UZUMBA (PTY)LTD

RISK MANAGEMENT AND COMPLIANCE PROGRAMME

Reviewed and updated on the 22nd of October 2024

Table of Contents

1. Introduction

1.1. Uzumba Pty (Ltd) (Uzumba) carries on a business of high value goods dealer, dealing in krugerrands and precious metals. Krugarrands and precious metals are a high-value attractive commodity and dealing with them makes the business vulnerable to crime syndicates who wish to disguise the true origin of their assets, which exposes the business to liabilities under Anti-Money Laundering (AML) Law and Combating the Financing Terrorism (CFT). Consequently, our business is listed under Item 20 of Schedule 1 to the FIC Act as an accountable institution.

2. Risk Management and Compliance Programme (RMCP) for Uzumba (Pty) Ltd

2.1. Section 42(1) of the FIC Act requires accountable institution to develop, document, maintain and implement a programme for anti-money laundering, counter terrorist financing and proliferation financing risk management and compliance.

2.2. We have conducted a reassessment of our business activities/services and this RMCP will enable us to:

(i) Identify,

(ii) Assess,

(iii) monitor,

(iv) mitigate, and

(v) manage the risks that our products or services may involve or facilitate money laundering activities or the financing of terrorist and related activities as required in terms of section 42(2)(a) of the FIC Act.

2.3. In conducting this assessment, the business has carefully considered The Sector Risk Assessment for Krugerrand dealers that was published by the Financial Intelligence Centre (FIC) in 2022.

2.4. This RMCP uses a risk-based approach to determine the minimum reasonable and practical measures that the business will implement to achieve FICA objectives.

2.5. In addition, this RMCP is to be complemented with all legislations applicable to the business' internal controls, standard operating procedures and company policies.

2.6. The business has conducted a reassessment of the business activities/ services with the purpose and objective of identifying, assessing and better understanding of the inherent money laundering and terrorist financing risks.

3. The Risk Based Approach

3.1. As required by the FIC Act, our RMCP incorporates a risk-based approach to limiting our exposure to being exploited to promote money laundering or terrorist financing activities.

3.2. The risk-based approach requires the business to conduct

(i) A simplified due diligence for low-risk clients and business relationships

(ii) An enhanced due diligence for higher risk clients and business relationships

3.3. Applying a risk-based approach allows us to accurately assess the risk involved with regards to clients and business relationships by considering amongst others the:

(i) Client profile;

(ii) Nature of the business;

(iii) Type and transaction;

(iv) Duration of the client relationship with us;

(v) Source of funds;

(vi) Jurisdiction of the client;

(vii) Transaction value; and

(viii) Type of entity that we are dealing with.

(Refer to Annexure A for our details analysis of risk Factors)

3.4. We are, in addition, required to be aware of the risk in relation to how our services may be abused by persons who are intent on carrying out money laundering and/or terrorist activities.

3.5. Given the above, the key focus of this RMCP is to ensure that the business is able to identify, assess, monitor, mitigate, and manage the risk that our clients might, during their relationship with us, be seeking to launder money or finance terrorism.

3.6. We are also required to comply with Public Compliance Communication No 53 on Risk Management and Compliance Programme in terms of Section 42 of FICA which can be viewed at https://www.fic.gov.za/Documents/220830%20PCC%2053%20RMCP%20Final.pdf.

3.7. Additionally, the measures that we are required to implement and adopt are dealt with under the headings below.

4. Customer Due Diligence Measures

4.1. Customer Due Diligence (CDD) measures are procedures used to identify, verify, and assess the risk of customers or clients to prevent:

(i) Money laundering
(ii) Terrorist financing
(iii) Identity theft
(iv) Financial crimes
(v) Sanctions evasion

4.2. Our CDD Measures includes:

4.2.1. **Customer Identification Program (CIP):** Verify customer identity through documents, data, or other information.

4.2.2. **Beneficial Ownership Identification:** Identify individuals with 25% or more ownership or control.

4.2.3. **Risk Assessment**: Evaluate customer risk based on factors like business type, location, and transaction history.

4.2.4. **Customer Screening**: Check customers against sanctions lists, PEP (Politically Exposed Persons) lists, and other relevant databases.

4.2.5. **Ongoing Monitoring:** Regularly review customer transactions and updates to ensure compliance.

4.2.6. **Enhanced Due Diligence (EDD):** Apply additional measures for high-risk customers, such as:

(i) Source of funds verification
(ii) Business description and purpose
(iii) Expected transaction activity
(iv) Regular updates on customer information

4.3. Uzumba will suspend a business relationship with clients who do not meet our CDD requirements.

4.4. Reinstatement of a business relationship will only occur after our CDD requirements have been met.

(See the table of Information Required for various client types below)

5. Section 21 - Prospective clients and clients

5.1. A prospective client is a client who approaches us with a view to entering into a business relationship after FICA became effective.

5.2. When we engage with a prospective client to enter into a single transaction or to establish a business relationship, we must, prior to concluding that single transaction or establishing that business relationship:

(i) Establish and verify the identity of the client;

(ii) If the client is acting on behalf of another person, establish and verify:

a) The identity of that other person; and

b) The client's authority to establish the business relationship or to conclude the single transaction on behalf of that other person; and

(iii) If another person is acting on behalf of the client, establish and verify:

a) The identity of that other person; and

b) That other person's authority to act on behalf of the client.

5.3. All prospective clients are required to complete our Application forms before onboarding.

5.4. Should the prospective client fail to disclose to us the nature of the business that the prospective client engages in and/or the beneficial ownership of the prospective client (despite requests made by us) for the information then we will decline to enter into the business relationship with the prospective client as required by Section 21E of FICA.

5.5. In this instance, and whilst no transaction has been concluded, we are nonetheless required in terms of Section 29 of FICA to file a suspicious activity report with the FIC.

5.6. In the event of us having established a business relationship with a client before FICA took effect, then we may not conclude a transaction in the course of that business relationship, unless we have taken the following prescribed steps:

(i) To establish and verify the identity of the client;

(ii) If another person acted on behalf of the client in establishing the business relationship to establish and verify the identity of the client;

5.7. If another person acted on behalf of the client in establishing the business relationship, to establish and verify:

(i) The identity of that other person; and

(ii) That other person's authority to act on behalf of the client;

5.8. If the client acted on behalf of another person in establishing the business relationship, to establish and verify:

(i) The identity of that other person; and

(ii) The client's authority to act on behalf of that other person; and

(iii) To trace all accounts at that accountable institution that are involved in transactions concluded in the course of that business relationship.

5.9. Should a client fail to satisfy the requirements as set out above then we will terminate our business relationship with such client as required by Section 21E of FICA.

5.10. In this instance, and whilst no further services may have been provided, we are nonetheless required in terms of Section 29 of FICA to file a suspicious activity report.

5.11. Notwithstanding the above, and under no circumstances whatsoever, will we establish a business relationship or conduct a single transaction with an anonymous client or client with an apparent false or fictitious name.

6. **Section 20 – Anonymous clients and client acting under false or fictitious names;**

6.1. The business does not establish a business relationship or conclude a single transaction with anonymous clients or client with an apparent false or fictitious name.

6.2. All prospective clients are required to complete our Application forms.

6.3. Should the prospective client fail to disclose to us the nature of the business that the prospective client engages in and/or the beneficial ownership of the prospective client (despite requests made by us) for the information then we will decline to enter into the business relationship with the prospective client as required by Section 21E of FICA.

6.4. In this instance, and whilst no transaction has been concluded, we are nonetheless required in terms of Section 29 of FICA to file a suspicious activity report with the FIC.

6.5. In the event of us having established a business relationship with a client before FICA took effect, then we may not conclude a transaction in the course of that business relationship, unless we have taken the following prescribed steps:

(i) To establish and verify the identity of the client;

(ii) If another person acted on behalf of the client in establishing the business relationship to establish and verify the identity of the client;

6.6. If another person acted on behalf of the client in establishing the business relationship, to establish and verify:

(i) The identity of that other person; and

(ii) That other person's authority to act on behalf of the client;

6.7. if the client acted on behalf of another person in establishing the business relationship, to establish and verify:

(i) the identity of that other person; and

(ii) the client's authority to act on behalf of that other person; and

(iii) to trace all accounts at that accountable institution that are involved in transactions concluded in the course of that business relationship.

6.8. Should a client fail to satisfy the requirements as set out above then we will terminate our business relationship with such client as required by Section 21E of FICA.

6.9. In this instance, and whilst no further services may have been provided, we are nonetheless required in terms of Section 29 of FICA to file a suspicious activity report.

6.10. As an overriding proviso, and under no circumstances whatsoever, will we establish a business relationship or conduct a single transaction with an anonymous client or client with an apparent false or fictitious name.

7. Section 21B - Legal persons, trusts and partnerships

7.1. If our client is a **legal person**, a **trust or a partnership**, we must establish:

(i) the nature of the client's business;

(ii) the ownership and control structure of the client; - the identity of the beneficial owner of the client.

7.2. If our client is a partnership we must establish:

(i) The name of the partnership;

(ii) The identity of every partner, including silent partners;

(iii) The identity of the person who exercises executive control over the partnership;

(iv) The identity of the person who is authorised to represent or bind the partnership; and

(v) Verify the identities of the persons so identified.

7.3. If our client is a trust, we must establish:

(i) The identifying name and number of the trust;

(ii) The address of the master of the high court where the trust is registered;

(iii) The identity of the founder of the trust;

(iv) The identity of each trustee and of any person who is authorised to represent or bind the trust;

(v) The identity of each beneficiary referred to in the trust deed or other document which created the trust and, if there are no named beneficiaries, establish how the beneficiaries of the trust are to be determined;

(vi) And verify the information obtained about the trust and the identities of the natural persons that have been so identified.

8. Beneficial owner

8.1. In establishing the identity of **the beneficial owner of the client**, we must determine the identity of each natural person who has a controlling ownership interest in the client.

8.2. If there is doubt as to who this might be, the identity of each natural person who exercises de facto control of the company must be established. This person might be a Chief Executive Officer, a Director or Manager.

8.3. In addition, the identity of the beneficial owner of the client must also be verified.

9. Our rules regarding the identification of clients are as follows:

9.1. Identification is received prior to any transactions being concluded and no transaction will be concluded without identification and verification of client.

9.2. Uzumba's Application Form or Offer to Purchase, which requires identification information of the client must be completed.

9.3. No product will be delivered until verification documentation is received.

9.4. The person receiving FICA documents must make copies, date and sign copies to note that originals have been seen.

9.5. Although Uzumba sells mostly to natural persons and corporate clients, the business is open to sell to any client type.

10. A summary of our basic identification and verification information and documents required from a client, irrespective of the deal type.

Client type	Information required	Verification documents/ Method
South African Citizens	● Full names ● Date of birth ● Identity number ● Residential address	● Identity document /or ● Driver's license/ or ● or Passport, and Any from the list below: ● Utility Bill not older than 3 months, ● Bank statement from another, ● Bank confirming the particulars of the person ● Recent lease or rental agreement ● Municipal rates and taxes invoice

		● Telephone/Cellular account ● Valid television license ● Recent Motor vehicle license ● Employer's certificate
Foreign Citizens	● Full names ● Date of birth ● Passport number ● Nationality ● Residential address	● Driver's license/or ● Passport and ● Work permit **NB: Non-resident do not need to submit proof of residence**
South African Companies	● Registration name ● Registration number ● Registered address ● Name under which business is conducted ● The address from which the company operate ● Personal details of the manager/CEO of the company ● The mandate officials who are authorized to establish a business relationship	● Company registration certificate Any of the documents below: ● Utility bill/ ● Company statement/ ● Recent lease or rental agreement/ ● Municipal rates/ ● taxes invoice/ ● Telkom account/
Other legal person (Includes government	● Name of the legal person; ● The address from which it operates; ● Its legal form (i.e local municipality); and ● Full name, date of birth, identity number, residential address and contact particulars of each natural person who is authorised to act on behalf of the legal person	● Constitution or other founding documents. ● Copies of ID of each representative

11. Section 21 C - Ongoing due diligence

11.1. Business relationships and client conduct are not static, and we must, on an ongoing basis, monitor the relationships by considering:

(i) The source of funds, to ensure that the transactions are consistent with our knowledge of the client, the client's business and risk profile;

(ii) The background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent business or lawful purpose; and

(iii) Keeping information obtained for the purpose of establishing and verifying the identities of clients.

11.2. Should we suspect a suspicious or unusual transaction during the course of a business relationship, then such transaction must similarly be investigated.

11.3. The following would form the basis of this investigation:

(i) who is involved in the transaction;

(ii) Who is there a commercial and lawful purpose for the transaction; - the source/origin of funding for the transaction.

11.4. The determination in relation to suspicion or a suspicious transaction:

(i) May arise from the consideration of a number of factors that may seem to be innocent, if viewed in isolation, but raise suspicion when taken together.

(ii) All relevant factors must, therefore, be considered;

(iii) Does not arise from a full-scale investigation but rather a reasonable evaluation of all relevant facts and circumstances.

11.5. By knowing our clients and regularly assessing them and their transactions for the duration of our business relationship, we can guard against and prevent money laundering and terrorist financing.

12. Section 21D – Doubts about veracity of previously obtained information

12.1. To the extent that we have any **doubts about the veracity** of previously obtained information we must repeat the verification process and take such additional reasonable steps to verify the information obtained prior to engaging or continuing in a business relationship.

13. High-risk clients – Enhanced Due Diligence

13.1. It is important for us to be able to identify where it is necessary for us to conduct **enhanced due diligence** methods for higher risk business relationships.

13.2. We would, in addition to what is set out below, identify a high-risk client as any client who:

(i) is a natural person, but is not a citizen or permanent resident of South Africa;

(ii) has no operations or premises in South Africa;

(iii) is a party to an unusual or complicated transaction;

(iv) has an unusual or inexplicable preference for dealing *via* correspondence or *via* electronic media, as opposed to in person, particularly for the purposes of the customer due diligence;

(v) has a blatant lack of concern or disregard for the costs involved in a transaction;
or - is deliberately evasive or vague when providing documentation or information.

13.3. Where enhanced due diligence procedures are required, these shall be designed on an *ad hoc* basis, in consultation with the Compliance Officer and the Managing Director, with regard to the risk that they are intended to mitigate, or the suspicious or unusual behavior they are required to explain.

13.4. For all other clients, standard customer due diligence will be sufficient.

13.5. Standard customer due diligence procedures for the various categories of clients are outlined in the Application form or Offer to purchase.

14. Section 21E - Inability to conduct customer due diligence

14.1. If we are unable to:

(i) Establish and verify the identity of a client or other relevant person in accordance with section 21 or 21B

(ii) Obtain information contemplated in section 21A; or

(iii) Conduct ongoing due diligence as contemplated in section 21C, we:

a) will not establish a business relationship or conclude a single transaction with the client;

b) will not conclude a transaction in the course of business relationship, or perform any act to give effect to a single transaction; or

c) Must terminate the existing business relations ship with a client and consider making a report under section 29 of the fic act, as the case may be.

15. Section 21F to H - Foreign Politically Exposed Persons (FPEPs), Domestic Politically Exposed Persons (DPEPs) and their family members and their known close associates

15.1. These categories of people must be given special treatment in terms of FICA. People falling into this category are those listed in Schedule 3A, 3B and 3C of the FIC Act.

15.2. If we are dealing with Foreign Politically Exposed Persons, or their family members or known close associates, these people are automatically high risk and additional client due diligence steps must be taken before establishing a business relationship or entering into a single transaction with such a person.

15.3. These enhanced steps that the business must follow are the following:

i. You will require director approval to establish the business relationship; and
ii. You will need to establish the source of wealth of the client and his or her source of funds to conclude the transaction; and
iii. Enhanced ongoing monitoring of the business relationship must be conducted.

15.4. In the event that your basic FICA verification and client due diligence investigations in respect of a DPEP and/or their family members and their known close associates shows a higher risk, the same enhanced steps must be implemented.

15.5. For all other clients, standard customer due diligence will be sufficient.

15.6. Standard customer due diligence procedures for the various categories of clients are outlined in the questionnaires contained in the Schedules at the end of this RMCP.

15.7. Where enhanced due diligence procedures are required, these shall be designed on an ad hoc basis, in consultation with the Compliance Officer and the Managing Director, with regard to the risk that they are intended to mitigate, or the suspicious or unusual behaviour they are required to explain.

16. Co-operation with other accountable institutions

16.1. If we have a client in common with another Accountable Institution, (a Secondary Accountable Institution); and:

(i) That client in common is in respect of the same transaction, and

(ii) The secondary accountable institution agrees to subject, or has already subjected the client to customer due diligence procedures in accordance with that secondary accountable institution's own RMCP; and

(iii) The secondary accountable institution agrees to furnish us with:

(iv) A letter to the effect that it has satisfied itself as to the identity and other prescribed particulars of the client in compliance with FICA, and

(v) Copies of the documents and / or records of the information relied upon to carry out the secondary accountable institution's customer due diligence procedures in respect of the client,

(vi) Then we may, instead of applying our own customer due diligence, rely on the letter and documents provided by the secondary accountable institution, and thus be regarded as having complied with FICA and the RMCP.

(vii) If the letter from the Secondary Accountable Institution does not cover all the information that would have been required in terms of our RMCP, we must supplement the information in the letter by means of our own customer due diligence.

17. Section 22 - Keeping of Records

17.1. By their very nature, the results of our FICA enquiries are privileged personal records relating to our clients. The business is required to keep record of information acquired pursuant to section 21 to 21H of the FIC Act

17.2. No records are to be removed from the file for any reason without the authority of the FICA Compliance Officer and no such records are to be made available to any third party without the consent of the client to whom they relate, unless required by law.

17.3. FICA records are to be retained on the individual transaction file in our office and in our archives where we keep our old files, for a period of 5 years. If a report is made, the FICA records must be retained for a period of 5 years from the date of the report.

17.4. The Compliance Officer may elect to keep the records and documents, or any part thereof in an electronic format. The Managing Director and Compliance Officer shall, in such case, ensure that backup copies of all records and documents that are stored in an electronic format are made immediately a record that has been electronically captured.

18. Records kept by third party

18.1. In the event that Uzumba enlists a third party (such as Metro file, Document Warehouse, etc.) to retain records on our behalf in accordance with FICA, Uzumba will provide the FIC with the following details:

(i) The Third parties':

a. Full name if the third party is a neutral person; or

b. Registered name if the third party is a close corporation or company;

(ii) The name under which the third party conducts business;

(iii) The name and contact particulars of the individual who exercises control over the access to the records;

(iv) The address where the records are kept;

(v) The address from where the third-party exercises control of the records;

(vi) The full name and contact particulars of the individual who liaises with the third party on behalf of Uzumba concerning the retention of records

19. Assessment of AML Risks

It is important for the Business to understand the risks posed within the context of the products being sold. Accordingly, the risks are dependent upon the services being rendered. Uzumba will examine and keep records of all business relations and transactions as follows:

19.1. Complex or unusually large transactions

The business shall examine cash desk transactions in at least the manner described herein. The manner in which complex or unusually large transactions are examined may include:

(i) By comparing the routine manner in which the transactions were concluded in the past for the client against a different or complicated manner requested by the client in current transaction;

(ii) By comparing the values of previous transactions concluded by a client against the values of current transactions where the values are obviously larger.

(iii) The examinations concerned shall be made using reasonable and practical methods available to the business and shall be conducted at regular intervals.

19.2. Unusual patterns of transactions which have no apparent business or lawful purpose and high-risk factors

19.2.1. Conducting businesses with DPEPs and those closely associated with or related to them:

(i) Conducting business relationships in unusual circumstances.

(ii) Obscuring the identity of beneficial owners or controlling interests through shelf or front companies or nominee shares or bearer shares.

(iii) Enabling company formation and asset administration over different countries without any ostensible legal, tax, business, economic or other reason.

(iv) Conducting business involving unusual and unexplained complexity in control or ownership structures without an economic purpose.

(v) Conducting business in unconventional circumstances considering full context.

(vi) Conducting business with extraordinary and substantial amounts of cash.

(vii) Conducting business using new technologies may have inherent weaknesses for exploitation by criminals.

(viii) Operating as non-profit organizations engaging in transactions having no logical economic purpose or ostensible purpose with other parties.

(ix) Acting on behalf of an undisclosed person.

(x) Entering into transactions being affected mainly through the use of virtual assets to preserve anonymity, without motivation.

(xi) Being suspected of being engaged in falsifying or misleading activities.

19.3. Transaction Risk - The business will take into account that the following services may present higher risk:

(i) The Business being expected to act as a financial intermediary in a business transaction by receiving and transmitting funds through accounts under their control.

(ii) Clients depositing funds in the Business account which do not involve products being sold by Uzumba

(iii) Receiving payments from account different to bank confirmation letter received during KYC

(iv) Clients requesting financial transactions to occur outside the Business account

(v) Services facilitating the concealment of beneficial ownership from competent authorities.

(vi) Payments received from unfamiliar or unknown third parties and unconventional cash payments.

(vii) Use of anonymous and/or unusual payment methods, virtual currency and wealth transfer without a clear economic or other legitimate reason.

(viii) Transactions involving closely connected persons with no rational explanations and no apparent economic or other legitimate reason.

(ix) Transactions not adequately accounted for including incorrect invoicing of goods/services, falsely described goods/services, and multiple trading of goods/services.

The business will not consider the above risk categories in isolation. A holistic approach will accordingly be adopted to ensure a suitable risk assessment.

20. Monitoring of AML Risk

20.1. The business will, in the context of an extended client relationship, likely be exposed to changes in the client's risk profile. The Business will, where appropriate, conduct ongoing risk and control assessments to monitor a client's risk profile. The degree of ongoing monitoring will depend on several factors, including:

(i) The size of the business;
(ii) The business's available resources;
(iii) The risk profile of the client, as assessed at the inception of the client relationship;
(iv) The nature of changes that have occurred since inception of the client relationship;
(v) Changes in sources of funds to which the client may have accessed; and
(vi) Instructions to execute further risk-related services or transactions.

20.2. The business, where appropriately, regularly:

(i) Assess the effectiveness of its policies, systems and controls; and
(ii) Set up systems to detect unusual and suspicious transactions with reference to beneficial ownership.

21. Mitigating AML Risk

21.1. The business will adopt relevant policies to guide the implementation of this Program and ensure that training is being completed at regular intervals.

21.2. The FIC specific measures to be considered with reference to of higher AML/CFT risks, include:

(i) Increased review periods of client information.

(ii) Utilising more or higher quality sources for the vetting of information (impacts both quality and quantity).

(iii) Senior management involvement in decisions to on-board clients.

(iv) Limited reliance on another accountable institution's controls.

(v) Only on-board the Client with the approval of the Risk Officer;

22. Record Keeping and Reporting

22.1. The Business will keep a record of the information required under sections 21 to 21H of the Act, which includes information relating to:

(i) Verification of client's details;

(ii) With reference to a business relationship, the nature and 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.

(iii) Every transaction, whether the transaction is a single transaction or concluded in the course of a business relationship which the business has with the client, that are reasonably necessary to enable that transaction to be readily reconstructed, which must, amongst other, reflect the following information:

a. The amount and currency involved;

b. The parties to and date on which the transaction was concluded; and o the nature of the transaction and business correspondence.

23. Reportable transactions and activities

(i) Subject to legal professional privilege, section 29 of the FIC Act requires any person who is employed by a business to report to the FIC suspicious and unusual transactions relating to the proceeds of unlawful activities connected to the affairs of such business.

(ii) Accordingly, a report may need to be made to the FIC where an employee knows or suspects (or ought reasonably to have known or suspected) that the Business:

(iii) Has 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;

(iv) Is party to a transaction that:

(v) 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;

(vi) Has no business or lawful purpose;

(vii) Is constructed to avoid any reporting duty under the FIC Act; or

(viii) May be relevant to the investigation of any evasion or attempted evasion of a duty to pay tax or any other duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Service; or

(ix) Relates to an offence relating to the financing of terrorist and related activities

(x) The business uses EFT to pay its precious metals suppliers. EFT is the business's preferred method of payment. The business does not accept cash in the premises, the business also prohibits the use cash in our business transactions

(xi) FICA provides for the obligation to report cash transactions above the prescribed threshold (R49 999.99) in terms of section 28. Uzumba is required to file a cash threshold report with the FIC when it has knowledge of the transaction that exceeds the prescribed threshold.

(xii) In an event that clients deposit money into Business's bank account, the Business will still report the transaction even though the bank could have reported it (dual reporting)

(i) Section 29 of FICA places duty to report strs BY the following persons:

a. A person who carries on a business at Uzumba, or

b. A person who is in charge of or manages a business of Uzumba, or

c. A person who is employed by Uzumba.

24. Client Risk Rating Factors

24.1. Products and services risks

(i) Certain products and services are regarded as posing a higher risk for money laundering purposes.

(ii) The products and services that we provide that are internationally recognised as more likely to be abused by criminals in the money laundering process include: **Krugerrands** and **other items of high value:**

Krugerrand dealers may knowingly or unwittingly assist criminals by accepting cash that is proceeds of unlawful activities in exchange for Krugerrands or other items of high value.

We must be specifically vigilant insofar as the payment for our services is concerned as this could in some instances, also be a channel for money laundering, with the use of cash pointing to a higher likelihood of funds derived from criminal activities.

24.2. Client risks

24.2.1. Some clients, such as FPEPs, DPEPS, complex legal structures or foreigners potentially pose a higher risk for money laundering, depending on the identified circumstances. The establishment of complex structures, involving legal persons (companies) and legal arrangements such as trusts and partnerships including where such structures are named as beneficiaries for a trust – could possibly be aimed at concealing the ultimate beneficial owners of such legal persons and arrangements. This risk rating will be conducted when onboarding the client and will be reassessed from time to time.

24.2.2. When dealing with our clients, we must be aware of, *inter alia*, the following possible scenarios (and our reporting obligations in respect thereof) pertaining to the nature and behaviour of the clients that could point to possible money laundering:

(i) Clients trying to conceal their identities
(ii) Transactions inconsistent with their stated income or occupation
(iii) Clients using an unusual source of funds to transact
(iv) Transactions that do not have legitimate or economic reason
(v) Clients ceasing their business relationships upon request for customer due diligence information

24.3. Transaction Risk

24.3.1. We are aware that international research and literature indicate that criminals can potentially use Krugerrands dealers creating an impression of the legitimacy to transactions involving the proceeds of crime.

24.3.2. We must in any such transaction monitor:

(i) The nature and purpose of these transactions

(ii) Their monetary worth and means of payment involved so as to ensure that we give effect to our obligations in terms of the FIC Act insofar as they relate to money laundering risks associated with these transactions

24.3.3. We must be specifically vigilant of transactions that are potentially high risk for money laundering. These would include:

(i) The use of cash or crypto currencies in transactions.

(ii) The reversing of transactions with a request to repay funds already paid and transactions that do not make economic sense.

24.3.4. The business will not accept cash (above the threshold) or crypto currencies for the payment of services or in respect of any transaction.

24.3.5. Other factors the business will look at include

(i) The Business being expected to act as a financial intermediary in a business transaction by receiving and transmitting funds through accounts under their control.

(ii) Clients depositing funds in the Business account which do not involve products being sold by Uzumba

(iii) Receiving payments from account different to bank confirmation letter received during KYC

(iv) Clients requesting financial transactions to occur outside the Business account

(v) Services facilitating the concealment of beneficial ownership from competent authorities.

(vi) Payments received from unfamiliar or unknown third parties and unconventional cash payments.

(vii) Use of anonymous and/or unusual payment methods, virtual currency and wealth transfer without a clear economic or other legitimate reason.

(viii) Transactions involving closely connected persons with no rational explanations and no apparent economic or other legitimate reason.

(ix) Transactions not adequately accounted for including incorrect invoicing of goods/services, falsely described goods/services, and multiple trading of goods/services.

24.3.6. The business will not consider the above risk categories in isolation. A holistic approach will accordingly be adopted to ensure a suitable risk assessment.

23.4. Risks relating to delivery channels

23.4.1. We must be aware of the delivery channels that we use to attract and deal with clients.

23.4.2. Delivery channels that may obscure or conceal the true identity of the client, or that result in clients not being on-boarded face-to-face, may increase the risk of our firm being abused by criminals to launder the proceeds of crime.

23.4.3. Additionally, we will not use intermediary to onboard our clients.

23.4.4. In our use of technology:

(i) To advertise our services and to conduct business.

(ii) To conduct business with clients via social media platforms.

23.4.5. We must be aware of the potential higher risks associated with the less stringent verification requirements of social media. Where social media platforms are used to share information on products or services or to on-board clients, we must ensure that such clients are properly identified and verified and that all the relevant information pertaining to the risks posed by such clients is obtained.

23.4.6. Where third party service providers are used to assist with the identification and verification of clients or to introduce clients to the our practice, we must ensure that the third party is properly identified and verified and that its services are above board. We must be aware and consider that the payment of funds through a third party could be done to disguise the source of funds or certain assets. When such a situation occurs we must, in order to mitigate the risks, always ensure that we understand the source of the funds and the reason for constructing the transaction in this manner.

23.5. Geographic risk

23.5.1. Some foreign jurisdictions pose a higher risk for money laundering. It is important that we are aware of the risks posed by clients from these jurisdictions and that they have the necessary risk mitigation processes in place. This risk is exacerbated by the fact that transactions can take place electronically across regions and national jurisdictions, and that such transactions often require the services of Legal Practitioners.

23.5.2. The geographic location and services provided by our practice is also an important factor for determining ultimate money laundering risks.

24. Terrorist financing risk

24.1. Where we provide services to non-profit and non-governmental organisations, we should ensure that the funds used are in accordance with the stated objectives of these organisations.

24.2. In this regard we restate our obligations in sections 26A and 28A of FICA which relate to the screening of clients to ensure that clients are not included in United Nations Sanctions Lists.

25. ML/CFT Clients Risk Rating Matrix

This matrix allows Uzumba to assess risks based on factors like customer type, transaction size, and payment method, ensuring that higher-risk transactions receive additional scrutiny.

Risk Category	Low	Medium	High
Customer Type	Individual buyers, known customers	Small businesses, some verification	Anonymous/High-Net-Worth Individuals, minimal verification
Transaction Size	Small (<1000 Oz)	Medium (1001-4000 Oz)	Large (>4001 Oz)
Transaction Frequency	Occasional	Regular	Frequent/High-volume
Payment Method	Bank transfer verified	Cash/Credit card	Unverified/Third-party
Customer Verification	Verified ID/documents	Partial verification	No verification
Source of Funds	Declared/Verified	Undeclared/Unverified	Suspicious/Untraceable
Geographic Location	Local/Well-known areas	Regional/Border areas	High-risk/Conflict zones
Product Type	Standard Krugerrands	Collectible/High-value coins	Modified/Altered coins

Scoring table for **Silver, Gold, Krugerrands, and Minted Bars** based on risk levels, with assigned scores indicating risk. This scoring helps prioritize monitoring and due diligence based on the type of product, focusing more resources on higher-value items like minted bars and Krugerrands.

Product Type	Risk Level	Score	Reasoning
Silver	Low-Risk	1-2	Lower value, less appeal for high-risk activities
Gold	Medium-Risk	3-4	Moderate value, requires some due diligence
Krugerrands	Medium-High Risk	5-8	High value, popular for investment; requires enhanced due diligence
Minted Bars	High-Risk	9-12	Highest value, often high demand; intensive monitoring recommended

This scoring system helps to calculate total risk levels by summing scores across relevant risk categories, supporting a comprehensive risk assessment.

No	Risk Category	Description	Risk Level	Score
1.	Supplier/Client Registered Office Location	South Africa	Low	1
		Outside South Africa	Medium	3
		High-Risk Area	High	5
2.	Gold Origin	Non-Conflict Area	Low	1
		Conflict-Affected/High-Risk Area	High	5
3.	Gold Supplying Supplier/Client	No PEP involvement	Low	1
		Politically Exposed Persons (PEP)	High	5
4.	Business Activity	Lower Risk Industry	Low	1
		Higher Risk Industry (Arms, Gaming, etc.)	High	5
5.	Human Rights Abuses	None	Low	1
		Systematic or Widespread Abuses	High	5
6.	Bribery/Fraudulent Misrepresentation	No evidence	Low	1
		Evidence of Bribery/Misrepresentation	High	5
7.	Money Laundering/Financing Terrorism	No high-risk country or transactions	Low	1
		High-Risk Country or Transactions	High	5
8.	Transaction Type	Direct Purchase	Low	1
		Toll Refining	Medium	3
		Complex Transactions	High	5
9.	Source of Material	First-Tier Supplier	Low	1
		Multi-Tier Supplier	Medium	3
10.	Annual Volumes	<1000 Oz/month	Low	1
		1001-4000 Oz/month	Medium	3
		>4000/month	High	5
11.	Import Permit	No Permit	Low	1
		Active Permit	High	5
12.	Legal Action	None	Low	1
		Historic/Pending/Current Legal Action	High	5
13.	Licenses/Permits	Single License	Low	1
		Multiple Licenses	High	5
14.	Product Type	Silver	Low	1
		Gold	Medium	3
		Krugerrands	Medium-High	4
		Minted Bars	High	5
15.	Client Type	Individual investor	Low	1
		Small business	Medium	3
		Anonymous/High-net-worth	High	5
16.	Transaction Frequency	Occasional	Low	1
		Regular	Medium	3
		Frequent/High-volume	High	5
17.	Payment Method	Bank transfer verified	Low	1
		Cash/Credit card	Medium	3
		Unverified/Third-party	High	5

Customer scoring and the required actions compatible to the risk appetite

Risk Level	Score Range	Actions
Low-Risk	1-12	Routine monitoring
Medium-Risk	13-20	Enhanced due diligence
High-Risk	21 and above	Intensive monitoring, potential reporting

Mitigation Strategies
Implement enhanced customer due diligence
Monitor transactions regularly
Verify source of funds
Conduct regular risk assessments
Train staff on AML/CFT regulations

26. FIC Act regulatory reporting obligations

Under the Financial Intelligence Centre (FIC) Act, there are three main types of reports that accountable institutions are required to submit. These reports are crucial in helping prevent and detect financial crimes, such as money laundering and terrorist financing. Accountable institutions must ensure they comply with the FIC Act's reporting requirements to avoid penalties

26.1. Cash threshold reporting - Section 28 FIC Act

(i) As an accountable institution, we must report cash transactions of R49 999.99 and above

(ii) Cash transaction – Cash, coins, paper money and travellers' cheque (not an EFT)

(iii) Report must be done within **three business days** of the transaction.

26.2. Terrorist property reporting – Sections 26A, 26 C and 28A of the FIC ACT

26.2.1. In terms of Section 28A FIC Act

(i) The business if in its possession or under its control property owned or controlled by or on behalf of, or at the direction of terrorist, and/or a sanctioned person must within five days of becoming aware report that fact and the prescribed particulars to the FIC.

(ii) An accountable institution must scrutinise its client information to determine whether such person is designated on a targeted financial sanctions list

26.2.2. The business's process of screening of employees for competence and integrity and scrutinising of employee information against applicable targeted

financial sanctions lists as a money laundering, terrorist financing and proliferation financing control measure.

26.2.3. All prospective employees and current employees:

(i) Are to be screened for competence and integrity, and

(ii) Their information will in addition be scrutinised against the targeted financial sanctions lists, in order to identify, assess, monitor, mitigate and manage the risk of money laundering, terrorist financing and proliferation financing.

26.2.4. The screening will take place periodically and will be done in a risk-based manner.

26.2.5. As an accountable institution, he business we are required and we will scrutinise information concerning our prospective clients and current clients upon notice being given under section 26A (3) of the FIC Act.

26.2.6. We will in addition, and in respect of all employees and potential employees:

(i) Check that they are not listed on any targeted financial sanctions lists.

(ii) Verify/confirm their identity.

(iii) Verify and confirm all references.

(iv) Verify and confirm all qualifications.

26.2.7. The outcome of the screening process shall be made available to FIC upon request.

26.2.8. These reports are filed when there's a match with a party on the targeted financial sanctions list or the United Nations Security Council Resolution 1267 list.

Reporting: Cash threshold and terrorist property reporting considerations

(i) Like the CDD obligations discussed above, the business's reporting obligations relating to cash threshold reports (CTRs) in terms of section 28 and terrorist property reports (TPRs) in terms of section 28A of the FIC Act only arise in a transaction or business relationship relating to a high- value good with a client

(ii) CTR or TPR regulatory reporting obligations do not arise for transactions or business relationships relating to items that are not high-value goods (i.e. where the item is less than R100 000). For example, the business enters into a transaction of less than R100 000 per item, and they receive cash, this would not be reportable, unless it is a suspicious or unusual transaction.

(iii) Should the business enter into a transaction in relation to a high-value good, and the client pays a portion of the R100 000 or more in cash which meets the CTR reporting

threshold of R49 999.99 and above, the cash element remains reportable to the FIC as a CTR

26.3. Section 29 - Suspicious and unusual transaction reporting

When filing STRs, SARs, TFTRs, TFARs the suspicion or knowledge relates to:

(i) The proceeds of unlawful activity
(ii) Unlawful activity
(iii) Facilitating the transfer of proceeds of unlawful activity
(iv) Has no apparent business or lawful purpose
(v) May be relevant to the investigation of an evasion or attempted evasion of a duty to pay tax evasion or attempted tax evasion
(vi) An offence relating to the financing of terrorist and related activities
(vii) The contravention of a prohibition under section 26B of the FIC Act and/or
(viii) Any structuring of a transaction or activity which is conducted for the purpose of avoiding giving rise to a reporting duty under the FIC Act.

26.4. Trends and Indicators to be aware of

(i) High-value goods are vulnerable to abuse by criminals for money laundering, terrorist financing and proliferation financing.
(ii) Trends indicate criminals often seek to buy high-value goods with the proceeds of crime.
(iii) Use of attorneys to launder proceeds of crime through high-end goods.
(iv) Use of third-party spouse to hide the proceeds of crimes.
(v) Use of personal accounts to move funds generated from business transactions.
(vi) Transaction patterns inconsistent with client's profile.
(vii) Flow of funds from accounts to offshore destinations.
(viii) Dealers often want to transact in cash to avoid detection.
(ix) Low barriers to entry in the sector
(x) Stolen Krugerrands could be melted down, recast into another gold form and sold for cash.
(xi) Foreign nationals purchasing gold bullion through multiple transactions over a short period

(xii) Purchases for no apparent commercial or investment purpose

(xiii) Krugerrands are moved from or to a jurisdiction designated as high-risk for money laundering activities or sensitive or non-cooperative jurisdictions.

(xiv) Unusual pattern of Kruger rand transactions and the nature of the transactions are inconsistent with the customer profile

(xv) The transaction involves the use of front or shell companies where the client is an entity

(xvi) Original source of funds to buy Krugerrands cannot be established

(xvii) Goods purchased by suspected criminal syndicates

26.5. When does the duty to report STR arise?

26.5.1. If this person knows or suspects that:

(i) The business has received or is about to receive the proceeds of unlawful activities.

(ii) A transaction or series of transactions to which the business is a party–

a. Facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities.

b. has no apparent business or lawful purpose.

c. Is conducted to avoid giving rise to reporting duty under the FIC Act.

d. 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; or

(iii) The business has been used or is about to be used in any way for money laundering purposes.

(iv) The business shall examine high risk transactions in at least the manner described herein. The way unusual patterns of transaction which have no apparent business or lawful purpose are examined may include:

a) Having regard to prescribed reports relating to suspicious transactions and terror financing that were considered by AMLCO or filed with the FIC.

b) Having regard as to whether the transaction was concluded for purposes of purchase of Uzumba Products.

c) By comparing the values of previous transactions concluded by a client against values of current transactions where the values are obviously larger.

26.6. How to detect an STR

(i) The Compliance Officer will monitor the client's transaction to see if there is anything unusual or suspicious.

(ii) The Compliance must refer to the information gathered to profile clients to assist in the identification of proceeds of crime or transactions that are reportable to the FIC.

26.7. Internal procedure for reporting STRs

(i) If any employee of Uzumba becomes aware of a transaction that is suspicious or unusual, such employee will contact the Compliance Officer to discuss the transaction or any internal party involved.

(ii) The Compliance Officer will, after examining the transaction, exercise his discretion to decide whether to continue with the report or not.

(iii) If after some consideration the Compliance Officer finds the transaction reportable, the Compliance Officer will report such transaction accordingly.

(iv) In an instance where the Compliance Officer decides not to report a transaction, they must document the reasons why the transaction was not reported.

26.8. <u>How to file a report to the FIC</u>

(i) All reports must be filed electronically on the goAML EE section of the FIC's website www.fic.gov.za.

(ii) The Compliance Officer will login with their username and password at the FIC's website,

(iii) Go to Reports and select the relevant report type and provide the required information.

(iv) If the Compliance Officer is unsure as to how to complete the report, they must contact the FIC's at 0860 342 342 for assistance by Call Centre Agent.

27. Dealing with additional requests subsequent to the reports

27.1. A reporter who submitted a report in terms of section 28, section 29 or section 31 may be requested by:

(i) The FIC; or

(ii) An investigating authority acting with the permission of the FIC or under the authority of an authorized officer, to provide the FIC or the investigating authority with such additional information concerning the report and the grounds for the report as they may reasonably require performing their functions.

(iii) The Compliance Officer will furnish the requested information in the Uzumba' s position to the requesting authority as soon as possible but not later than 5 working days, upon receipt of such request. If for some reason, the requested information is not available. The Compliance Officer will notify the requesting authority accordingly.

28. Ongoing monitoring

28.1. The Business must compare each Transaction under a Business Relationship against the information provided by the Client in the Questionnaire pertaining to the –

(i) Nature of the Business Relationship; and

(ii) The purpose of the Business Relationship; and

(iii) The source of the funds that will finance the Business Relationship and must update such information and any other documents originally forming part of the CDD in respect of that Client where necessary.

28.2. Whenever fulfilling the duty described above, the Business must simultaneously consider whether the Transaction that necessitated the information update is reportable.

28.3.

29. Enhanced Due Diligence

29.1.1. The business will screen all suppliers of precious metals and transactions against the lists of persons, entities or countries issued by the government or any competent authority. Uzumba currently does this on an ongoing basis as new list is published by FIC.

30. Keeping records of written findings

30.1. For the examinations referred to above, the business shall document and keep its written findings, which may be achieved by filing the appropriate records used for the examination in a suitable manner for future purposes.

30.2. Where the findings confirm any suspicion of money laundering or terror financing activities, the relevant prescribed report shall be filed with the FIC by the business.

31. Section 43 - Training Processes

31.1. One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering and terrorist financing, and who are well trained in the identification of unusual activities or transactions which may prove to be suspicious.

(i) Uzumba' s policy regarding training is as follows:

a) No new staff member will be allowed to engage with clients before they receive FICA compliance training.

b) All staff members who were employed before this policy became operational must receive Training within 14 days.

c) All Sales persons, Administration Managers and anyone who have access to any transaction upon which FICA provisions applies.

d) Uzumba' s will provide refresher training to staff members as and when required or as and when the legislative requirements change.

e) Uzumba will require a training provider to verbally assess the competency of the staff to re-enforce compliance requirements, measures and processes.

f) Uzumba' s will ensure that an attendance register is signed by all attendees and kept in the Business.

32. Section 42A - Appointment and responsibilities of an AML Compliance Officer

32.1. Uzumba, the company will have Busisiwe Charity Ngwenya as the AML Compliance Officer

32.2. Her responsibilities and accountabilities are as follows:

(i) To ensure that the business and its employees comply with FICA provisions of and this RCMP, related company policies, procedures and directives regarding the FIC Act are implemented with priority.

(ii) Ensure that all prescribed reports are filed timeously with the FIC.

(iii) Ensure that all prescribed requests (s27 and s32), directives, interventions (s34) and monitoring orders (s35) received from the FIC are addressed timeously or implemented as soon as is practicable (as the case may be).

(iv) Ensure that all relevant employees receive ongoing prescribed FICA training as soon as is practicable and in line with those provisions that are relevant to the functions they perform.

(v) Ensure that all relevant employees undergo voluntary refresher training.

(vi) Maintain accurate records (including supporting documentation) relating to prescribed reports. These records shall also provide for reasons why reports were not submitted to the FIC.

(vii) Identify areas of risk in relation to money laundering and terror financing and to escalate the risks concerned to the business's Compliance.

(viii) Amend the business's registration particulars and the details of the AMLCO and MLRO as and when required to do so.

(ix) Ensure that the FIC is notified in writing within ninety (90) days after making any change(s) to the business's prescribed registration particulars that were previously furnished to the FIC.

(x) Notify the FIC without delay of the change of particulars of a third party appointed to keep its records.

(xi) Closely monitor the goAML Message Board and ensure that the appropriate actions are taken by the business.

(xii) Ensure that the reporting obligations including the remediation and successful resubmission of any prescribed reports, especially CTRs and CTRAs, are attended to within the prescribed periods.

(xiii) Review and investigate all Founding Reports, investigate the merits thereof and submit, if necessary, file the prescribed report concerned with the FIC within the prescribed periods.

(xiv) Remain independent and maintain an unfettered discretion to ultimately decide on whether or not to file a prescribed with the FIC. The AMLCO may engage other employees or management during his/her investigation, however he/she shall not be influenced by any of the afore-going persons in making the ultimate decision to file prescribed reports.

(xv) Monitor and escalate goAML system-related matters that prevent or have the potential to prevent reporting to the FIC IT department.

(xvi) Ensure that appropriate internal disciplinary action is taken against any employee that breaches any FIC requirements or this RMCP.

(xvii) Facilitate and co-ordinate inspections and audits carried out by the FIC, supervisory body and internal audit.

33. Responsibilities and accountabilities of employees

Employees involved in transactions with clients are always to remain vigilant to*:*

(i) Ascertain if transactions or activities are suspicious or unusual.

(ii) Ascertain if transactions or activities are related to terror financing; and Identify within reason persons listed on the UN Sanctions List

(iii) The employees concerned are to report the above transactions or persons to their immediate supervisors or line management to enable the completion of a Founding Report.

(iv) Reasonable steps are to be taken by employees to ensure that the clients who are subject to the possible filing of prescribed reports are not alerted.

(v) Employees are strictly prohibited from providing or offering to provide clients any assistance to enable clients to circumvent any obligation imposed in terms of the FIC Act.

(vi) Clients may, however, be assisted in good faith with alternative solutions that do not amount to a circumvention of the FIC Act, this RMCP or gaming legislation.

(vii) In addition to the above, employees are to seek the advice of their supervisors, management or the AMLCO if they are faced with any unique situations or uncertainty regarding the The business's FICA obligations.

(viii) Employees shall not take unlawful instructions from their supervisors or management to assist clients who do not comply with the FIC Act or the Business

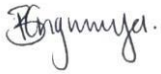
(ix) Retail's RMCP. In such cases, the employee concerned shall report the supervisor or member of management to the AMLCO.

34. Disciplinary steps against staff for failure to adhere to this policy

34.1. Any staff member who has been trained on FICA requirements and this RCMP is compelled to uphold these rules.

34.2. Failure to comply with any of the rules will result in disciplinary actions outlined in the **CODE OF EMPLOYMENT PRACTISE.**

<u>This RMCP has been approved for use at the Uzumba by:</u>

Name	**Designation**	**Signature**
Busisiwe Charity Ngwenya	Director	

ANNEXURE "A"

1. **RISKS BASED ON THE SECTOR SURVEY AND RESEARCH**

The risk factors used in this Annexure align with those used in the FIC's Guidance Note 7.

1.1.1. Products and services risks

(ii) Certain products and services are regarded as posing a higher risk for money laundering purposes.

(iii) The products and services that we provide that are internationally recognised as more likely to be abused by criminals in the money laundering process include:

(iv) Here's a risk assessment for Krugerrand dealers and dealers in precious stones based on sector survey and research:

1.1.2. High-Risk Factors:

(i) **Money Laundering:** Krugerrand dealers and precious stone dealers are vulnerable to money laundering due to the high value and anonymity of transactions.

(ii) **Terrorist Financing:** Precious stones and gold coins can be used to finance terrorist activities.

(iii) **Illicit Trade**: Smuggling and trading of conflict diamonds, blood diamonds, and other illicit precious stones.

1.1.3. Medium-Risk Factors:

(i) **Customer Due Diligence:** Difficulty verifying customer identity and source of funds.

(ii) **Cash-Based Transactions:** High-risk transactions involving large amounts of cash.

(iii) **Cross-Border Transactions:** Increased risk of money laundering and terrorist financing.

(iv) **Lack of Regulation:** Limited regulatory oversight in some jurisdictions.

(v) **Valuation and Authenticity:** Difficulty verifying authenticity and value of precious stones and Krugerrands.

1.1.4. Low-Risk Factors:

(i) Established Businesses: Well-established dealers with strong reputations.

(ii) Regulatory Compliance: Dealers adhering to anti-money laundering (AML) and know-your-customer (KYC) regulations.

(iii) Transparent Transactions: Use of traceable payment methods.

1.1.5. Mitigation Strategies:

(i) Enhanced Customer Due Diligence.

(ii) Regular Training for Staff.

(iii) Implementation of AML/KYC Policies.

(iv) Use of Technology for Transaction Monitoring.

(v) Regular Audits and Compliance Checks.

1.1.6. Relevant Regulations:

(i) Financial Intelligence Centre Act (FICA)
(ii) Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) regulations.
(iii) Precious Metals and Precious Stones Act
(iv) Kimberley Process Certification Scheme (KPCS) for diamond trade.

1.1.7. Industry Best Practices:

(i) Membership with industry associations (e.g., South African Diamond and Precious Metals Regulator).
(ii) Adherence to international standards (e.g., World Diamond Council).
(iii) Regular risk assessments and compliance audits.

1.1.8. Risk-based approach: Treatment of risk

1.1.8.1. The business has the following controls in place:

(i) Processes,

(ii) systems,

(iii) resources,

(iv) monitoring,

(v) reporting, and

(vi) training etc.

1.1.8.2. The control must be in proportion to the risk i.e.

a) Higher money laundering and terrorist financing risk – enhanced due diligence
b) Medium risk – standard due diligence
c) Lower money laundering and terrorist financing risk – simplified due diligence.

Risk will be adequately treated – level of residual risk is acceptable and within the risk appetite of the business.

2. **DOMESTIC POLITICALLY EXPOSED PERSONS**

2.1.2. A domestic politically exposed person is an individual who holds, including in an acting position for a period exceeding six months, or has held at any time in the preceding 12 months, in the Republic:

2.1.3. A prominent public function including that of:

2.1.3.1. The President or Deputy President;

2.1.3.2. A Government Minister or Deputy Minister;

2.1.3.3. The Premier of a province;

2.1.3.4. A member of the Executive Council of a province;

2.1.3.5. An Executive Mayor of a municipality elected in terms of the Local Government: Municipal Structures Act, 1998 (Act No. 117 of 1998);

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

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

2.1.3.8. 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);

2.1.3.9. 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);

2.1.3.10. 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);

2.1.3.11. 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);

2.1.3.12. 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);

2.1.3.13. An Ambassador or High Commissioner or other senior representative of a foreign government based in the Republic;

2.1.3.14. An Officer of the South African National Defence Force above the rank of Major-General;

2.2. The position of:

2.2.2. Chairperson of the Board of Directors;

2.2.3. Chairperson of the Audit Committee;

2.2.4. Executive Officer; or

2.2.5. 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; or

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

3. FOREIGN POLITICALLY EXPOSED PERSONS

A foreign politically exposed persons (FPEPs) is an individual who holds, or has held at any time in the preceding 12 months, in any foreign country a prominent public function including that of a:

3.1. Head of State or head of a country or government;

3.2. Member of a foreign royal family;

3.3. Government minister or equivalent senior politician or leader of a political party;

3.4. Senior judicial official;

3.5. Senior executive of a state-owned corporation; or

3.6. High-ranking member of the military.

4. IMMIDIATE FAMILY MEMBERS

Immediate family members of Domestic Prominent Influential Persons and Foreign Prominent Public Officials include, but are not limited to:

4.1. Their spouse, civil partner or life partner;

4.2. Their previous spouse, civil partner or life partner;

4.3. Children and step-children and their spouse, civil partner or life partner;

4.4. Their parents; and

4.5. Siblings or step-siblings and their spouse, civil partner or life partner.

5. LIST OF DOMESTIC POLITICALLY EXPOSED PERSONS

The following people are DPEPs –

1) President or deputy president of South Africa;
2) Cabinet minister or deputy minister;
3) Premier of a province;
4) Member of executive council of a province;
5) Mayor of a municipality;
6) Leader of a political party;
7) Member of a royal family or a senior traditional leader;
8) Head, accounting officer or chief financial officer of a national or provincial department;
9) Manager or chief financial officer of a municipality;
10) Chairperson, chief executive officer, accounting authority, chief financial officer or chief investment officer of a public entity;
11) Prominent judge in the Constitutional Court, Supreme Court of Appeal or the High Court or any equivalent court;
12) Ambassador, high commissioner or senior representative of a foreign country who is based in South Africa;
13) Person occupying any of the following positions, in a company that sells goods or services to the government worth more than R49,999.00–
    i. Chairperson of the board of directors;
    ii. Chairperson of audit committee;
    iii. Executive officer; or
    iv. Chief financial officer.

6. **DEFINATIONS**

In this RMCP, the following words and expressions bear the meanings ascribed to them –

1. **"Business"** means the selling business to which this RMCP applies;
2. **"Business Relationship"** means an arrangement between the Business and a Client that contemplates a series of Transactions over a period of time;
3. **"Cash"** means paper money, coins or traveller's cheques;
4. **"CDD"** means the customer due diligence referred to in section 21 of FICA
5. **"Client"** means a person who has mandated the Business, where –

a) such person or its Counter-Party is likely, in the discretion of the Risk Officer, to transfer Value to the Business; or such person or its Counter-Party has firmly indicated that it would like or is ready to transfer Value to the Business in giving effect to a single Transaction or a Business Relationship, and in any given situation, the determination of who the Client is must be made in accordance to the principles articulated in the general notes at the end of each table below;

6. **"DPEPs"** means a domestic politically exposed person, being any person, or immediate family member or known close associate of a person, listed on page 26 below;
7. **"Employee"** means any person acting as such within the Business (whether as a director, shareholder, member, manager, employee, or contractor), or any other Client facing staff member of the Business;
8. **"FATF"** means the Financial Action Task Force (of which South Africa is a member), an international standard-setting body dedicated to combating MLFT, and headquartered in Paris, France;
9. **"FATF Member State"** means any country listed on the FATF's official website www.fatf-gafi.org
10. **"FIC"** means the Financial Intelligence Centre, a juristic person created under chapter 2 of FICA;
11. **"FICA"** means the Financial Intelligence Centre Act, No 38 of 2001, as amended from time to time;
12. **"FPEPs"** means a Foreign politically Exposed, being a person, or immediate family member or known close associate of a person, who occupies, or within the past 12 (twelve) months occupied, any of the positions listed on page 26 below, in a country other than South Africa;
13. **"Governmental Authority"** means any public authority, and includes (without limitation)

a) The South African Revenue Service; and

b) The Commission for Intellectual Property and Companies; and

c) Any organ of state;

14. **"ID"** means any document issued by a Governmental Authority that describes and identifies a natural person by his or her personal attributes, and which attributes must at least include his

or her (i) forename and middle name (or initials), (ii) surname, (iii) unique identifying number, (iv) date of birth, and (vi) facial image. ID includes any of the following –

a) Green, bar-coded South African identity document;

b) South African identity card;

c) South African passport;

d) South African driver's license; and

e) Foreign passport;

15. **"Legacy Client"** is any person who had a business relationship with the Business before the Implementation Date, and in respect of whom the Business already has customer due diligence information as at the Implementation Date, albeit in terms of the FICA dispensation that applied prior to this RMCP becoming effective;

16. **"List 1267"** means a list published at the URL http://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list on which list appear persons and entities that are under financial sanctions pursuant to resolution 1267 of the United Nations Security Council, and which list is amended from time to time;

17. **"MLFT"** means money laundering and the financing of terrorism, where "money laundering" refers to any practice through which the proceeds of crime are dealt with so as to obscure their illegal origins;

18. **"Prospective Client"** means a person who approaches the Business to enlist the Business' services, but that person or its Counter-Party – is not yet likely, in the discretion of the Risk Officer, to transfer any Value to the Business; or has not yet firmly indicated that it would like or is ready to transfer Value to the Business;

19. **"Representative"** means, for purposes of the Questionnaire, the person who is authorised to complete the Questionnaire and deal with the Business on behalf of the Client;

20. **"Risk Officer"** means – the person within the Business charged with overseeing compliance with FICA and this RMCP; or if no specific person has been so charged, then the Business' highest decision-making organ, all of the members of which shall be jointly responsible for the Business' FICA and RMCP compliance; or if the Business does not have any decision-making organs, then the manager of the Business;

21. **"RMCP"** means the risk management and compliance programme contained in this document, which has been designed in response to the Business' obligations under section 42 of FICA;

22. **"Terrorist Activities"** means any of the offences specified in POCDATARA, all of which relate to terrorism; and

23. **"Transaction"** means a transaction between the Business and the Client under which Value will be transferred between the Business on one hand, and the Client, its Principal or its Representative, its Counter-Party or any other person for the Client's account on the other hand.