviewed annually or when the RMCP is updated to ensure its continued effectiveness. Risk-based decisions are taken to mitigate and manage ML/TF/PF risk based on screening outcomes.

The institution will complete a risk rating matrix for each (prospective) employee and for each screening event, excluding on going TFS list screening:

Employee Risk Rating Form Template

Name: _____

Position: _____

Date: _____

Reason for screening: _____

Risk Factor Map	High	Medium	Low
Level of employee access to sensitive customer/transaction data	e.g., unrestricted access (management)	e.g., partial access	e.g., no access
Ability to alter AML/CFT controls or decision-making	e.g., can make significant changes	e.g., can make minor changes	e.g., no ability to make changes
Interaction with high-risk customers (e.g., PEPs)	e.g., frequent interaction	e.g., occasional interaction	e.g., no interaction

Connections to high-risk geographies	e.g., citizen or frequent travel	e.g., occasional travel	e.g., no connections
Competence	e.g., lacks necessary skills, knowledge, or expertise for the role	e.g., has some relevant skills, knowledge, or expertise, but may require additional training or support	e.g., possesses all necessary skills, knowledge, and expertise for the role
Integrity	e.g., criminal record related to financial crimes, money laundering, or dishonesty; significant violations of the institution's code of conduct	e.g., has a criminal record, but unrelated to financial crimes, money laundering, or dishonesty; consistently demonstrates honesty and adheres to the institution's code of conduct	e.g., no criminal record; consistently demonstrates honesty and adheres to the institution's code of conduct
TFS List	e.g., employee appears on the TFS list		e.g., employee does not appear on the TFS list and has no known connections to listed individuals or entities

Overall Risk Rating

Based on the above factors, the employee's overall ML/TF/PF risk is:

	CRITICAL – Individual on TFS list and may not be employed				
	High		**Medium**		**Low**

Screening	**Outcome**
Competence	e.g. Position requires a recognized qualification. Qualification verified with MIE on 01/05/2024.
Integrity	e.g. Criminal check done – No adverse comments.
TFS List	e.g. Individual is reflecting on the TFS list.

Outcome:

The prospective employee was not employed due to an adverse hit on the TFS list.

Management signoff:

_____

OBO Accountable Institution

Registration with the Centre (section 43B)

Any person or category of persons who, on commencing a new business, fall within the list of accountable institutions (or reporting institutions) in Schedule 1 (or Schedule 3 for reporting institutions) must, within 90 days of the day the business is opened (authorised as financial services provider), register with the Centre. Registration is done via the www.fic.gov.za website.

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

COMPLIANCE AND ENFORCEMENT

The FIC Act distinguishes between administrative sanctions and criminal offences.

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

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

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

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

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

POCA penalties for committing a section 2(1) offence equals a fine not exceeding R1000 million or to imprisonment for a period up to imprisonment for life. POCA penalties for committing a section 4, 5 or 6 offence equals a fine not exceeding R100 million or to imprisonment for a period not exceeding 30 years.

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

Crypto Consult (PTY) LTD

FSP 55052 | REG: 2024/392954/07
389 Victoria Street, Waterkloof, Pretoria, 0181
L: +27 12 460 1330 | M:+27 68 607 8728

APPROVAL OF RISK MANAGEMENT COMPLIANCE PROGRAMME

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

Signature: .....

Full name: Gideon Frylinck

Designation: DIRECTOR

Signed on this day of 12 February 2026 in Pretoria