LAND AND AGRICULTURAL DEVELOPMENT BANK OF SOUTH AFRICA

ANTI-MONEY LAUNDERING (AML) & COMBATING THE FINANCING OF TERRORISM (CFT) AND SANCTIONS RISK MANAGEMENT AND COMPLIANCE PROGRAM (RMCP)

TABLE OF CONTENTS

1. LIST OF ACRONYMS

No	ACRONYMS	DESCRIPTION AND DEFINITION OF TERMS
1.	AI	Accountable Institution
2.	AML / CFT	Anti-Money Laundering and Combating the Financing of Terrorism.
3.	BUs	Business Units
4.	Board	Board of Directors of the Land Bank
5.	BRA	Business Risk Assessment
6.	CA	Competent Authority
7.	CAC	Credit Adjudication Committee
8.	CCC	Commercial Credit Committee
9.	CDD	Client Due Diligence
10.	CFT	Combatting the Financing of Terrorism
11.	CIC	Credit and Investment Committee
12.	CIV	Client Identification and Verification
13.	CRA	Client Risk Assessment
14.	CRMC	Credit Risk Management Committee
15.	CTR	Cash Threshold Report
16.	EDD	Enhanced Due Diligence
17.	ECC	Executive Credit Committee
18.	EXCO	Executive Committee of the Bank

No	ACRONYMS	DESCRIPTION AND DEFINITION OF TERMS
19.	FATF	Financial Action Task Force
20.	FIC	Financial Intelligence Centre
21.	FICA	Financial Intelligence Centre Act, 38 of 2001, as amended and read with the Financial Intelligence Centre Amendment Act (No 11 of 2008)
22.	KYC	Know Your Client
23.	MLCO	Anti-Money Laundering Compliance Officer
24.	Bank	The Land and Agricultural Development Bank of SA
25.	ML / TF	Money Laundering and Terrorist Financing
26.	ODD	On-going Due Diligence
27.	PEP	Politically Exposed Person
28.	PFMA	Public Finance Management Act
29.	DPIP	Domestic Prominent Influential Person
30.	FPPO	Foreign Prominent Public Official
31.	POCA	Prevention of Organised Crime Act, 121 of 1998
32.	POCDATARA	Protection of Constitutional Democracy Against Terrorist and Related Activities Act, No. 33 of 2004.
33.	PRECCA	Prevention and Combating of Corrupt Activities Act, 12 of 2004, as amended
34.	PCC	Provincial Credit Committee
35.	RBA	Risk Based Approach
36.	RGC	Risk and Governance Committee
37.	RMCP	Risk Management and Compliance Programme

No	ACRONYMS	DESCRIPTION AND DEFINITION OF TERMS
38.	SEC	Social and Ethics Committee
39.	STR	Suspicious Transaction Report
40.	TPR	Terrorist Property Report
41.	UBO	Ultimate Beneficial Owner
42.	UNSCR	United Nations Security Council Resolution
43.	RCC	Regional Credit Committee
43.	SAR	Suspicious Activity Report
44.	STR	Suspicious Transaction Report

Note: If a term is referred to more than three times in a document, the acronym is used instead of the full term.

2. GLOSSARY OF TERMS

No.	TERMS	DESCRIPTION
1.	Accountable Institution	Is defined as a person referred to in Schedule 1 of the FIC Act or similarly designated in terms of equivalent legislation in any other country outside South Africa. Thus, a person or organisation that carries on the business of any entity listed in Schedule 1 of the Act would be regarded as an accountable institution. Alternatively, is any person or entity as described in Schedule 1 of the Financial Intelligence Centre Act No. 38 of 2001 who must ensure adherence to the legal requirements and responsibilities as set out therein.
2.	Primary Accountable Institution and Secondary Accountable Institution	An accountable institution can be split into two distinct categories: • Primary Accountable Institution: These institutions are responsible for verifying and keeping record of the identities of their clientele. • Secondary Accountable Institutions: These institutions rely on the adherence of the Primary Accountable Institutions and as such, are not required to verify the identities of the Primary Accountable Institution's clients.
3.	Act	Financial Intelligence Centre Act No. 38 of 2001 (also known as "FICA"), as amended from time to time
4.	Business Relationship	An arrangement between a client and an accountable institution for the purpose of concluding transactions regularly.
5.	Business Units	Comprises all of Land Bank's operations and functions as follows (a) Divisions, (b) Departments and (c) Business Units
6.	Client	A natural person or legal person / entity that enters into a business relationship or concludes a single transaction with an accountable institution in terms of which the accountable institution provides a financial product or service.
7.	Cash	Cash is defined in section 1 of the FIC Act as: a) 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; and b) Travellers' cheques. Cash does not include bearer negotiable instruments as defined in the FIC Act. It also does not include a transfer of funds by
		means of bank cheque, bank draft, electronic funds transfer, wire transfer or other written order that does not involve the physical transfer of cash. These methods of transferring funds are not regarded as cash and are therefore not reportable under section 28 of the FIC Act. Other examples of Cash Equivalents include Treasury bills, Treasury notes, Commercial Paper, Certificates of deposits, money market funds are also excluded from the definition of Cash

No.	TERMS	DESCRIPTION
8.	Client Due Diligence	is the identification and verification of client information to enable an accountable institution to assess client ML / TF risk
9.	Competent Authority	is a public authority with designated responsibilities for combating ML / TF and that has the authority to issue financial sanctions against natural persons, groups, legal person/entity and/or countries to prevent and suppress terrorism and ML / TF
10.	Risk Management and Compliance Programme (RMCP	means the programme contemplated in section 42(1). An accountable institution must develop, document, maintain and implement a programme for anti-money laundering and counter-terrorist financing risk management and compliance. A Risk Management and Compliance Programme must— (a) enable the accountable institution to— (i) identify; (ii) assess; (iii) monitor; (iv)mitigate, and (v) manage, the risk that the provision by the accountable institution of products or services may involve or facilitate money laundering activities or the financing of terrorist and related activities;
11.	Risk (as per FIC Guideline 7)	According to international best practice risk rating methodology, risk refers to the likelihood and impact of uncertain events on set objectives. The impact can be either a positive or negative deviation from what is expected. This uncertainty is a function of three factors: threat, vulnerability and consequence
12.	Inherent and residual risks	Inherent risk is the risk of an event or circumstance that exists before controls or mitigation measures are applied by the accountable institution. Residual risk is the level of risk that remains after controls and mitigation measures were implemented by the accountable institution.
13.	ML/TF risk management (as per FIC Guideline 7)	ML/TF risk management is a process that includes the identification of ML/TF risks, the assessment of these risks, and the development of methods to manage and mitigate the risks that have been identified.
		According to ISO 31000: 2018 (International Organization for Standardization), risk may be managed or dealt with, as follows: • Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; • Accepting or increasing the risk in order to pursue an opportunity; • Removing the risk source; • Changing the likelihood; • Changing the consequences; • Sharing the risk with another party or parties (including contracts and risk financing); • Retaining the risk by informed decision.
14.	Risk-rating	implies assigning different categories to different levels of risk according to a risk scale and classifying the ML/TF risks pertaining to different relationships or client engagements in terms of the assigned categories.

No.	TERMS	DESCRIPTION
15.	Domestic Prominent Influential 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 South Africa, a prominent public function as listed in Schedule 3A of the FIC Act. A prominent public function 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); 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);

No.	TERMS	DESCRIPTION
		(vii) 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); (viii) 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); (ix) 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 M--management Act, 1999 (Act No. 1 of 1999); or (x) 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); (xi) 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); (xii) an ambassador or high commissioner or other senior representative of a foreign government based in the Republic; (xiii) an officer of the South African National Defence Force above the rank of major general; (b) the position of—(i) chairperson of the board of directors; (ii) chairperson of the audit committee; (iii) executive officer; or (xiv) 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 (c) the position of head, or other executive directly accountable to that head, of an international organisation based in the Republic If the Bank engages to establish a business relationship, or the beneficial owner of that prospective client who is a Domestic Prominent Influential Person, the Bank must— (a) obtain EXCO and/or Board approval for establishing the business relationship; (b) take reasonable measures to establish the source of wealth and source of funds of the client; and (c) conduct enhanced ongoing monitoring of the business relationship.
16.	Employee	Is Temporary employees or secondees; Fixed term contractors; Independent Contractors; and / or other person acting on behalf of such accountable institution.

No.	TERMS	DESCRIPTION
17.	Exposure	An act or omission whereby an accountable institution has not met its statutory, supervisory and regulatory requirements which has led to a risk event.
18.	Non-compliance	means any act or omission that constitutes a failure to comply with a provision of this Act or any order, determination, or directive made in terms of the FICA and which does not constitute an offence in terms of this Act, and 'fails to comply', 'failure to comply', noncompliant and 'not complying' have a corresponding meaning
19.	Enhanced Due Diligence	An increased due diligence performed by an accountable institution on clients that pose a greater risk from a ML / TF perspective.
20.	Financial Intelligence Centre	The Financial Intelligence Centre is South Africa's national centre for gathering, analysis and dissemination of financial intelligence. It was established to identify proceeds of crime, combat money laundering and the financing of terrorism and, in so doing, has a primary role to protect the integrity of South Africa's financial system. For the purposes of abbreviation, it is also referred to as "FIC
21.	Foreign Prominent Public Official	A (FPPO) is an individual who holds, or has held at any time in the preceding 12 months, in a foreign country a prominent public function as listed in Schedule 3B of the FIC Act Alternately, a foreign prominent public official 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— (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. If the Bank engages to establish a business relationship, or the beneficial owner of that prospective client who is a foreign prominent public official, the Bank must— (a) obtain EXCO approval and/or Board for establishing the business relationship; (b) take reasonable measures to establish the source of wealth and source of funds of the client; and (c) conduct enhanced ongoing monitoring of the business relationship.
22.	Financial Action Task Force:	The Financial Action Task Force is an intergovernmental organization founded in 1989 on the initiative of the G7 to develop policies to combat money laundering. In 2001, its mandate was expanded to include terrorism financing. For the purposes of abbreviation, it is also referred to as "FATF".

No.	TERMS	DESCRIPTION
23.	Legal Person / Entity	Is a local or foreign legal person / entity (whether incorporated or not) and includes: • South African Companies (Private, Public and Listed); • Close Corporations; • Trusts; • Foreign Companies. • Other legal person / entity • Entities created by specific legislation or other founding documents e.g. a constitution and include: • Partnerships; • Deceased Estates; • Curatorship / Liquidation and Sequestrations; • Pension Schemes / Pension and Provident Funds; • Organs of State; • Non-Profit Organisations (NPOs); • Non-Government Organisations (NGOs); and • Informal Bodies (e.g. Schools, Clubs, Stokvels).
24.	Politically Exposed Person	Is a natural person who is or has in the past held a prominent public function If the Bank engages to establish a business relationship, or the beneficial owner of that prospective client who is a Politically Exposed Person, the Bank must— (a) obtain EXCO approval and/or Board approval for establishing the business relationship; (b) take reasonable measures to establish the source of wealth and source of funds of the client; and (c) conduct enhanced ongoing monitoring of the business relationship.
25.	Natural Person	A human being, as opposed to a legal person / entity.
26.	Related Party	A related party is someone who is connected to the primary client, e.g. • A mandated official; • A member of a close corporation; • Parent or guardian of a minor; • Director of a company; • A surety / guarantor; • a named beneficiary at the time of client take on or at pay - out stage of a defined product; • Founder / donor / beneficiaries / trustees; • Beneficiaries / members of community entities and charities etc.; • Persons duly authorised to establish a relationship on behalf of the client or act on behalf of a client with the Bank, or who are the UBO in the entity and/or will derive benefit from the entity, and

No.	TERMS	DESCRIPTION
		• A legal person / entity or natural person who holds 25% or more shareholding / voting rights in such legal person / entity.
27.	Sanctions	Are restrictive measures imposed by a competent authority against natural persons (individuals), groups (are inclusive of terrorist groups, religious groups, financial groups, etc.), legal persons / entities, and / or countries to prevent and suppress terrorism and terrorist financing.
28.	Senior Management	In this context of this document, it means Executive Committee of the Bank
29.	Terrorism Financing [TF]	Includes the financing of terrorist acts and of terrorists and terrorist organisations (FATF 2001/2010). Consequently, terrorist financing offences relate to any person who wilfully provides or collects funds with the unlawful intention (or in the knowledge) that they are to be used by terrorist organizations to carry out an attack.
30.	Transaction	A transaction between an AI and a client: • Concluded in the course of a business relationship; or • Other than a transaction concluded in the course of a business relationship (once off / single transaction) e.g. the disposal of assets (vehicles, furniture etc.) sold to third parties.
31.	Trust	Means a trust defined in section 1 of the Trust Property Control Act, 1988 (Act No. 57 of 1988), other than a trust established— (a) by virtue of a testamentary disposition; (b) by virtue of a court order; (c) in respect of persons under curatorship; or (d) 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;

No.	TERMS	DESCRIPTION
32.	Money Laundering	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. defined in line with sections 4, 5 and 6 of the Prevention of Organised Crime Act (POCA) - Any person who knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and - (a) enters into any agreement or engages in any arrangement or transaction with anyone in connection with that property, whether such agreement, arrangement or transaction is legally enforceable or not; or (b) performs any other act in connection with such property, whether it is performed independently or in concert with any other person, which has or is likely to have the effect- (i) of concealing or disguising the nature, source, location, disposition or movement of the said property or its ownership or any interest which anyone may have in respect thereof; or (ii) of enabling or assisting any person who has committed or commits an offence, whether in the Republic or elsewhere- (aa) to avoid prosecution; or (bb) to remove or diminish any property acquired directly, or indirectly, as a result of the commission of an offence, shall be guilty of an offence. Assisting another to benefit from proceeds of unlawful activities . Any person who knows or ought reasonably to have known that another person has obtained the proceeds of unlawful activities, and who enters into any agreement with anyone or engages in any arrangement or transaction whereby- (a) the retention or the control by or on behalf of the said other person of the proceeds of unlawful activities is facilitated; or (b) the said proceeds of unlawful activities are used to make funds available to the said other person or to acquire property on his or her behalf or to benefit him or her in any other way, shall be guilty of an offence. Acquisition, possession or use of proceeds of unlawful activities 6. Any person who- (a) acquires; (b) uses; or (c) has possession of, property and who knows or ought reasonably to have known that it is or forms part of the proceeds of unlawful activities of another person, shall be guilty of an offence.".
33.	Money Laundering Compliance Officer	Is responsible for the oversight of the institution's anti-money laundering activities and is the key person in the implementation of the anti-money laundering strategy of the institution

No.	TERMS	DESCRIPTION
34.	On-going Due Diligence	Is the periodic review of the client to ensure that the identification and verification information relating to the client is still current and relevant Alternatively, ongoing due diligence in respect of a business relationship which includes— (a) monitoring of transactions undertaken throughout the course of the relationship, including, where necessary— (i) the source of funds, to ensure that the transactions are consistent with the accountable institution's knowledge of the client and the client's business and risk profile; and (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 (b) keeping information obtained for the purpose of establishing and verifying the identities of clients pursuant to sections 21, 21A and 21B of FICA
35.	Offence relating to the financing of terrorist and related activities	Means an offence under section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004)
36.	Ultimate Beneficial Owner	Is the natural person(s) who ultimately owns or controls a client and includes those persons who exercise ultimate effective control over the management of a legal person / entity or arrangement

3. PURPOSE OF RISK MANAGEMENT & COMPLIANCE PROGRAMME

3.1 The purpose of the Risk Management & Compliance Programme (RMCP) as contained herein is to formally document the Bank's commitment to compliance with the Financial Intelligence Centre Act of South Africa (FICA) as amended from time to time as well as compliance with the requirements of any associated Anti-Money Laundering and Counter-Terrorism Financing legislation;

3.2 Section 42 (2B) states that the board of directors, senior management or other person or group of persons exercising the highest level of authority in an accountable institution must approve the Risk Management and Compliance Programme (CRMP) of the institution, as such in a case of the Bank, the highest level of authority is the Board.

4. APPLICATION OF THE RISK MANAGEMENT & COMPLIANCE PROGRAMME

4.1 This Risk Management & Compliance Programme is applicable to the Bank and its employees.

5. BACKGROUND TO A NEED FOR RMCP

5.1 The Land Bank is a Specialist Agricultural Development Finance Institution (DFI) addressing agricultural and rural development in South Africa and the Bank plays a crucial role in helping South Africa to realize its development imperatives. The vision of the Land Bank is to be a fully integrated agricultural DFI that promotes,

facilitates and supports agricultural and rural development. Part of the Bank's mission is to promote and facilitate access to ownership of land by the historically disadvantaged, increase levels of productive agricultural land use, assisting emerging farmers with finance and technical support and finance commercial farmers.

5.2 As part of execution of its mandate in line with the Land Bank Act, the Bank enters into business relationships and concludes business transactions that require compliance to principles of all anti-money laundering / combating the financing of terrorism (AML/CFT) as found in the FICA, POCA and POCDATARA.

5.3 Section 4 of the POCA criminalised money laundering in South Africa, while terrorist financing was criminalised in terms of the POCDATARA. The Financial Intelligence Centre Act (FICA) was adopted in South Africa in order to implement all anti-money laundering / combating the financing of terrorism (AML/CFT) measures.

5.4 The Land Bank is not listed explicitly like other accountable institutions in schedule I, which are institutions that must fully comply with FICA or reporting institutions in schedule 3 of FICA. The Land Bank is an accountable institution as envisaged in item 4 and item 11 of schedule I of FICA. Item 4 includes all authorised users of an Exchange as defined in the Securities Services Act, No 36 of 2004. Item I includes all lenders of money against the securities of securities. Further, the compliance requirement is derived or implied from section 50(b) (ii) of National Credit Act. Bank Insurance Companies (Subsidiaries) will have to comply with FICA, as it is a requirement of the Financial Advisory and Intermediary Services Act, 37 of 2002. All the above clearly indicate that Land Bank has to ensure full compliance with FICA.

5.5 Land Bank is committed to sustaining a secure and robust financial system by being aware of its responsibilities cognisant of global and local efforts to manage risks arising from AML / CFT & Sanctions and considers the requirements of FICA, POCDATARA, PRECCA and POCA;

5.6 The RMCP has been developed by considering best practices such as the FATF recommendations and standards as well as considering the requirements of the Land and Agricultural Development Bank Act of 2002 (LBA), Public Finance Management Act (PFMA) of 1999, Treasury Regulations (TR) and the King Report on Corporate Governance.

5.7 FICA requires the Bank to:

5.7.1 identify and verify clients and other persons associated with client-client due diligence;

5.7.2 keep records of business relationships and transactions;

5.7.3 report suspicious and unusual transactions and activity to the FIC;

5.7.4 report cash transactions above R49 999.99 to the FIC;

5.7.5 report property associated with terrorist and related activities to the FIC;

5.7.6 formulate and implement a risk management and compliance programme;

5.7.7 train employees of principles of FIC and CRMP;

5.7.8 appoint a person responsible to ensure compliance - the MLCO

5.7.9 ensure ongoing adherence to and monitoring of AML and CFT policies, processes, practices procedures and plans; and

5.7.10 register itself and all its accountable and reporting institutions.

5.8 POCDATARA expands the reporting requirements in POCA and FICA to include, the reporting of:

5.8.1 terrorist financing and related activities;

5.8.2 property, which is connected to an offence relating to the financing of terrorist and related activities; and

5.8.3 designated individuals and entities.

5.9 PRECCA creates the offenses relating to corruption and corrupt activities in South Africa and includes, inter alia, the following:

5.9.1 Provides for the strengthening of measures to prevent and combat corruption and corrupt activities; and

5.9.2 Provides for investigative measures in respect of corruption and related activities.

5.10 POCA creates the offences relating to money laundering in SA and include:

5.10.1 the activity of money laundering;

5.10.2 assisting another to benefit from proceeds of unlawful activities; and

5.10.3 acquisition, use or possession of the proceeds of unlawful activities of another.

6. OBJECTIVES OF RMCP FOR LAND BANK

6.1 Overall objectives for an RMCP are to ensure that:

6.1.1 All necessary client information is obtained, verified and recorded during the establishment of a business relationship with clients. All necessary client information and records are retained and stored for the prescribed period.

6.1.2 All transactions deemed suspicious or unusual and all legally prescribed transactions are reported within the prescribed time period (on time) to the appropriate authorities.

6.1.3 All transactions deemed to have a link to property associated with terrorism and or related activities are reported within the prescribed time period (on time) to the appropriate authorities.

6.1.4 Compliance with the FICA requirements together with the attendant Money Laundering Control Regulations.

6.2 The intention is to provide a framework within which the acceptance, maintenance and monitoring of business relationships and transactions with clients, suppliers and employees are managed by the Bank. This framework sets out the expectations and defines the principles that the Bank is expected to implement in order to mitigate the operational, regulatory and reputational risks associated with AML/CFT and Sanctions.

6.3 This RMCP provides information and guidance on the following key areas:

6.3.1 Governance

6.3.2 Client Identification and Verification

6.3.3 Risk Based approach

6.3.4 Client Due Diligence

6.3.5 Enhanced Due Diligence

6.3.6 Ongoing Due Diligence

6.3.7 AML Screening (PEP/DPIP/FPPO/Sanctioned/Adverse Media)

6.3.8 Client exit and Preventing re entry

6.3.9 Record keeping and management

6.3.10 Reporting obligation

6.3.11 Training and Awareness

7. GROUP APPROACH TO AML/CFT AND SANCTIONS MONITORING

7.1 Land Bank as a group prescribes to the philosophy and approach to AML/CFT and Sanctions compliance as outlined in this RMCP. Land Bank Life Insurance Company (SOC) Limited (LBLIC) and Land Bank Insurance (SOC) Limited (LBIC), referred herein as "Land Bank Insurance" or LBI to refer to both LBIC and LBLIC, are subsidiaries of the Land Bank.

7.2 LBLIC and LBIC are wholly owned subsidiaries of the Land Bank. LBIC and LBLIC offer short term and long-term insurance and risk solutions respectively to the agricultural sector. LBIC and LBLIC have their own AML/CFT and Sanctions Framework that has been approved by the LBIC and LBLIC Board.

7.3 However, the LBLIC, and LBIC, have developed a more specific AML/CFT and Sanctions Framework for these subsidiaries due to the different business complexities, two different balance sheets and capital structures. For prudency and transparency, the combined assurance model assists the two entities to get a holistic view of risk controls and reporting .

7.4 In line with Board Notice 158 of 2014 published by the insurance industry regulator, the Financial Services Board (now Financial Sector Conduct Authority -(FSCA), the risk management policies are in place to deal with Enterprise Risk Management (including AML/CFT and Sanctions) in both LBIC and LBLIC.

8. RMCP

8.1 Accountable Institutions are expected to adopt a written RMCP that is reasonably designed to ensure proper recordkeeping and reporting of certain transactions, and to prevent the business from being used to launder money. The RMCP must include, at a minimum, the following:

`8.1.1. Adoption of a written AML/CFT and Sanctions RMCP with internal policies, procedures and controls for:

- Verifying client identification;
- Report transactions as required by regulations;
- Creating and retaining records of business relationships and single transactions;
- Responding to law enforcement requests;
- Licensing requirements;
- Compliance with local regulatory requirements;
- Employee training.

8.1.2. The designation of a MLCO who is responsible for assuring that:

- Policies and procedures are followed;
- Procedures are updated as needed;
- Training and education are provided;
- Reports are properly filed as required by your local regulations;
- A periodic review is conducted to verify the effectiveness of the RMCP;

8.1.3 Ensuring both Land Bank requirements and local regulations are followed;

8.1.4 Updating the RMCP as necessary due to changes in laws or regulations.

8.1.5 An ongoing employee training programme that:

8.1.5.1 Explains policies and procedures;

8.1.5.2 Teaches how to identify suspicious activity.

8.1.6 A Periodic Review of the RMCP:

8.1.6.1 The review should take place as needed and be as thorough as needed based on the risks specific to the Bank and the requirements of the local regulations.

8.1.6.2 The person identified as qualified per the local regulations must conduct the review. If none is specified, the review may be performed by internal employees, but cannot be performed by your MLCO.

9. STATEMENT OF COMMITMENT TO COMPLIANCE

9.1 The RMCP provides general guidance to Land Bank and its subsidiary employees on complying with FICA.

9.2 The Land Bank strives to comply with the letter and spirit of all legislation, statutes, sub-ordinate legislation, regulation, guidance note, directives and supervisory requirements that apply to its business. Land Bank and all its employees are committed to ensure compliance with FICA, PRECCA, POCA and POCDATARA.

9.3 To this end, the Land Bank shall implement all reasonable measures required under FICA in ensuring that at all times and as far as is reasonably possible that the bank:

9.3.1 positively identifies its clients and their representatives;

9.3.2 maintains appropriate records of client and transaction details; timeously reports to the FIC all transactions as prescribed by FICA;

9.3.3 educates its staff as to the nature and effect of the legislation;

9.3.4 regularly trains its staff on the policy, rules, systems and procedures necessary to ensure compliance;

9.3.5 has in place appropriate reporting and communication lines to ensure compliance;

9.3.6 processes to maintain communications with respective Regulatory bodies;

9.3.7 has its registration with FIC is in order as prescribed, will notify the FIC in writing of any changes to the particulars furnished to the FIC within 90 days after such a change, and

9.3.8 appoints a MLCO responsible for AML/CFT and Sanctions Compliance.

9.4 Land Bank is committed to establishing and maintaining an internal culture of awareness and vigilance with respect to money laundering and to this end shall endeavour to co-operate with all similarly committed parties, public and private.

9.5 The Bank will make documentation describing this RMCP available to each of its employees involved in transactions to which the Act applies.

9.6 The Bank will, on request, make a copy of this RMCP available to the FIC; or any other supervisory body which performs regulatory or supervisory functions in respect of the Bank.

9.7 The Boards will ensure compliance with the provisions of the Act and the RMCP.

9.8 The compliance function of the Bank will assist the Boards in discharging their obligations under the Act and the RMCP will assign persons with sufficient competence and seniority to ensure the effectiveness of the RMCP and compliance by the employees of the Bank with the provisions of the Act and the RMCP.

9.9 This RMCP will be reviewed biennially or as and when applicable legislation is amended or business operations demand from time to time.

10. AML OVERVIEW

10.1 What Is Money Laundering?

10.1.1 Money laundering is the attempt to conceal or disguise the nature, location, source, ownership, control or movement of illegally obtained money. Money laundering is illegal.

10.1.2 There are three stages to Money Laundering:

Placement, Layering, and Integration

10.1.2.1 The first-time funds derived from criminal activities are used in a legitimate money transfer is referred to as **Placement.** An example of this would be splitting a large portion of cash into smaller sums and thereafter depositing the smaller amounts into a bank account, or purchasing a series of monetary instruments (cheques, money orders, etc.) with the smaller amounts.

10.1.2.2 Creating a series of transactions or movements to hide the first transaction is referred to as **Layering (**sometimes referred to as **structuring)**. The purpose is to cloud the trail of the funds and separate them from their illegitimate source. The funds might be channelled through various means for example; the purchase and sale of investment instruments, purchasing property and selling it soon after, or the launderer might simply wire the funds through a series of accounts at various banks across the globe.

10.1.2.3 The return of funds to legitimate activities is referred to as **Integration**. This generally ensues the successful stages of placement and layering. The launderer at this stage causes the funds to re-enter the economy and appear to be legitimate. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

10.1.3 Although use of all three stages is common, it is not always utilised by the criminal who wishes to launder funds. In some instances, criminals may choose to merely 'place' the illegally derived funds into the economy by merely depositing the money into his or her bank account, without any layering occurring. They can withdraw the money and spend it at their will.

10.2 What is terror financing?

10.2.1 Financing of terrorism is the collection or provision of funds for the purpose of enhancing the ability of an entity or anyone who is involved in terrorism or related activities to commit an act that is regarded as a terrorist act. Funds may be raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

10.3 What is the Financial Action Task Force (FATF)?

10.3.1 The FATF is an inter-governmental policy making body, comprised of over 30 countries, that has a ministerial mandate to establish international standards for combating money laundering and terrorist financing. Several jurisdictions have joined the FATF or a FATF-style regional body, and have committed at the ministerial level to implementing the FATF standards and having their anti-money laundering and combating of terror financing (AML/CFT) systems assessed. Within Africa, the Eastern

and Southern African Anti-Money Laundering Group (ESAAMLG) was established to serve as a FATF style regional body for Eastern and Southern African countries.

10.4 What does the FATF do?

10.4.1 Sets international standards to combat money laundering and terrorist financing;

10.4.2 Assesses its members' compliance with the FATF standards through a peer review process of mutual evaluations; and

10.4.3 Conducts typologies studies of money laundering and terrorist financing methods, trends and techniques;

10.4.4 Internationally promotes the adoption and application of measures to combat money laundering.

10.5 What are the FATF Recommendations?

10.5.1 These are internationally endorsed global standards for implementing effective AML/CFT and Sanctions measures. They increase the transparency of the financial system (making it easier to detect criminal activity) and enable countries to successfully act against money launderers and terrorist financiers.

10.6 What are the benefits of a country implementing the FATF Recommendations?

10.6.1 Secure a more transparent and stable financial system that is more attractive to foreign investors. Corrupt and opaque financial systems are inherently unstable. Excessive money laundering can cause increased volatility of international capital flows and exchange rates, market disparities, and distortions of investment and trade flows.

10.6.2 Ensure that financial institutions are not vulnerable to infiltration or abuse by organised crime groups. Financial institutions that are exploited in this manner are exposed to reputational risk, financial instability, diminished public confidence, threats to safety and soundness, and direct losses.

10.6.3 Build the capacity to fight terrorism and trace terrorist money. Terrorists need money to finance attacks. Tracing this money is one of the few preventive tools that a government has against terrorism.

10.6.4 Meet binding international obligations, and avoid the risk of sanctions or other action by the international community. The international community—through numerous international treaties, United Nations Security Council Resolutions and best practices—has endorsed the FATF Recommendations at the highest political level.

10.6.5 Avoid becoming a haven for criminals. Countries with weak AML/CFT and Sanctions systems are attractive to criminals because they provide an environment in which criminals can enjoy the proceeds of their crimes and finance their illicit activities with little fear of facing punishment.

10.7 Who should report suspicious and unusual transactions?

10.7.1 FICA requires a person who carries on a business, or is in charge of or manages a business, or who is employed by a business, and who has a suspicion of money laundering or terror financing activity or unusual transaction, to report this to the Centre. Your knowledge of the information in this RMCP may help prevent the bank from being victimised by money launderers and assist with complying with the law. In addition, your compliance with these requirements may help law enforcement agents in their efforts to track down and capture terrorists who illegally launder money.

11. CLIENT IDENTIFICATION AND VERIFICATION

11.1 To establish a business relationship with a prospective client, the Bank has to obtain the appropriate information from the person seeking to establish the business relationship or from the person acting on behalf of that prospective client. The information obtained is, where necessary, required to be verified by comparing it with information and/or documentation obtained from source(s) as required by agreed standards.

11.2 For each new business relationship / single transaction, documents must be obtained at pre-approval / servicing stage in compliance with Client Identification Verification ("CIV") requirements and to ascertain the identity of the client that we are dealing with.

11.3 FICA standard forms / checklists are available at the client on boarding stage for the purposes of Know your Client ("KYC") in line with FICA**. [Refer to Appendix 1 for Land Bank's FICA checklists]** These documents should be submitted to the MLCO for conducting client EDD.

11.4 By verifying the client's identity and that of the juristic entity, partnership or trust, the Bank is trying to establish whether such persons / entities are authentic and legitimate, i.e. the Bank is trying to identify who the beneficial owners are of the juristic entities, partnerships or trusts. In terms of Section 21B of FICA, it is mandatory for the Bank to identify and verify all natural and juristic entities including beneficial ownership of the juristic entities.

11.5 FICA further defines beneficial owner, in respect of a legal person, as a natural person who, independently or together with another person, directly or indirectly –

a) owns the legal person; or

b) exercises effective control of the legal person

11.6 Furthermore, identification of clients through the verification process mitigates the Bank's exposure to the risk of money laundering or other illegal or criminal activities that might affect its reputation.

11.7 **NB:** In the verification process of a juristic person, the Bank must ensure that the persons acting on behalf of such entities have the requisite authority to enter into business transactions with the Bank.

12. RISK BASED APPROACH

12.1 A risk-based approach is the assessment of the varying risks associated with different types of clients, transactions, distribution channels, jurisdictions, processes, systems, and activity profile in order to maximise the effectiveness of AML/CFT and Sanctions compliance.

12.2 A risk-based approach has systems and controls that are commensurate with the specific risks of money laundering and terrorist financing. Assessing risk has become one of the most important steps in creating compliance with AML/CFT and Sanctions. Higher money laundering and terrorist financing risks demand stronger controls than warranted by individuals/ entities deemed to be of lower risk. However, all categories of risk, whether low, medium, high must be mitigated by the application of controls.

12.3 A risk-based approach is preferable as opposed to a rules-based approach because it

12.3.1 is more flexible – money laundering and terrorist financing risk varies across clients, products and delivery channels;

12.3.2 is more effective – accountable institutions are equipped to effectively assess and mitigate the particular money laundering and terrorist financing risks they face;

12.3.3 is more proportionate - a risk-based approach promotes a common sense and an intelligent approach to AML/CFT and Sanctions rather than a 'check the box' approach; and

12.3.4 allows firms to minimise the adverse impact of AML/CFT and Sanctions procedures on their legitimate clients.

12.4 The Bank must obtain certain information and verify certain particulars against information and or documentation, which:

12.4.1 can reasonably be expected to achieve such verification

12.4.2 is obtained by reasonably practical means and

12.4.3 which can be considered as being a credible and from a reputable source, considering any guidance notes and public compliance communications concerning verification.

12.5 This means, the Bank must assess what information and/or documentation may be necessary to achieve verification of the particulars and the means by which it may be obtained (e.g. from a third-party source). The Bank must then exercise its judgment and decide what the appropriate balance is between the level of verification and the most practical means to obtain such verification.

12.6 A risk-based approach does not question whether client due diligence ("CDD") will be conducted but determines the extent of the CDD measures that are applied in any given circumstances.

12.7 Reasonable' indicates that in those circumstances a risk-based approach to the verification of the particulars in question may be applied. This implies the greater the risk, the greater the amount of information and the

more advanced and stringent the level of verification required. The balance between the accuracy of the verification required on the one hand, and the level of effort invested in the means to obtain such verification on the other, has to be commensurate with the nature of the risk involved in any given business relationship or transaction.

12.8 Applying a risk-based approach of the relevant particulars implies that the Bank can accurately assess the risk involved. It also implies that the Bank can make an informed decision based on its risk assessment as to the appropriate methods and levels of verification that should be applied in a given circumstance.

12.9 Client Risk Profiling enables the Bank to follow a risk-based approach, where standard due diligence and standard monitoring will be conducted on medium and low risk business relationships while enhanced due diligence and enhanced monitoring will be conducted on high risk business relationships.

12.10 KYC requirements entail obtaining additional client information to assist the Bank to risk profile their clients and apply enhanced due diligence and enhanced monitoring where necessary.

12.11 Client risk profiling is an element of "know your client" (KYC) procedures through which the Bank:

12.11.1 determines the type of activity that is considered 'normal and expected' for a client;

12.11.2 matches a client's behaviour against that of clients with a similar risk profile; 8.10.3 identifies the associated client money laundering and terrorist financing risk; and

12.11.3 monitors that activity to determine if it stays within the client profile.

12.12 The Bank determines the source of funds, source of wealth and expected transactional activity to obtain static information on the client against which the clients' activity can be compared. The source of funds, source of wealth and expected transactional activity are not risk rated or utilised in determining whether the client is rated as, high, medium or low risk.

12.13 Deviations from the profile and anticipated transactions could trigger inquiries and scrutiny of the account. Client risk profiling is of value when certain attributes of client require us to scrutinise the client due to the high risk of money laundering and terrorist financing and determining when enhanced due diligence and enhanced monitoring should be conducted.

12.14 The Bank will conduct pro-active client risk profiling through the client on-boarding process and as well as reactive client risk profiling during the on-going monitoring process using the AML risk profiling system that the Bank will develop. In the interim, a risk profiling spreadsheet will be used by the MLCO to determine the upfront client risk rating. On-going client risk monitoring will be conducted by the Post Investment Management Services (PIMS) department of the Bank. The nature and scope of monitoring by the PIMS department are still to be determined .

12.15 The Bank assesses the risk of a client using the five (5) risk elements and specific risk scoring which determines if a client is high, medium or low risk. This is depicted in **Figure 1** below:

1. Client type	Scoring
Government	0

4. Adverse Media	Scoring
Allegations of wrong doing (Yes)	7

Individual	0
Close Corporation	0
Company	2
Partnership	2
Trust	3
Co-Ops	2

Allegations of wrong doing (No)	0
Regulatory Sanctions (Yes)	8
Regulatory Sanctions (No)	0
Criminal Sanctions (Yes)	8
Criminal Sanctions (No)	0
Administrative Sanctions (Yes)	8
Administrative Sanctions (No)	0

2. PEP Screening	**Scoring**
PEP(Yes)	5
PEP(No)	0
DPIP/FPPO(Yes)	5
DPIP/FPPO(No)	0
Sanctioned (Yes)	8
Sanctioned (No)	0

5. Distribution Channel	**Scoring**
Direct	0
Provincial Network	0
Service Level Partners	2

3. Span of Control/Influence	**Scoring**
Director: Private Company (Yes)	1
Director: Private Company (No)	0
Director: Public Company (Yes)	2
Director: Public Company (No)	0
Director: SOE (Yes)	7
Director: SOE (No)	0
Director/Mayor/Municipal Manager/Executive/Public Office Bearers: National Government (Yes)	7
Director/Mayor/Municipal Manager/Executive Public Office Bearers /: National Government (No)	0
Director/Mayor/Municipal Manager/Executive Public Office Bearers /: Provincial Government (Yes)	7
Director/Mayor/Municipal Manager/Executive/ Public Office Bearers: Provincial Government (No)	0
Director/Mayor/Municipal Manager/Executive Public Office Bearers /: Regional/District (Yes)	5
Director/Mayor/Municipal Manager/Executive Public Office Bearers /: Regional/District (No)	0

Figure 1: Client Risk Scoring – Source: FATF recommendations

NOTE: The numbers used in the scoring above aims to replicate the level of risk (Refer to Table 1 below).

Scores	**Risk**
0-2	**Low**

3-4	**Medium**
5+	**High**

Furthermore, in terms of the FATF recommendations, all clients identified as PEPs and/or have adverse media should be classified as High Risk with EDD that should be considered

12.16 The overall client AML risk score is determined by the following:

Client AML risk rating = [Client Type Score] + [Distribution Channel Score] + [Span of Control] + [Adverse Media Score] + [PEP Screening Score]

12.17 The client AML risk rating will determine the level of AML/CFT risk that the client poses to the Bank. This is depicted in the **Figure 2** below:

Risk Rating	Client risk rating
Low	0 to 1
Medium	2 to 4
High	5 +

Figure 2: Client Risk Rating

12.18 The clients risk rating is reviewed periodically according to the level of risk that the client poses to the Bank. The frequency of review is depicted in **Figure 3** below:

Risk Rating	Frequency of Review
Low	Every 3 years
Medium	Every 2 years
High	Every year

Figure 3: Frequency of Review

12.19 A trigger event that would require a review of a risk classification would include changes to the typologies, legislation and international best practice. Trigger events may also include the following:

- Change in clients address;
- Change in clients banking details;

- Change in juristic entity shareholding, directors, trustees, beneficiaries
- A new transaction/contract by a new or existing client/supplier
- Changes to the PEP/DPIP/FPPO/Adverse media status of the client/supplier

PEP Risk Classification

The Bank further categorises the different type of individuals that are considered to be *Domestic Prominent Influential Person (DPIP),), Foreign Prominent Public Official (FPPO) or Politically Exposed Person (PEP)*. These categorizations would determine the Governance Committee, at which approval to continue with the transaction, would be sought. The categories are depicted in the table below.

PEP/DFIP/FPPO/ DESCRIPTION	CATERGORY OF PEP/DFIP/FPPO	AML RISK CLASSIFICATION
President/Deputy President of South Africa	1	HIGH
Minister/Deputy Minister/Director General : National Government	2	
Minister/Deputy Minister/Director General / : Provincial Government	3	
Members of Parliament	4	
Executive political party official -NEC of Political Party (top 6)	5	
Traditional/Tribal leaders- Kings of Royal Families	6	
South African Ambassadors to Foreign Countries	7	
Directors/Executive Managers - State Owned Companies (Schedule 1 & 2 of the PFMA)	8	MEDIUM
Foreign Politically Exposed Persons	9	
Director/Mayor/Municipal Manager/Executive/Public Office Bearers : Regional/District	10	
Judges (Constitutional Court, Supreme Court)	11	
Traditional/Tribal Leaders- Chiefs	12	
Relative and Close associates of Domestic Prominent Influential Person (DPIP), Foreign Prominent Public Official (FPPO) or Politically Exposed Person (PEP)	13	LOW
Judges-High Court and Magistrates Court	14	
Directors/Executive Managers - State Owned Companies (Schedule 3 of the PFMA)	15	
Note		
1- The above applies to active and inactive PEPs		
2- Spouse and immediate family members of the PEP (including adopted child) will fall in the same classification as the PEP		

Table- PEP risk classification

12.20 A client may generate a high score if the associated party to the client is high. In such instances, the Bank must conduct enhanced due diligence on the client and associated party.

12.21 The Bank has identified a few instances where a client is deemed as high risk, irrespective of the weightings of the factors afforded to that client. Clients deemed automatically high risk include:

- PEP/DPIP/FPPO's (either through the client being listed as a PEP on the PEP lists screened by the Bank

  or as a result of their occupation, nature of business activity/industry or salutation); and/or
- Sanctioned individuals/entities.
- Adverse media

What processes should be in place when dealing with PEP/DPIP/FPPO?

It is crucial that accountable institutions address the issue of PEP/DPIP/FPPO in their risk framework and group money laundering control policy. PEP/DPIP/FPPO should be regarded as high-risk clients and, as a result, enhanced due diligence should be performed on this category of client. Heightened scrutiny has to be applied whenever PEP/DPIP/FPPO or families of PEP/DPIP/FPPO or closely associated persons of the PEP/DPIP/FPPO are the contracting parties or the beneficial owners of the assets concerned, or have power of disposal over assets by virtue of a power of attorney or signature authorisation.

The Wolfsburg principles provide additional guidance on how to recognise and deal with a PEP/DPIP/FPPO. In addition to the standardised identification and verification procedures, the following prompts are appropriate to recognise PEP/DPIP/FPPO:

- The question whether clients or other persons involved in the business relationship perform a political function should form part of the standardised client onboarding process, especially in cases of clients from corruption prone countries;
- Client advisers should deal exclusively with clients from a specific country/region to improve their knowledge and understanding of the political situation in that country/region;
- The issue of PEP/DPIP/FPPO should form part of a banks regular KYC training programs; Banks may use databases listing names of PEP/DPIP/FPPO including their families, closely associated persons and advisors.

12.22 Where a client is rated as high risk, the client EDD template (**Refer to Appendix 2: AML Enhanced Due Diligence)** needs to be completed by the MLCO and the EDD process continues (Refer to EDD process below). The template details what information and documentation needs to be obtained to satisfy the requirements of EDD for that particular high-risk type. Risk rating of a juristic entity would include risk rating the Beneficial Owner.

12.23 The AML risk rating of clients and DD process is depicted in **Figure 4** below:

Risk Rating	Description	Process
Low	These clients pose a low risk to the Bank.	Client Due Diligence (CDD) will be performed by the Risk Function and approved by EXCO for all transactions (e.g. other commercial transactions/suppliers/legal matters with low risk PEPs) in line with the Delegations of Powers Framework except for blended finance transactions. For Blended Finance Transactions with Low Risk PEPs identified, these will be discussed and approved at EXCO. For purposes of turnaround times for these transactions, the relevant credit approval committees, both at management and board levels, may grant a conditional approval of the deal, subject to SEC approving the PEP.
		The relevant approval credit committee must be notified of the outcome of the SEC approval and also notify the RGC
Medium	These clients pose a higher risk to the Bank.	Client Due Diligence (CDD) will be performed by the Risk Function, recommended by EXCO and approved by SEC for all transactions (e.g. other commercial transactions/suppliers/legal matters with medium risk PEPs) in line with the Delegations of Powers Framework except for blended finance transactions. For Blended Finance Transactions with Medium Risk PEPs identified, these will be recommended EXCO and approved by SEC For purposes of turnaround times for these transactions, the relevant credit approval committees, both at management and board levels, may grant a conditional approval of the deal, subject to SEC approving the PEP. The relevant approval credit committee must be notified of the

Risk Rating	Description	Process
		outcome of the SEC approval and also notify the RGC and Board
High	These are clients that pose a significant risk to the Bank. Establishing a business relationship or concluding a single transaction with these clients is not prohibited but may expose the Bank to reputational Risk	Enhanced Due Diligence (EDD) will be performed by the Risk Function, recommended by EXCO and SEC, and approved by Board for all transactions in line with the Delegations of Powers Framework including blended finance transactions and/or adverse media, other commercial transactions/suppliers/legal matters For purposes of turnaround times for in the blended finance transactions, the relevant credit approval committees, both at management and board levels, may grant a conditional approval of the deal, subject to Board approving the PEP. The relevant approval credit committee must be notified of the outcome of the Board approval and also notify the RGC -

Figure 4: AML Risk Rating and DD

13. CLIENT DUE DILLIGENCE (CDD).

13.1 CDD is the measures taken to:

13.1.1 identify and verify the identity of a client using reliable, independent source documents, data or information obtained from the client and stored on the Banks SAP portal.;

13.1.2 understand the purpose and intended nature of the business relationship or transaction;

13.1.3 monitor the client's transactions to ensure they are consistent with the bank's knowledge of that client, their business and risk profile; and

13.1.4 maintain client information and documentation to ensure it remains accurate and current.

13.2 CDD must be completed prior to taking on a client, i.e. at client on boarding stage. It comprises of the identification and verification of client information, persons acting on behalf of a client or clients acting on behalf of another person, and the identification of the beneficial owner to enable the bank to assess client its AML/CFT and Sanctions risk.

13.3 CDD must be conducted when:

13.3.1 The Bank is establishing a business relationship or concluding single/multiple transactions

13.3.2 When you doubt the veracity or adequacy of documents, data, or other information previously

obtained for the purpose of KYC.

13.4 A business relationship may not be established nor a single transaction concluded with:

13.4.1 An anonymous client; or

13.4.2 A client with an apparent false or fictitious name.

13.5 Should the Bank be unable to establish and verify the identity of a client or other relevant person, or to conduct ongoing due diligence, the Bank shall not establish a single transaction with the client or will terminate an existing business relationship with the client as the case may be. The Bank shall also consider making a Suspicious and Unusual Transaction Report to FIC should such be found.

13.6 CDD is the key source of information used for the purpose of determining whether a client is a PEP/DPIP/FPPO in his own right or a PEP/DPIP/FPPO through his / her relatives, associates or beneficial owner(s) as well as determining whether a STR and/or TPR should be filed with the FIC.

13.7 Information obtained from a client via CDD may be compared against additional independent sources in order to verify the accuracy of the information. The following third-party verifications can be done:

13.7.1 Databases, including the National Treasury's database of blacklisted suppliers. To compensate for a lagged updating of the National Treasury's database, the annual reports of the public sector institutions are a key consideration during the AML screening, where such reports are available

13.7.2 CIPC;

13.7.3 ITC;

13.7.4 Experian;

13.7.5 Braby's;

13.7.6 Windeed;

13.7.7 Aktex ETL;

13.7.8 Other internet-based directories and databases;

13.7.9 Google and satellite to verify actual Land;

13.7.10 Companies' Annual Reports, where available

13.7.11 Companies' Annual Financial Statements, where available

13.8 Auditors

- An entity's auditor (as defined in the Public Accountants and Auditors Act, No, 80 of 1991) may be utilised to verify the details of the entity, and any associated persons, by obtaining a report from the auditors confirming the details submitted by the client. Internal audit may also examine the adequacy and effectiveness of the AML Policy and processes.

13.9 Internal Employees

- Employees of the Bank may confirm that the property exists and verify the address via site inspections.

14. ENHANCED DUE DILIGENCE (EDD)

14.1 Where a client is identified as high risk, EDD must be conducted and will be applied in any of the following instances:

14.1.1 Where the client has been identified as a PEP/DPIP/FPPO, a family member or close associate of a PEP/DPIP/FPPO; and/or

14.1.2 Where the client has been identified as high risk, according to the client's risk assessment; and/or

14.1.3 Where the client has been identified as having adverse media that may pose a reputational risk to the Bank.

14.2 For EDD the Bank is required to obtain the following additional information:

14.2.1 individuals with ownership or control over the account i.e. beneficial owners, all guarantors

14.2.2 occupation of beneficial owner and guarantors (mandatory);

14.2.3 industry/nature of business of beneficial owners and guarantors (mandatory);

14.2.4 banking references for the client;

14.2.5 domicile of the client;

14.2.6 source of funds and source of wealth of the client to be established; and

14.2.7 adverse media checks.

14.3 For clients that are identified as high, an EDD is required, The Board took a strategic decision to decentralise the credit mandates with the view of improving turnaround times. This has resulted in the formation of three new management Credit Committees located in the Provinces and Regional offices (on a hybrid platform-i.e. combination of virtual & physical). Only the Board and Credit & Investment Committee remain unchanged in terms of the credit governance structures. In the Board meeting of September 2022, the Board had further requested the implementation of additional conditions as part of the new blended finance programme, requiring the Social and Ethics Committee (SEC) approve all Low/Medium Risk PEP regardless of size of transaction. In implementing and operationalizing the Board's resolution, the only change to the AML governance process, is where a client is an individual or juristic entity classified as a PEP with no adverse media, with a PEP classification of low or medium, is then escalated to SEC for approval. This will be noted at Board via SEC report. This is depicted below

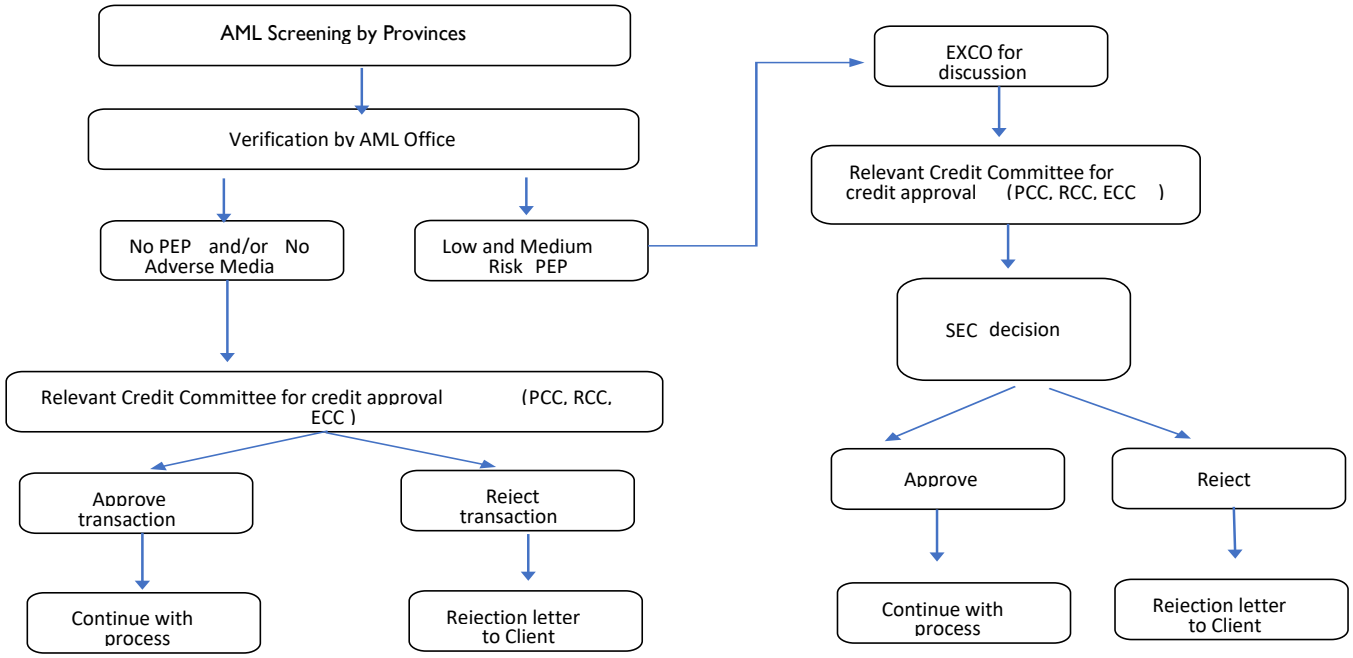
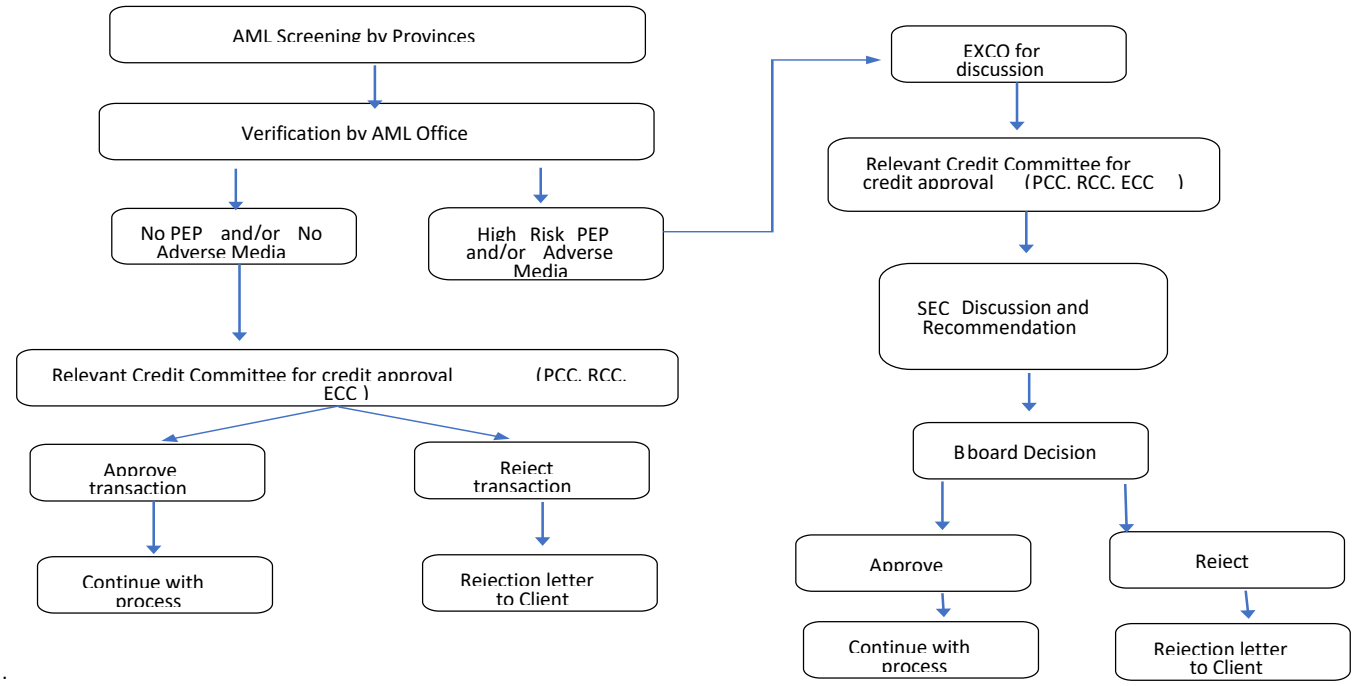


Diagram 1: EDD Process Flow

14.4 Where the transaction has High Risk PEPs and/or adverse media the EDD process continues as depicted in the diagram below.



14.5 Where the Board has taken the decision not to onboard the client due to adverse media and reputational risk posed to the Bank, a rejection letter needs to be sent to the client informing him/her of the decision taken.

14.6 The relevant BU in consultation with the Legal Department and the MLCO will draft the client rejection letter.

14.7 For suppliers identified as high Risk (High Risk PEP/DPIP/FPPO/adverse media), an EDD Is required, which will be followed by a recommendation from the Procurement Committee, discussion at EXCO for onward submission to SEC. Deliberation at SEC would occur for recommendation to the Board for approval.

14.8 The EDD process flow is depicted in **Diagram 2** below:

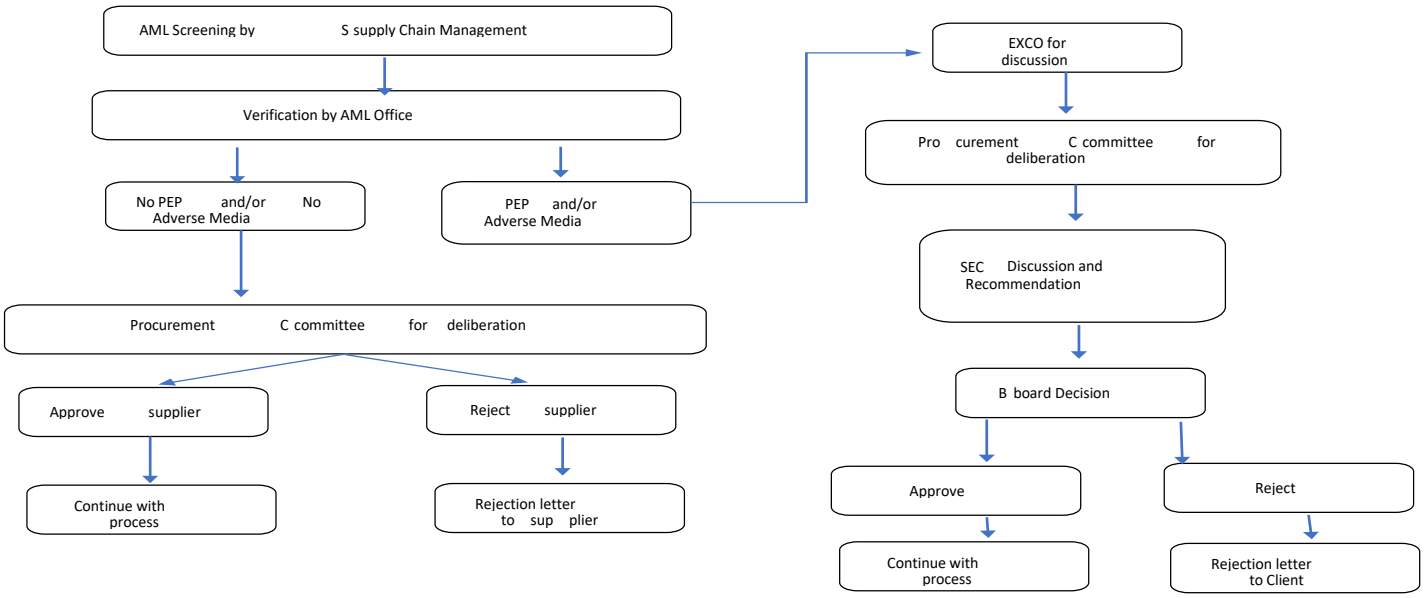


Diagram 2: EDD Process Flow

Note 1: for all other commercial transactions /suppliers where low Risk PEPs have been identified, EXCO will be the approving authority, whilst for medium Risk PEPs it will be SEC

Supplier/Bidder rejection/disqualification

14.9 The Bank is governed by the PFMA, National Treasury Regulations and instruction notes such as Instruction Note 3 of 2021/2022 and others which details the process on restricting suppliers from doing business with Government. The Office of the Chief Procurement Officer (CPO) within the National Treasury emphasized the following key points in respect of restricting a supplier to adverse media and the potential of reputational risk:

14.9.1 If there are no objective criteria that speaks to the reputational, legal, financial risk of awarding a contract, the bidder/supplier cannot be disqualified, as such all bid invitation documents will reflect on this criterion.

14.9.2 The criteria for due diligence are specific to the scope of services of that are required. It is not possible to disqualify a bidder on such grounds.

14.9.3 If the bidder is not restricted and/or listed on the National Treasury's database of restricted suppliers,

then there are no grounds to disqualify the bidder. We note that National Treasury's database are at times not updated and possibly incomplete. We therefore aim to use other publicly available information such as Company annual reports and Annual Financial Statements to enhance our decision-making process

14.9.4 The Accounting Authority (Board) may write to the bidder to clarify the issues that are being raised on the public platform and the bidder should indicate why the evaluation of the bid proposal should continue.

14.9.5 The Accounting Authority (Board) should also mitigate the risks – should the bidder be awarded the contract. The exit clause must make provisions for justifiable grounds to terminate.

14.9.6 The FIC Guidance Note 7 advances mitigation for managing high risk transactions, clients or relationships, that is,

(i) process to exit from high risk relationships, that would be inserting exit clauses in the performance contract of the service provider in a case of the Bank;

(ii) approval procedures for high risk transactions and relationships, that would be Board approving PEPs and high-risk clients in a case of the Bank (or delegation of such to an Executive for approval for purposes of turnaround times) and

(iii) adequate supervision for high risk activities or clients, that would be on-going due diligence and governance reporting of the high-risk activities and employing higher quality sources of vetting information;

14.10 The FIC Guidance Note 7 also advances that wholesale refusal of services or termination of services to a class of clients may give rise to financial exclusion risk and reputational risk to the accountable institution.

14.11 Furthermore, the FIC Guidance Note 7 advances that avoiding risk by refusing services or terminating or restricting business relationships should be used a measure of last resort where an accountable institution has reached a conclusion that ML/TF risks relating to specific clients cannot be mitigated adequately or effectively

15. ON-GOING DUE DILLIGENCE (ODD)

15.1 The Bank, must during course of a business relationship, perform on-going risk rating of existing clients. The success of accurately risk rating clients is dependent on several factors, inclusive of the following:

15.1.1 Knowledge of the client;

15.1.2 Valid, relevant & accurate client information; and

15.1.3 Clearly defined trigger events.

15.2 The on-going monitoring of client activity to establish if the client behaviour is consistent with their original risk rating is a key due diligence factor. Trigger events could negatively affect the risk rating of clients, which would require action as per the risk rating.

15.3 The review frequency of clients based on their risk rating is set out in **Figure 5** below:

Risk Rating	Frequency of ODD
Low	Every 3 years.
Medium	Every 2 years.
High	Every year.

Figure 5: Client due diligence frequency

15.4 Note: A trigger event may occur outside of the set review frequency, which could cause a review outside of the pre-determined timeframes above.

16. AML SCREENING

16.1. AML SANCTIONS SCREENING

16.1.1- FATF Recommendation 6, requires each country to implement targeted financial sanctions control regimes to comply with the UNSCR 1267 (1999) and its successor resolutions relating to the prevention and suppression of terrorism and terrorist financing. These resolutions require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any natural persons, groups, legal person / entity and/or country designated by the UNSC under Chapter VII of the Charter of the United Nations.

16.1.2 The regulatory framework in SA with respect to Sanctions consists primarily of the following pieces of legislation, namely: FICA; and POCDATARA

Application of the legislative requirements

16.1.3 From a SA legislative point of view, section 25 read together with section 4 of POCDATARA is a response to implementing FATF Recommendation 6:

16.1.4 Section 4 of POCDATARA expressly prohibits the Bank from dealing with such sanctioned natural or legal persons /entities pursuant to section 25 of POCDATARA. Any person that has any dealings with such sanctioned natural or legal person / entity is in contravention of section 4 and is guilty of an offence.

16.1.5 Section 25 of POCDATARA requires the President of SA to issue a proclamation in respect of any natural persons, groups, legal person / entity and/or country that has been designated as sanctioned by the UNSC in a resolution to combat or prevent terrorist and related activities.

16.1.6 To ensure that the Bank does not enter into a business relationship or arrangement with sanctioned natural persons, groups, legal person / entity and/or country as designated in the UNSC's Sanctions list, the Bank is committed to screening natural persons, groups, legal person / entity and/or country against sanctions lists (Dow Jones Watch lists).

16.1.7 FICA prescribes that if an AI is found to be dealing with a sanctioned natural or legal person / entity pursuant to section 25 of POCDATARA, and is in possession or has under its control property owned or controlled by or on behalf of, such sanctioned persons, the AI must report in the prescribed format that fact as soon as possible but not later than 5 working days (excluding weekends and public holidays) after it has been established that it holds property of such sanctioned persons to the FIC.

16.1.8 The Bank is committed to freezing the property and exiting the business relationship relating to a true match against the UNSC Sanctions list, as promptly and as effectively as possible.

16.2. AML PEP SCREENING

Politically Exposed Persons (PEPs) and Domestic Prominent Influential Persons (DPIPs)

16.2.1 The definition of a PEP is wide-ranging and according to FATF[1], the term PEP:

- Is used for an individual who is or has in the past been entrusted with prominent public functions in a particular country; and
- Would include people closely related or with close association to a PEP.

16.2.2 FICA defines a DPIP as the following:

- A domestic prominent influential 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 a prominent public function

16.2.3 FICA defines FPPO as the following

- A foreign prominent public official 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 any foreign country a prominent public function

16.2.4 Due to their position and influence, it is recognised that many PEP/DPIP/FPPO are in positions that

[1] International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – FATF

Recommendations February 2012

potentially can be abused for the purpose of committing money-laundering offences and related predicate offences, including corruption & bribery and conducting activities related to terrorist financing[2].

16.2.5 The potential risks associated with business relationships or single transactions with PEP/DPIP/FPPO are perceived to be one of the high-risk categories of clients, particularly with regard to money laundering and corruption in today's highly regulated environment. Thus, business relationships or single transactions with PEP/DPIP/FPPO constitute a high risk for Land Bank if not managed properly.

16.2.6 Relationships / transactions with PPEP/DPIP/FPPO may give rise to increased risks due to the possibility that individuals holding such political / influential positions may misuse their power for personal gain or advantage and of their families and / or close associates. PPEP/DPIP/FPPOs justify the application of additional AML / CFT processes to prevent improper influence or misuse of financial systems and to detect such potential abuse.

16.2.7 The following are some examples of PEPs:

- Heads of State and their deputies;
- Heads and Deputies of Regional Government (Premier);
- Heads of Government agencies and cabinet Ministers;
- Regional/Provincial Government Ministers;
- Members of National Parliament;
- Members of Provincial Legislature;
- Senior Civil Servants (National/Regional/Provincial Government);
- Local Government officials (City Mayors, Councillors and Municipal Managers);
- Senior Embassy and Consul staff;
- Members of Houses of Traditional Leadership (Kings and Chiefs);
- Senior members of the Police Services;
- Senior members of the army and/ or influential officials, functionaries and military leaders and people with similar functions international or supernatural organisations;
- Senior members of the Secret Services;
- Senior members of the Judiciary (Judges, Magistrates and Prosecutors);
- Senior and/ or influential representatives of religious organisations;
- Political Leaders;

[2] FATF Guidance – Politically Exposed Persons – Recommendations 12 and 22 June 2013

- Labour Group Officials;
- Influential functionaries in the private sector and public services administration;
- Key leaders of State-owned Enterprises;
- Private companies, trusts, foundations, or other juristic persons owned or co-owned by PEP's, whether directly or indirectly; and
- Any business/ and or joint venture that has been formed by, or for the benefit of a senior political figure.

People closely related or associated to a PEP/DPIP/FPPO include family and associates

Close Family

16.2.8 Close Family members are individuals who are related to the PEP/DPIP/FPPO either directly (consanguinity) or through marriage or civil forms of partnership. The following examples serve as an aid in defining and identifying close family members:

- Spouses and life partners;
- Children and siblings;
- Parents and grandparents;
- Uncles and aunts;
- Nephews and nieces; and
- Relatives by marriage.
-

Close Associates of a PEP / DPIP/FPPO

16.2.9 Close associates are individuals who are closely connected to a PEP/DPIP/FPPO, either socially or professionally and would include:

- Close business associates / partners (especially those that share beneficial ownership of legal entities with the PEP/DPIP/FPPO or who are otherwise connected e.g. through joint membership of a company Board);
- Personal / financial advisors / consultants or persons acting in a fiduciary capacity for the PEP/DPIP/FPPO; and
- Any other person who benefits significantly as a result of being close with such a person.

Improper Influence

16.2.10 Improper influence is defined as personal power that induces another person to give consideration

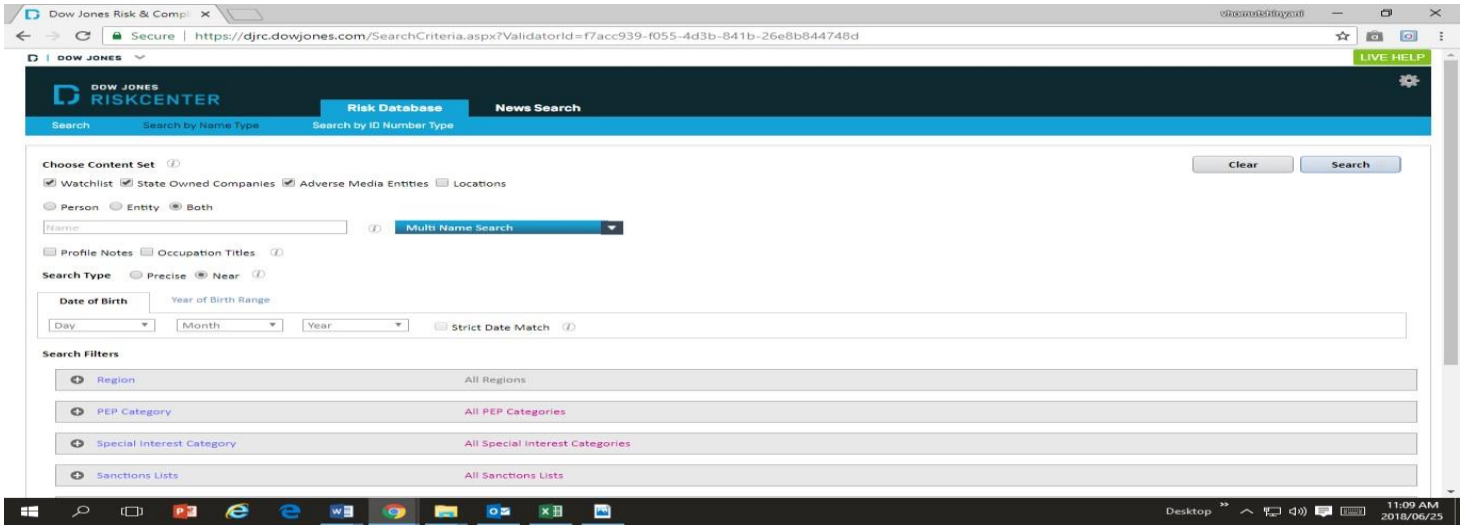
or to act on any basis other than the merits of the matter.

16.2.11 Ability to influence can be defined as individuals holding positions in the State or private sector where by virtue of their position may misuse their power and influence for personal gain and advantage or for the personal gain or advantage of family and close associates. Such individuals may also use their families or close associates to conceal funds or assets that have been misappropriated as a result of abuse of their official position. Such individuals also. are in a position to exert undue influence on decisions regarding the conduct of their business

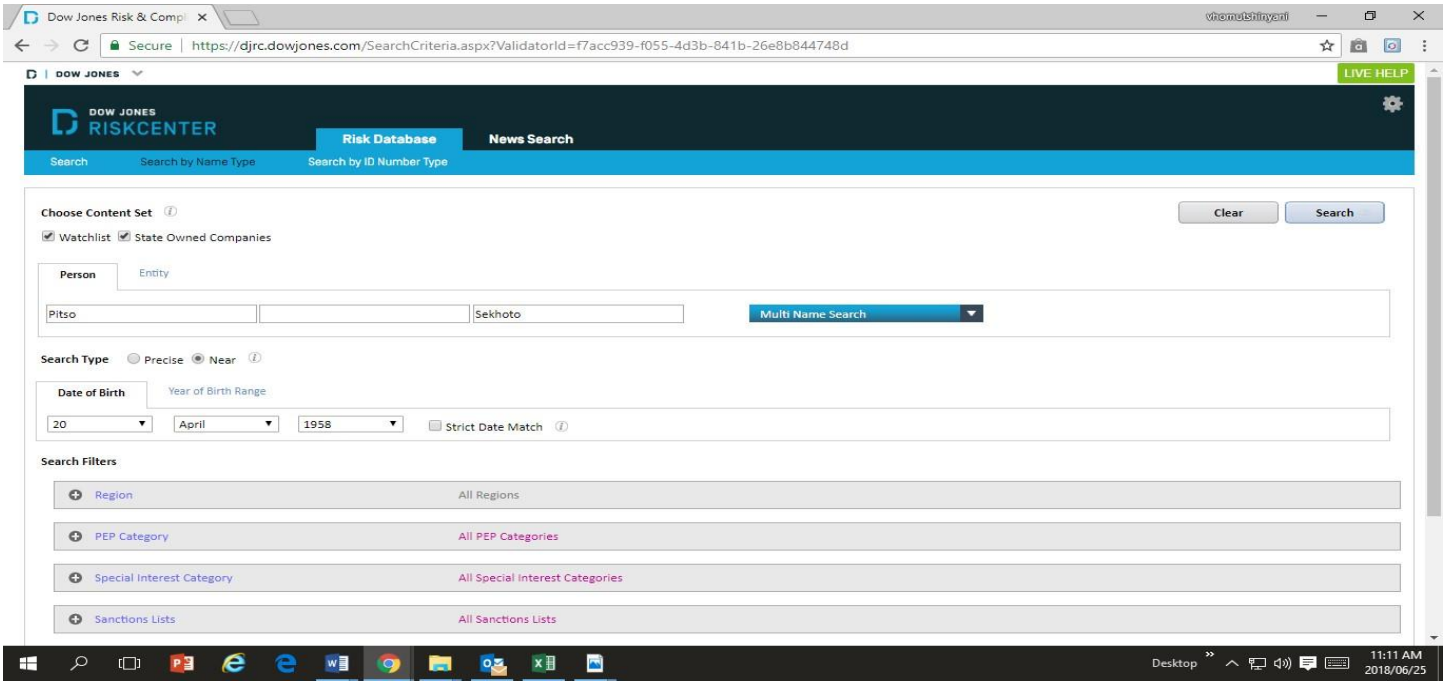
16.2.12 The Bank must mitigate against PEP/DPIP/FPPO risks by ensuring that it has rigorous processes to screen PEP/DPIP/FPPO to safeguard the reputation of the Bank. Screening for PEPs/PIPs also ensures that the Bank complies with the various Directives, Guidance and Public Compliance Communication issued by FIC aimed at combating money laundering, terrorist financing, the prevention and detection of fraud and other corrupt practices. The Bank currently utilises the Dow Jones screening software to conduct PEP/DPIP/FPPO/Sanction and adverse media screening.

16.2.13 Dow **Jones AML/CFT screening methodology**

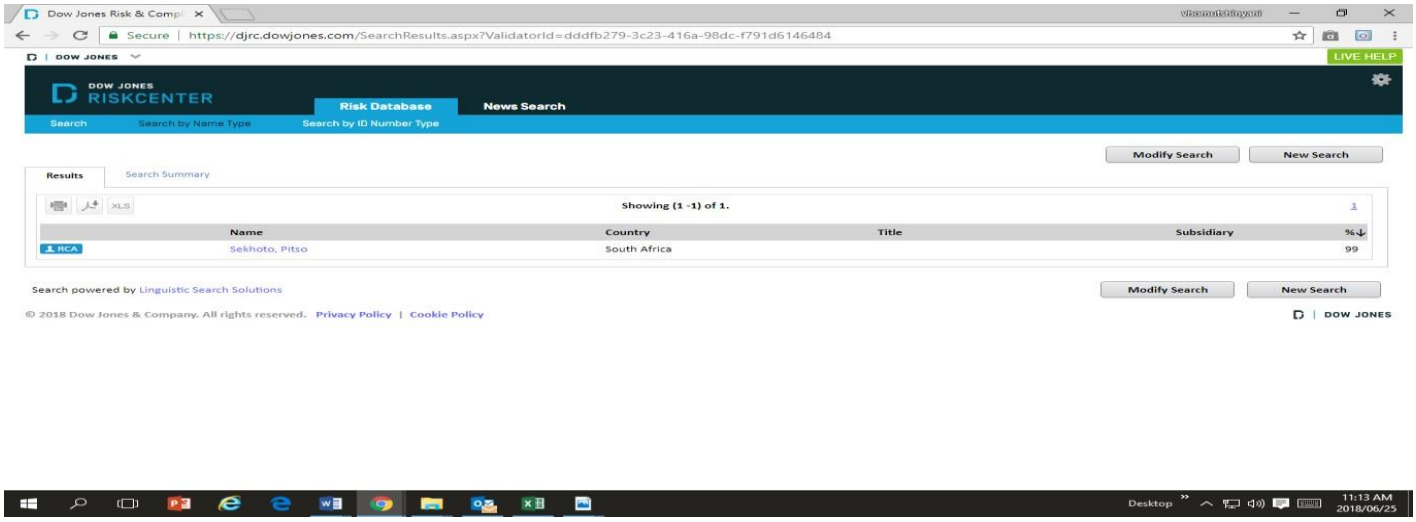
Step 1: Choose the content search, select Watchlist, State owned companies and Adverse Media Entities



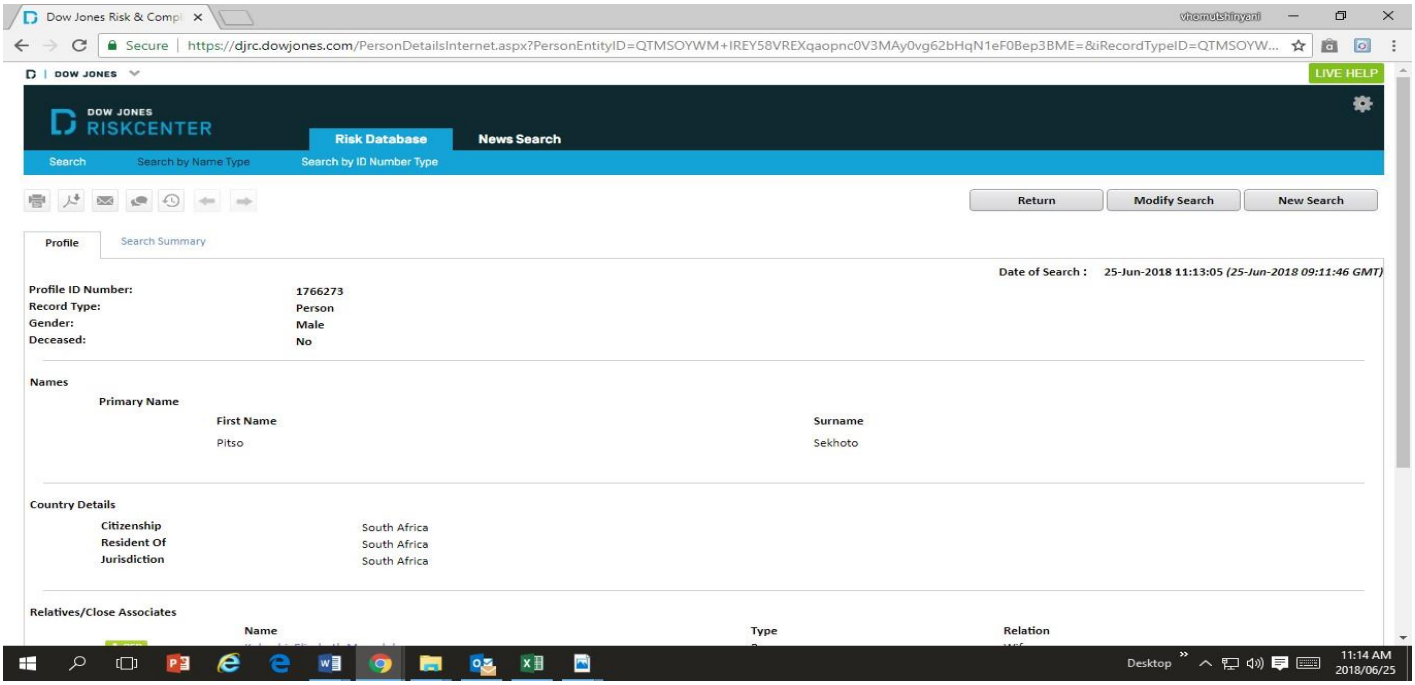
Step 2: Compete First name, middle name, surname and date of birth. Press search button



Step 3: Search results



Step 4: Dow Jones results



16.2.14 Furthermore, according to the Basel Committee on banking supervision there is a compelling need for financial institutions considering a relationship with a person who it suspects of being a PEP to identify that person fully, as well as people and companies that are clearly related to him or her.

16.2.15 Please note that globally and locally penalties & fines have been imposed on financial institutions that established business relationships with PEP/DPIP/FPPO without following adequate "KYC" and EDD procedures.

16.2.16 Where a potential client is a PEP/DPIP/FPPO, a pre-approval process must be completed before establishing a business relationship or concluding a single transaction with such a client. All known information regarding the PEP/DPIP/FPPO in terms of his / her full identification particulars, current status (active or retired), background, close business associates, any known adverse media reports, the extent of the PEP's involvement and / or interests in the transaction or entity must be considered before a business relationship can be established or concluding a single transaction.

16.2.17 It must be borne in mind that, the fact that a PEP/DPIP/FPPO has been identified or subsequently found to be involved in a transaction should not by itself create reasons for the declining or rejection of that transaction or application. In principle, there is nothing wrong with doing business with a PEP/DPIP/FPPO, provided that a due diligence has been conducted prior to the establishment of a business relationship or the conclusion a single transaction. Similarly, should an existing client's status change to a PEP/DPIP/FPPO, all information related to the client as noted above must be obtained to determine the continued acceptability of the client and the risk.

16.2.18 A business relationship with a PEP/DPIP/FPPO cannot be rejected purely based on a determination

that the potential / existing client is a PEP/DPIP/FPPO. This is contrary to the form and substance of the money laundering and control regulatory recommendations. The RMCP is not intended to create reasons for declining of transactions or applications by clients who fall within the definition of PEPs/PIPs.

16.2.19 The decision to establish a business relationship with a PEP/DPIP/FPPO depends on the approval of the EXCO and/or SEC and/or Board. The quarterly risk report to EXCO, SEC and RGC reflects on all AML screening reports regardless of the risk rating.

16.2.20 For example, the following will be some of the reasons for rejecting a business relationship with a PEP/DPIP/FPPO:

- Sanctioned or designated individuals / entities;
- When the risk of taking on or retaining existing business falls outside the acceptable risk appetite of the Bank; and
- Where there is adverse information on the individuals / entities, who may tarnish the reputation of the Bank and the continuation of the relationship therefore becomes undesirable.

16.2.21 FATF in February 2012[3] expanded the mandatory requirements for domestic PEPs and those of international organisations, in line with the objectives of Article 52 of the United Nations Convention against Corruption, which provides a similar definition of a PEP as, discussed under number 5 above that includes both domestic and foreign PEPs. Consistent with this objective, FATF (Recommendation 12) [4] provides guidelines on the treatment of PEPs in that it requires AIs to implement measures to an have appropriate risk management system in place to determine whether clients or beneficial owners are PEPs inclusive of foreign PEPs, or related or connected to a foreign PEP, and, if so, take additional measures beyond the normal CDD (Recommendation 10)[5] to determine if and when they are doing business with them. In addition, financial institutions are required to take reasonable measures to determine whether the beneficiaries of a life insurance policy and / or where required the beneficial owner or the beneficiary is a PEP.

Process to be followed when a PEP/DPIP/FPPO is identified

Pre-approval discovery

16.2.23 The following is a step-by-step illustration of the process to be followed when a PEP/DPIP/FPPO has

[3] The International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, February 2012

[4] FATF Guidance, Politically Exposed Persons (Recommendations 12 and 22), June 2013

[5] Recommendation 10 deals with Client Due Diligence and Tipping off

been discovered / identified during the CDD process i.e. prior to establishing a business relationship and concluding a single transaction.

Step 1

- When a PEP/DPIP/FPPO, family member or associate has been discovered during CDD stage, an EDD process should be conducted by the MLCO. This will entail obtaining more publicly known information about the client from relevant independent sources. The MLCO will submit the EDD with all relevant known information regarding the PEP to EXCO for deliberations. It will then pass to the credit committee structures to determine the financial viability of the transaction
- For blended finance transactions that have low and/or medium risk PEP identified, approval will be granted by SEC for noting at Board.
- For all transactions that have high risk PEPs and/or adverse media identified SEC and EXCO would deliberate and make a recommendation to Board for approval.

Step 2

- The Board will consider the information presented and decide on the matter. The submission may include any other additional information presented verbally or in writing.

Step 3

- If Board approves the transaction, then the transaction can continue as per the relevant internal processes (relevant credit committee for credit approval). It must also be determined if the approval is conditional or not. The PIMS must thereafter ensure continuous monitoring of the PEP/DPIP/FPPO account and ensure adherence to the conditions.

Step 4

- If Board rejects the business relationship or transaction then the process for rejected business applications will be followed and a rejection letter should be sent to the client. The applicable BU will be responsible for preparing the rejection letter in consultation with the Legal Department and MLCO.

Post approval discovery

16.2.24 The on-going transaction screening / monitoring procedure undertaken after acceptance or on-boarding of business from clients will uncover PEP/DPIP/FPPO when screened against Dow Jones.

16.2.25 The MLCO may also uncover PEP/DPIP/FPPO as part of their regular compliance monitoring process. This will occur mostly through the daily / monthly screening of the existing client database or when an existing client initiates a request e.g. re-applies for additional products.

16.2.26 The following is a step-by-step guide of the process to be followed when such a PEP/DPIP/FPPO client is identified i.e. PEP/DPIP/FPPO post approval / post on-boarding or an existing client: Once the EDD has been concluded, the MLCO must submit the EDD report as per steps 1-4 above.

Foreign prominent public official (FPPO)

16.2.27 All FPPOs (individuals who are or have been entrusted with prominent public functions by a foreign country) will be treated in the same manner as local PEP/DPIP. All the processes that are followed when identifying and verifying local PEP/DPIP will also be applicable to the FPPO. The decision to establish or maintain a business relationship with a FPPO will be taken by the Board together with the MLCO. Whilst country of domicile or nationality may be relevant in determining the level of risk for a local / domestic PEP/DPIP, FPPO are always High Risk.

16.2.28 Often FPPO establish business relationships or conclude a single transaction by using third parties, such as intermediaries, legal entities or legal arrangements to circumvent AML / CFT and anticorruption safeguards. Where such third parties are used by FPPO, beneficial ownership must be established to mitigate against AML / CFT or terror financing risk.

16.2.29 In terms of the Landbank Act, the Bank is only allowed to give disbursements to SA citizens. However, directors of juristic entities as well investors and /or suppliers may have foreign nationals in their corporate structure. We therefore apply the FICA and FATF guidelines in managing this risk.

Monitoring and reporting

16.2.30 Once the Bank has established a business relationship with a PEP/DPIP/FPPO, the PIMS will conduct on-going monitoring on the PEP/DPIP/FPPO and advise the Board and the MLCO on any changes in the profile or activities of the PEP/DPIP/FPPO, if any. The MLCO is required to maintain an up to date monthly list of all PEP/DPIP/FPPO and report these to the EXCO. The MLCO must provide the EXCO, SEC and RGC with quarterly reports on all approved transactions with PEP/DPIP/FPP or an interim urgent report when there is any known and verified adverse report about a PEP/DPIP/FPPO together with a recommendation. This reporting is in addition to the regular reporting obligations under FICA (CTRs, STRs and TPRs).

Dealing with PEP/DPIP/FPPO in the procurement process

16.2.31 When the Bank contracts with service providers, it is necessary to screen such providers to determine if they are PEP/DPIP/FPPO. Where PEP/DPIP/FPPO are identified, the Head of Procurement must submit this information to the MLCO in order to conduct an EDD.

16.2.32 Once the EDD is completed by the MLCO, the relevant governance structure at management or board

level depending on the risk rating will make the final assessment and approve or decline the business relationship.

Dealing with PEP/DPIP/FPPO in the recruitment and selection process

16.2.33 When the bank contracts with a prospective employee, it is necessary to screen such persons to determine if they are PEP/DPIP/FPPO/ or have adverse media.

16.2.34 The EDD will be conducted by the MLCO and recommendations made as per the relevant governance approval process.

Dealing with PEP/DPIP/FPPO in the legal process

16.2.35 Where the Bank is a party to the transaction in the legal process, EDD will be conducted by the MLCO and recommendations made as per relevant governance approval processes in terms of the risk rating Where the activities take place outside the Bank, which potentially shifts responsibility to parties involved-i.e. When bidder or purchaser is identified subject to Court proceedings as managed by the Legal Services, the AML process will be triggered. The EDD will be conducted by the MLCO and recommendations made as per the relevant governance approval process in terms of the risk rating .

NOTE 2- SCREENING FOR PEP/DPIP/FPPO should occur every time there is new transaction/facility entered into by the client . In the procurement space, screening should occur each and every time a service provider is awarded a contract to provide services to the Bank.

16.3. ADVERSE MEDIA

16.3.1 As an additional measure to combat money laundering / terrorist financing risks, the Bank must determine the reputational risks that it may be exposed to due to its relationship with high-risk clients and clients who may be re-classified as high risk due to a trigger event. As such, the Bank must perform adverse media checks in order to assess whether a prospective or existing client or supplier or employee:

- May pose a reputational risk to the Bank;
- May pose a security risk to the Bank;
- Has not disclosed or has concealed relevant information about him / her / itself which maybe to the detriment of the Bank;
- Could be susceptible to coercion as a result of his / her / its geographic location or activities; or
- Is engaging or suspected of engaging in illegal activities, or with natural or legal persons

who may pose a reputational risk to the Bank.

16.3.2 The MLCO will perform and document adverse media checks using Dow Jones Factiva and publicly available sources of information for prospective or existing clients. Adverse media checks must be performed at the during the CDD, EDD and ODD stages. Furthermore, adverse media checks must be performed when an existing low or medium risk client's risk rating is changed to high risk as a result of the re-calculation of a client risk rating during a trigger event.

16.3.3 All reasonable efforts must be made to publish only facts and statements that can be verified, not personal opinions or speculations.

16.3.4 An important consequence of the information-sharing revolution is the opportunities for learning and social connection, however, "the vast quantity of and accessibility to information online has prompted concerns about credibility as the origin of information, its quality, and its veracity are less clear than ever before." This has resulted in a drive for individuals to evaluate information and identify the information that they can trust.

16.3.5 Individuals traditionally "reduced uncertainty about credibility include judgments based on personal knowledge or on vicarious information (e.g., reputation) concerning the trustworthiness of a source or piece of information, and by relying on traditional information intermediaries such as experts, opinion leaders, and information arbiters to help guide their credibility decisions.

16.3.6 The MLCO will consider the following when attempting to determine the credibility of information:

- **Accuracy** refers to the degree to which a web site or other source is error free and whether the information can be verified offline.
- The **authority** of a web site may be gauged by noting who authored the information, what the author's credentials and qualifications are, and whether the site is recommended by a trusted other.
- **Objectivity** involves identifying the author's purpose for providing the information and whether the information provided is fact or opinion, which also includes understanding whether there might be commercial intent or a conflict of interest, as well as the nature of relationships between linked information sources (e.g., the meaning of "sponsored links" on a Google search output page).
- **Currency** refers to how up-to-date the information is, and coverage refers to the comprehensiveness or depth of the information provided.[6]

[6] Credibility and trust of information in online environments: The use of cognitive heuristics by Miriam J. Metzger*, Andrew J. Flanagin; Department of Communication, University of California, Santa Barbara, Santa Barbara, CA 93106, USA https://pdfs.semanticscholar.org/d61b/8f7869ebe18d35e35015066003948c364789.pdf

Further considerations:

16.3.7 Know the "Generic Top-Level Domains (GTLDs"

The most common GTLDs and what they generally mean when assessing for credibility:

- ☐ com (commercial): This is the most popular GTLD. Originally used for commercial purposes, this is now used for almost any web site imaginable. Anyone can have a .com. Proceed with caution and a critical eye.
- ☐ .net (network): Originally meant for network sites, this GTLD, too, is often used for many nonnetwork-related information. Anyone can have a .net. Proceed with caution and a critical eye.
- ☐ .gov (government): These sites are restricted to government use only. This is not a public domain one can simply purchase. Often an excellent source of statistical data.
- ☐ .org (organization): This GTLD was intended for organizations and non-profits. However, it has quickly been embraced by the general public. Be aware of the bias of the particular organization. Proceed with caution and a critical eye.
- ☐ .edu (education): This GTLD is generally used by universities and other formal educational institutions. Many research sciences will publish through their associated university.

16.3.8 "Identify the kind of contents: Is it a news story? Or is it an opinion piece? Is it a reaction to someone else's content? Who produced the content: Is it a news organization? Or is it a publication that is sponsored by a think tank, or a political group or a corporation? Where the organization gets its money. If it's a non-profit or an advocacy group, where did that money come from? If that isn't clear, that's a problem.

16.3.9 Who and what are the sources cited and why should I believe them? News content usually cites sources for the information provided. These are the people quoted, or the documents or reports or data being referred to. As you read, listen or watch a piece of content, note who is being cited.

16.3.10 International best practice dictates that unfavourable information or adverse media should be found across a wide variety of news sources which includes both traditional news outlets and those from unstructured sources.

16.3.11 The Bank can only go as far as identify what is on these publishing houses websites. We cannot go further than that because it is beyond our control and sphere of influence. A detailed forensic report would have to be commissioned to investigate further.

16.3.12 The various management committees manage reputational risk. The management committees are required to immediately report all matters identified to the Executive Committee for discussion. The Chief Risk Officer is responsible for immediately notifying Board.

16.3.13 The Risk Appetite Framework monitors indicators for reputational risk. All matters that lead to reputational risk is immediately escalated to:

- Executive Committee and Board for approval and/or discussion.
- Determine materiality
- Application of relevant mitigations

16.3.14 Reputational Risk relates to on boarding and or existing relationships in respect of:

- Clients
- Vendors
- Staff

16.3.15 The Process flow for matters of reputational risk is depicted in **Diagram 3** below

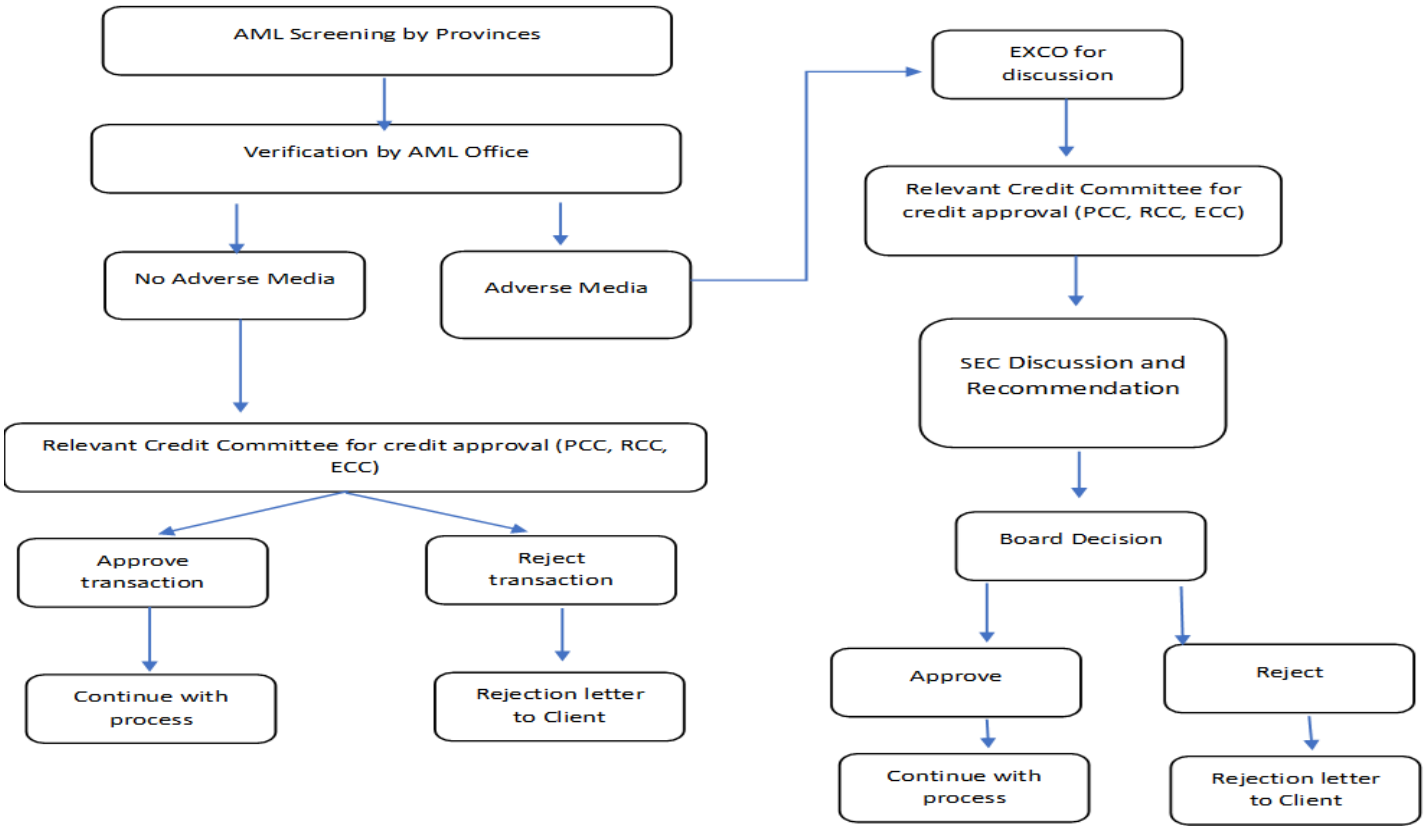


Diagram 3: Reputational Risk Process

16.3.16 AML Screening reports are valid for a period of 6 months from date of issue by the AML Compliance Officer.

17. CLIENT EXIT AND PREVENT RE-ENTRY

Client exit

17.1 In accordance with the Banks risk appetite, the Bank may decide to discontinue with a business relationship. In order to ensure that the process to terminate a potential or existing business relationship is fair, consistent and objective, the following governance and oversight should be carried out:

17.2 All the due diligence, CIV and screening of which the outcomes will give rise to the business relationship to be terminated, should be included in the recommendation to the EXCO and other relevant Board Committees; and

17.3 The EXCO will determine the merits of the case and will take the following factors into account when formulating a decision:

- Applicable legislation;
- Information gathered and the risk status of the potential or existing clients from the CIV, due diligence and screening activities conducted; and
- Impact of the reputational risk for either continuing or terminating the potential or existing business relationship with the client.

17.4 The outcome of the process to terminate or continue with the potential or existing business relationship must be properly documented and signed off by the relevant Senior Management;

17.5 The documentation should be filed according to the applicable statutory, supervisory, regulatory and the Banks Records Management requirements;

17.6 The outcome off all potential and existing client business relationship termination cases should be noted at the SEC and RGC;

Potential and Existing Clients

17.7 In the case of potential clients, the following factors should be considered in order for the Bank to formulate a case for potential or existing business relationship termination, for recommendation to the EXCO and or relevant Board Committee:

- Adverse results for the potential client from the CIV exercise conducted;
- Positive alert on the potential client traced on the AML and/or the Sanctions watch list; and Instructions received by the relevant regulator to terminate a policy or relationship.

17.8 In the case of existing clients, the following factors should be considered in order for the Bank to formulate a case for potential or existing business relationship termination, for recommendation to the EXCO and or relevant Board Committee:

- Adverse results for the existing client

- A material/significant number of STR 's for the existing client;
- Positive alert on the existing client traced on the AML and/or the Sanctions watch list; and Instructions received by the relevant regulator to terminate a relationship.

Internal Watch lists

17.9 An internal watch list is a list that is maintained and kept to reflect all the clients across the Bank, which have been exited, or the relationship declined by the Bank. When clients are exited or the relationship declined, the Bank must ensure that the client does not re-enter the Bank in a different branch or capacity. The watch list is a tool to protect the Banks reputation from doing business with unsatisfactory clients. Watch lists also enable the various BUs to share information amongst one another and to leverage off each other and to help identify clients who could cause reputational damage to the Bank.

17.10 The watch list will provide an integrated list of clients or potential clients who have been exited or declined for various reasons, such as, but not limited to:

- The client is suspected or known to have taken part in terrorist financing;
- The client is suspected or known to have laundered money;
- The client is suspected or known to have been involved in bribery and/or corruption;
- The client is suspected or known to be associated with a criminal group;
- The client or associated party has substantial adverse media from a reliable source to be involved with money laundering / terrorist financing, bribery, corruption, and/or sanctioned legal persons / entities and/or is suspected or known to be associated with sanctioned individuals, countries or entities;
- If the client has been involved in tax avoidance and/or tax evasion; and
- The risk posed by the client is too high to be acceptable to the Bank as it may cause reputational damage;

17.11 When a client has been flagged as potentially being included on the watch list, it is the duty of the MLCO to investigate this client further to establish details around this client and verify that they must be on the watch list. This process must be completed before the client is on-boarded.

17.12 The MLCO must ensure that the employees within the respective BUs are aware of the internal watch list. The MLCO must ensure that the respective employees do not tip off these clients. The MLCO must engage with his / her colleagues in the different BUs regarding the watch list.

Prohibited accounts

17.13 The following clients may not engage with the Bank with regards to a single transaction or a business relationship:

- Sanctioned legal person / entity or natural persons listed on the United Nations Security Council list; and Government entities from those countries in a Sanctioned Country; and

- Clients who have been convicted in relation to money laundering / terrorist financing activities including illicit activities.

17.14 When an employee becomes aware that he / she is dealing with a client on the prohibited accounts list, the employee must immediately report this information to the MLCO via the STR Mailbox [STR@landbank.co.za]. The employee must immediately discontinue with the transaction or on-boarding process. The Senior Management is responsible for communicating with the client to inform the client that he / she or it is unable to engage with the Bank. The MLCO is responsible for discharging all the Banks reporting obligations where required.

17.15 The Banks legal department will provide guidance to the employee, MLCO and the relevant BU on how to proceed regarding communication with the client. With regards to a sanctioned client, the funds that are in the Banks possession must be frozen and the FIC (or relevant authority) informed of the funds.

18. MONITORING

18.1 AML/CFT and Sanctions Compliance monitoring focuses on the controls that are in place to protect the organisation against non-compliance.

18.2 It is important that the monitoring activities are focussed on the regulatory requirements that present the greatest risk to the Bank. The MLCO must always consider the following:

- the regulatory requirements as operationalised in the BUs;
- the CRMP's, as these should form the foundation on which the monitoring plans are developed;
- any known areas that have resulted in incidents of non-compliance (over the past 12 months or longer);
- fines and penalties that have been paid by the Bank (over the past 12 months or longer);
- complaints of a regulatory nature (over the past 12 months or longer);
- compliance-related audit findings (internal and external);
- results of regulatory interactions specifically on-site reviews (over the past 12 months or longer);
- regulatory correspondence (over the past 12 months or longer); and
- any other material consideration.

Therefore, a risk-based approach to monitoring is followed.

Roles and responsibilities:

18.3 Business is responsible for operationalising compliance and regulatory requirements, to design and implement processes and controls that mitigate the related risks;

18.4 The MLCO will have oversight over the risks related to AML/CFT and Sanctions in the Bank. Furthermore, the MLCO will conduct monitoring on the controls in business to test the adequacy and effectiveness thereof.

18.5 The GM: ERM, compliance function and internal audit will have oversight over and conduct monitoring of the MLCO.

18.6 Refer to the Compliance Risk RMCP for guidance on roles and responsibilities, monitoring etc.

19. REPORTING

19.1 Reporting is an essential part of the compliance risk management process that allows management together with the MLCO to assess and discuss current and potential AML/CFT and Sanctions compliance risks.

19.2 The MLCO must ensure that the business management is informed and manages all identified AML/CFT and Sanctions compliance risks, issues and breaches following the escalation processes in the ERMF SoP.

19.3 Compliance reporting in the land bank must be done by all three lines of defence, as required by the Compliance framework.

Types of reporting

19.4 Incident reporting (may be immediate or periodic) -Management or regulators may request more frequent or other types of AML/CFT and Sanctions compliance-related reporting. The Land Bank Risk Appetite Framework Policy makes provision for 'zero tolerance' of compliance risk, and strict interpretation and application of this policy means that any and all incidents of non-compliance should be reported to EXCO and the board. Some incidents are so critical that they must be reported immediately. Some can be reported periodically, however, they must be reported as a minimum. All incidents must be reported to the business compliance function in a timely manner.

19.5 Cyclical reporting-As a minimum, breaches/incidents of non-compliance, KRIs, results of formal monitoring and level of compliance must be reported at:

- Operations Committee (monthly);
- Enterprise-Wide Risk Committees (quarterly);
- Risk and Governance Committee and Social and Ethics Committee (quarterly); and/or

- Other committees established to have oversight of any regulatory requirement.

20. REPORTING OBLIGATIONS

20.1 AML / CFT regulatory reporting obligations regarding STRs, CTRs, CTRA, TPRs, and Section 27s within the Bank must continue without interruption. The Bank must ensure that there are no delays in submitting such reports. The Bank must ensure that there is adequate resource allocation to allow for continuous and uninterrupted reporting.

20.2 SUSPICIOUS TRANSACTION REPORTING (STR)

What constitutes a suspicion?

20.2.1 A suspicious transaction will often be one when the transaction raises questions or gives rise to discomfort, apprehension or mistrust. When considering whether there is reason to be suspicious of a particular situation one should assess all the known circumstances relating to that situation. This includes the normal business practices and systems within the industry where the situation arises.

20.2.2 A suspicious situation may involve several factors that may on their own seem insignificant, but taken together, may raise suspicion concerning that situation. The context, in which a situation arises, therefore, is a significant factor in assessing suspicion. This will vary from business to business and from one client to another.

20.2.3 Section 29 of FICA defines a suspicious and/or unusual transaction as: A transaction where a person who carries out business, is in charge of business, manages business, who is employed by the AI and who knows, ought to reasonably have known or reasonably suspects that the business:

- Has received or is about to receive the proceeds of unlawful activities;
- Has received or is about to receive property which is connected to an offence relating to terrorist activities; and/or
- Has been or is about to be used to facilitate an offence relating to the financing of terrorist activity; and/or
- Has been or is about to be used in some way for Money Laundering / Terrorist Financing; and/or
- The transaction has no apparent lawful purpose; and/or
- The transaction may be relevant to an investigation of evasion or attempted evasion of a duty to pay tax, duty or levy imposed by revenue authorities (such as South African Revenue Services).

20.2.4 An employee, with the required knowledge, skill, training and experience is expected to report a suspicion.

20.2.5 An employee of the respective BU within the Bank who ought reasonably to know, or suspects that the Bank has received or is about to receive, payments from an illicit source, money that has been laundered, or money that will finance terrorism, has an obligation to report the transaction to the MLCO.

Is the reporter's identity protected?

Section 38 of the FICA provides for a broad range of measures to protect persons who participate in submitting reports

to the Centre. It guarantees that "no action, whether criminal or civil, can be instituted against any natural or legal person who complies in good faith with the reporting obligations of the FIC Act". Consequently, they cannot even be forced to give evidence concerning such a report in criminal proceedings arising from the report. However, such a person may choose to do so voluntarily. If a person who participated in submitting a report to the Centre elects not to testify, no evidence regarding that person's identity is admissible as evidence in criminal proceedings

20.2.6 All suspicious transactions must be reported to the MLCO within 2 days of the employee forming a suspicion. The MLCO is required to report all confirmed STRs to the FIC within 15 days (excluding Saturdays, Sundays and public holidays) from the date that the employee becomes aware of the suspicious or unusual activity or transaction.

Can an institution continue transacting with a client after a suspicious transaction report has been made?

The general rule is that a person may continue with a transaction from which a report emanates. However, section 34 of the FICA empowers the Centre to intervene in certain transactions after consulting with an accountable institution, reporting institution or person required to make a report. In such instances the accountable institution, reporting institution or person in question may not proceed with the carrying out of the transaction. The Centre's intervention is valid for a maximum period of 5 days and is aimed at creating an opportunity for the Centre to make the necessary enquiries and to inform and advise an investigating authority.

Procedure of filing a STR

20.2.7 When an employee within a respective BU becomes aware of a suspicious or unusual transaction, they must continue with the transaction unless directed to stop the transaction by the FIC, Chief Executive or the MLCO. Employees are prohibited from informing the client or any other employee that a report has been made.

20.2.8 The following six steps must be followed prior to deciding on whether a transaction / activity is/are sufficiently suspicious or unusual to warrant an investigation and report to the FIC via goAML-system (a FIC online reporting system).

20.2.8.1 STEP 1 - Formulate the suspicion

- A suspicious and / or unusual transaction / activity can present itself in many ways, which may include unusual business as described above.

- If an employee suspects that a transaction / activity is suspicious or unusual, the employee must report this transaction / activity to the respective MLCO together with all supporting documents as set out in Step 2 below.
- There may be instances were a suspicion was formulated by an employee, but the prospective client decided not to conclude the transaction. In this case, the employee must still report the activity or transaction to the MLCO.

20.2.8.2 STEP 2 – Completion of the STR form

- The employee must access the intranet.
- The employee must complete the STR form in detail **(Refer to Appendix 3: STR Form**).
- The employee must submit the STR form via email to STR@landbank.co.za or to the MLCO directly.
- The identity of the employee that submitted the report must be kept confidential by the MLCO.
- The MLCO remains the contact person for the STR.
- The MLCO must always acknowledge receipt of the STR report to the employee concerned.
- The MLCO must investigate the employee's report and either confirm or dismiss the suspicion report in accordance with the process set out in Step 3 below.

20.2.8.3 STEP 3 - Investigate the suspicion and/or unusual transaction or activity

- The MLCO must examine and investigate the STR report filed by the employee to ensure that There are sufficient grounds to classify the transaction or activity as suspicious and/or unusual;
- The form was completed correctly and all the relevant information was provided;
- The form is accompanied by the relevant document/s; and
- The manner in which the activity or transaction was investigated, sources relied on and possible interviews conducted must all be clearly documented.
- The MLCO must maintain a comprehensive record (refer step 5 below relating to record retention) of all STRs reported. Records must also be kept of all STRs reported by employees but not filed with the FIC. The reasons for these instances not being reported must be detailed in the records.

20.2.8.4 STEP 4 - Filing a STR

- The MLCO must determine whether a report must be submitted to the FIC within 15 days (excluding weekends and public holidays) from the date that the employee became aware of the suspicious and/or unusual transaction or activity.

- The STR must be filed by the MLCO to the FIC using the goAML system.

20.2.8.5 STEP 5 - Record retention

- The MLCO must ensure that the following information is retained:
  - Internal reports received from employees;
  - Records of the investigation by the MLCO;
  - Record of the STR filed; and
  - Record of the FIC STR reference number and other relevant information from the FIC must be maintained.
- The STR records must be retained for at least five years from the date on which the business relationship is terminated; or a single transaction is concluded.

20.2.8.6 STEP 6 - Management Information

- The MLCO is responsible for recordkeeping of all reported STRs.
- The MLCO must ensure that the client risk profile is re-assessed based on the STRs per client.
- If the client risk profile has changed to medium or high risk, the Business area must apply the required EDD / ODD process when dealing with this client in future.
- The MLCO must maintain record of all STRs reported to the FIC (via goAML).
- On a monthly basis the MLCO provide the CE and the EXCO with a report of all the STRs submitted for the preceding month and those reported to the FIC as STRs.

20.2.9 Transactions, which are reported to the FIC in terms of an STR, must be proceeded with unless the Bank has received formal communication from the FIC not to proceed. The FIC, through formal communication, may request the Bank to suspend a transaction associated with an STR for a period of no more than 5 days in order for the FIC to investigate the matter further. In these instances, the MLCO must ensure that the FIC has sent written correspondence regarding this and must then instruct the relevant employee to suspend the transaction unless such time as the suspension has been lifted by the FIC or communication is received to prohibit the transaction.

20.2.10 A failure on the part of an employee to report a STR will result in disciplinary action being taken against such an employee.

TIPPING OFF

20.2.11 In order to secure the confidentiality of the STR reported by the employee, the employee may only disclose information pertaining to that report to:

- Their line manager;
- MLCO.

20.2.12 This requirement prevents information about the report being communicated to the alleged criminal who may, as a result, evade the authorities. This requirement also protects the identity of the employee who has reported the matter from being communicated by a colleague to the client concerned.

ANONYMOUS REPORTING

20.2.13 Anonymous reporting is not encouraged, as the MLCO often needs to contact the employee to gain additional information for investigation purposes. However, it is acknowledged that there may be circumstances where an employee may be concerned with their safety or where employee involvement is suspected. In these instances, anonymous reporting would be acceptable. The Bank is currently using 0800 004 003 and landbank@behonest.co.za for Anonymous reporting of incidents of Fraud and Unethical Behaviour run by Advance Call Fraud & Ethics Hotline.

20.3 CTR / CTRA REPORTING

20.3.1 The CTR / CTRA reporting obligations below relate to those as contained in FICA.

What is Cash Threshold Reporting (CTR)?

20.3.2 Section 28 of FICA makes it obligatory for all accountable institutions and reporting institutions to report cash transactions above the prescribed limit to the Centre in the prescribed format.

What does "cash transactions" mean?

20.3.3 This means all transactions involving domestic and foreign notes and coins, and includes travellers' cheques.

20.3.4 The MLCO is required to monitor all bank accounts for cash deposits, single transactions and aggregated deposits, which exceed the threshold. The Finance Department must aggregate single transactions by / for the benefit of the same natural or legal person / entity within a 24-hour period from the time the first transaction was made to determine if, when aggregated, the fund's total an amount over R49999.99 The MLCO is required to report these transactions within 3 days (excluding Saturdays, Sundays and public holidays) of becoming aware to the FIC via the goAML online portal. Where the information provided by the bank is insufficient to complete a CTRA, the Bank must submit an STR.

Procedure for filing a CTR / CTRA

20.3.5 The MLCO must:

- **Step1:** Extract and identify daily all CTRs / CTRAs from the bank statements;

- **Step 2:** Identify all amounts above R49999.99 and all-recurring client information based on the reference number (Client name / Client Number.) conducted on the same day for aggregation purposes (i.e. within a 24-hour period).
- **Step 3:** Examine and investigate all transactions per client and aggregates amounts where applicable.
- **Step 4:** Report the transactions as CTR / CTRA and STRs where applicable to the FIC and keep records according to the requirements in section 22 of FICA.

20.3.6 Note: Oversight is conducted by the Compliance Department on all CTR and CTRAs to ensure that all transactions are identified and reported within the prescribed period.

20.3.7 The MLCO must ensure that the details of all bank accounts within the Bank are maintained centrally and updated on a monthly basis for all changes. Each statement received by the MLCO must be filed and kept for the prescribed period of five years.

Reporting on CTR / CTRA

20.3.8 The MLCO must on a monthly basis provide the CE and EXCO with a list of all CTR / CTRA reports submitted to the FIC. All reports made to the FIC must be retained and stored in line. These records must be kept for at least five years from the date on which:

☐ The business relationship is terminated; or

☐ A single transaction is concluded.

20.3.9 A failure on the part of an employee to report a CTR / CTRA will result in disciplinary action being taken against such an employee.

Cash transaction examples

20.3.10 The following are examples of single and aggregated cash transactions:

- Client Z makes a cash deposit of R50000 into the Banks account for a payment on Monday 15 September, Finance will become aware of the transaction on Tuesday 16 September and report this as a CTR to the FIC within 3 business days, by close of business on 19 September.
- Client A makes cash a deposit in the amount of R 50000 for payment at 12:15 pm on Monday, 15 August and then makes a further cash deposit of R 6 000.00 for another or the same AI product at 14h00 on 15 August. The Bank will only become aware of the deposit on Tuesday 16 August (at the earliest). The Bank must thus file a CTRA within 3 business days, by close of business on 19 August.

20.4 TPR REPORTING

20.4.1 The TPR reporting obligations below relate to those as contained in FICA.

20.4.2 The Bank has an obligation to report property in its possession or under its control, which is owned or controlled by, on behalf of or at the direction of:

- Any person who has committed or attempted to commit, or facilitated the commission of a specified offence as defined in POCDATARA (this relates to terrorism, terrorist related activity, terrorist funding etc.); or
- A specific person identified in a notice issued by the President of the Republic under Section 25 of POCDATARA.

20.4.3 Similarities between Money Laundering and Terrorist Financing (TF) may exist, however it is important to take note of the distinguishing characteristics of TF, which are *inter alia*:

- The TF may involve the use of legitimate and illegitimately obtained funds;
- The transfer of money to bank accounts from a sanctioned person to another; without a clear relationship with account holder; and
- TF may involve a number of uncomplicated transactions of smaller amounts.

20.4.4 Following the sanctions screening process performed on all clients, the Bank may identify certain clients who are deemed sanctioned on the sanctions lists. Sanctions are restrictive measures imposed by Competent Authorities against natural persons, groups, legal persons / entities and/or countries to prevent and suppress terrorism and terrorist financing e.g. the UNSC List.

20.4.5 There may be existing clients with the Bank or those clients that are attempting to enter into a business relationship and who may be on these sanctions lists. In these instances, the assets used by this natural or legal person(s) / entity (ies) are deemed suspicious and therefore, according to FICA, must be reported as a TPR. The Bank is required to freeze all related assets of these natural or legal persons / entities without delay and report it to the relevant FIC or relevant authorities.

20.4.6 The MLCO must file all TPRs with the FIC as soon as possible but no later than 5 days (excluding Saturdays, Sundays and public holidays) of the Bank becoming aware of the fact that it has property associated with terrorist and related activities in its possession or control. When filing a TPR, the MLCO must consider if a STR should be filed as well.

20.4.7 A failure on the part of an employee to report a TPR will result in disciplinary action being taken against such an employee.

21. REGULATORY REQUESTS

21.1 SECTION 27 REQUESTS

21.1.1 In certain instances, the FIC may request client information from the Bank. The Bank is legally obliged to respond to such requests within the stipulated time. The different forms, which an information request from the FIC can take, include, but are not limited to:

- The client; or
- A person acting on behalf of a client; or
- The client acting on behalf of a specified person.

21.2 SECTION 32 REQUESTS

21.2.1 The FIC may request additional information pursuant to a previous report filed with the FIC in terms of S28, S28A and S29.

21.3 OTHER FIC CORRESPONDENCE

21.3.1 Should an employee receive correspondence from a duly authorised representative of the FIC, such as to confirm whether a specific natural or legal person / entity is a client of the Bank, he / she must report this to the MLCO immediately. The MLCO must immediately acknowledge the request to the FIC or the authority acting on behalf of the FIC. The MLCO must ensure that all requests made by the FIC are in writing and on the official FIC letterhead. These requests must be stored and kept for record keeping purposes.

21.4 MAINTENANCE OF REPORTS MADE TO THE FIC

21.4.1 All reports made to the FIC must be kept for at least five years from the date on which: The business relationship is terminated; or A single transaction is concluded.

21.4.2 The MLCO must ensure that all reports that are submitted on AML (CTRs CTRAs, STRs, and TPRs) are backed up and stored in a secure manner that can be accessed in the event of a query from the CEO or the FIC. The information to be stored includes:

21.4.3

- All correspondence from FIC together with confirmations of the reports made;
- The reference or acknowledgement numbers of all reports made including any errors references; and
- Clear and legible screen shots or saved versions of the reports made;

21.4.3 All regulatory requests and other correspondence from the FIC must be stored in accordance with the Records Management Policy.

21.5 ACCESS TO RECORDS BY FIC

21.5.1 The Bank acknowledge that an authorised representative of the FIC has access during ordinary business hours to any records kept by or on behalf of the Bank and that such a representative 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 have been made in terms of the Act. This is subject to the requirement that the authorised representative of the FIC may, except in the case of

public records, exercise this right of access only by virtue of a warrant issued in accordance with the requirements of the Act. The Bank shall assist authorised FIC representatives in the exercise of their powers as required.

22. TRAINING

Training and awareness

22.1 The MLCO must ensure that all employees of the Bank are aware of their obligations in AML/CFT and Sanctions:

22.2 The AML / CFT and Sanctions documentation must be readily accessible to all employees. The training material must be simplistic, understandable and tailored to be role specific. This training must include:

- Introduction into ML / TF;
- CIV requirements;
- Transaction monitoring;
- Identifying and reporting to the FIC (STRs, TPRs and CTRS) and responding to regulatory requests;
- Record keeping and record retrieval requirements;
- Applicable legislation;
- Banks internal rules, policies and procedures including escalation processes; and
- Sanctions.

22.3 The MLCO must document his specific training requirements and approach, in addition, to overseeing and approving the role profiling which determines the training requirements of the employees

22.4 All new employees must undergo on-boarding and role specific AML / CFT training after they have joined the Bank. Employees may not engage directly with a client, until they have completed the training.

22.5 All employees must undergo annual refresher training which commences on 01 January every year. Any employee who joins the organisation and is subject to training within 3 months of the commencement of the annual refresher training, is not required to redo the training unless there has been a material change in the training material in such period.

22.6 Where an employee has not completed the training within the specified timeframe, such employee must be subjected to the appropriate consequence management as determined by the CEO. This may include restricting domain access until the training has been completed.

22.7 The MLCO must ensure that the respective BU training material is updated when necessary. The training material must be reviewed and updated at least annually.

22.8 In order to demonstrate knowledge of ML / TF controls, the MLCO must ensure that employees complete assessments after the completion of the training. All employees must attain a pass rate of 80%. Should an

employee not attain 80% within 3 attempts, they must undergo a coaching process with the MLCO to assist the employee in improving their knowledge.

Employees exempt from training obligation

22.9 The Bank accepts that there may be employees, who do not fall within the category of impacted staff, from an AML / CFT and Sanctions perspective, and will therefore not be required to complete any training Interventions as indicated above. These employees include:

- Executive drivers;
- Catering staff;
- Mail room staff;
- On-site security personnel; and
- Staff providing cleaning services.

Training approach

22.10 Training must be developed by the MLCO in accordance with the various risk exposures faced by employees in different roles and/or levels within the Bank. For example, employees with more AML / CFT and Sanctions risk exposure must be trained on more detailed AML / CFT & Sanctions information. Each BU must assess the various roles within their area to determine the appropriate level of training for each specific role.

Introductory AML / CFT and Sanctions Training

22.11 This module will consist of a basic introduction to AML / CFT and Sanctions as well as the legislative grounds. These employees are not required to complete an assessment but must attend the Bank's induction programme where AML / CFT and Sanctions matters are presented at a high level.

Intermediate AML / CFT and Sanctions Training

22.12 This module consists of more detailed introduction to AML / CFT and Sanctions inclusive of the legislative grounds and reporting requirements. Employees are required to complete an assessment, which should not be as detailed as the assessment used to demonstrate an acceptable knowledge of AML / CFT and Sanctions risks. A minimum pass rate of 80% must be obtained.

Advanced AML / CFT and Sanctions Training

22.13 This module consists of in-depth knowledge of AML / CFT and Sanctions, legislative grounds, reporting obligations and all related matters as outlined in this RMCP. Employees must complete an assessment with the pass rate of 80% must be obtained. This advanced training will be for those with specialised AML / CFT and Sanctions roles within the Bank.

Training records

22.14 Records must be kept of all AML / CFT and Sanctions training that has been provided to the employees of the Bank. Records must comprise of:

- Employee names;
- Employee numbers (identity number can be used where there is no employee number);
- The name of the BU that the employee works in;
- The details (including date) of the training undertaken and the format of the training; and ☐ Where an assessment has been completed, the result of such assessment.

22.15 Training records must be kept for a period of 5 years from the date that the training was provided. The MLCO must keep a central register of all of the training data, including the date of the end of the 5-year period.

23. RECORD KEEPING

23.1 A systematic method of storing copies of the documents must be created such that there is sufficient cross-referencing to aid the retrieval of documents for various reasons such as audits, onsite visits etc. In addition, documents and information must be filed and stored in a manner that is accessible and legible

23.2 The Bank is required to keep the following AML / CFT and Sanctions records:

23.2.1 All CIV information including:

- The client's CIV information;
- The nature of business and purpose of account / policy / contract;
- The intended business activity;
- The source of funds, income and wealth (and verification thereof where applicable);
- Transactions performed by clients (including single transactions);
- Bank statements and information related to bank accounts;
- Identity and authority of the client acting on behalf of another person;
- Identity and authority of another person acting on behalf of the client; and
- The details of all employees collecting this information.
- Any related business correspondence; and
- The identifying particulars of all accounts and account files related to the transaction

23.3 All records of the client's transactional history must be kept updated and stored;

23.4 STR, CTR, CTRA and TPR reports made to the FIC via the goAML platform;

23.5 STRs and TPRs which were investigated but were not reported to the FIC (including the reasons as to why they were not reported);

23.6 All regulatory requests received from the FIC, including our responses thereto;

23.7 All correspondence of what so ever nature received from or submitted to the FIC via email or goAML including rejected and pending transaction reports; and

23.8 Records relating to the training of employees.

23.9 Records of CIV information may be kept electronically or in physical, hard copy form. When stored electronically, documents must be stored in a portable document format (PDF). All documents must be in a clear and legible format and controls must be implemented within the BUs to prevent any alteration of records. In addition, all such records must be indexed and linked to the client profile. Records of CIV information may be kept electronically or in physical, hard copy form. When stored electronically, documents must be stored in

a portable document format (PDF). All documents must be in a clear and legible format and controls must be implemented within the BUs to prevent any alteration of records. In addition, all such records must be indexed and linked to the client profile;

23.10 Records are required to be kept for 5 years, from the termination of the business relationship or from the conclusion of a single transaction. The five-year period will begin on the date the business relationship is terminated, or a single transaction concluded. In instances where a single transaction gives rise to a STR, the five-year period will commence from the date the STR is submitted to the FIC.

23.11 All records kept in the terms of the Act, or any certified extract of any such record, or a certified printout of any extract of an electronic record, is on its mere production admissible as evidence in a court.

24. CONSEQUENCES OF NON-COMPLIANCE

24.1 GENERAL: Any failure by an employee to comply with the requirements of the Act or this RMCP shall result in the employee being subject to disciplinary action and possible dismissal.

24.2 FAILURE TO IDENTIFY PERSONS: The Bank will be non-compliant and be subject to an administrative sanction should it performs any act to give effect to a business relationship or single transaction in contravention of the Act.

24.3 FAILURE TO COMPLY WITH DUTY IN REGARD TO CUSTOMER DUE DILLIGENCE: The Bank will be non-compliant and subject to an administrative sanction should they fail to comply with the duty to perform the prescribed customer due diligence measures in accordance with the Act.

24.4 FAILURE TO KEEP RECORDS: The Bank will be non-compliant and subject to an administrative sanction should they fail to keep a record of information in terms of and in accordance with the requirements of the Act.

24.5 DESTROYING OR TAMPERING WITH RECORDS: Any person who wilfully tampers with a record kept in terms of the Act or wilfully destroys such a record, otherwise than in accordance with the Act is guilty of an offence.

24.6 FAILURE TO GIVE ASSISTANCE: The Bank is guilty of an offence should it fails to give assistance to a representative of the FIC in accordance with the Act.

24.7 CONTRAVENTION OF PROHIBITIONS RELATING TO PERSONS & ENTITIES INDENTIFIED BY THE SECURITY COUNCIL OF THE UNITED NATIONS: Any person who contravenes the provisions of the Act and fails to sanction screen clients or other persons is guilty of an offence

24.8 FAILURE TO ADVISE THE FIC: The Bank is guilty of an offence should it fails to report and inform the FIC in accordance with the Act.

24.9 FAILURE TO REPORT CASH TRANSACTIONS: The Bank is non-compliant and subject to both an administrative sanction and guilty of an offence should it fails to report the prescribed information in respect of a cash transaction within the prescribed period in accordance with the Act to the FIC.

24.10 FAILURE TO REPORT PROPERTY ASSOCIATED WITH TERRORIST & RELATED ACTIVITIES : The Bank is guilty of an offence and are both non-compliant and subject to an administrative sanction should it have in their possession, or under their control, property owned or controlled by, on behalf of, or at the direction of an entity associated with terrorist and related activities or a sanctioned entity as detailed in the Act, and fail to report that fact within the prescribed period and manner to the FIC or fail to comply with the directions of a Director or fail to scrutinise the information as contemplated in accordance with the Act.

24.11 FAILURE TO REPORT SUSPICIOUS OR UNUSUAL TRANSACTIONS: The Bank is guilty of an offence should it fails to enquire on or report to the FIC any suspicious or unusual transaction or series of transactions that they were aware of or ought to have been aware of.

24.12 UNAUTHORISED DISCLOSURE: The Bank is guilty of an offence should they make any unauthorised disclosures as detailed in the Act.

24.13 FAILURE TO SEND REPORTS TO THE FIC: The Bank is guilty of an offence should it fails to send a report regarding the conveyance of cash or a bearer negotiable instrument to the FIC in accordance with the requirements of the Act.

24.14 FAILURE TO COMPLY WITH FIC REQUESTS: The Bank is guilty of an offence should it fails to comply with a request made by the FIC or an investigating authority acting under the authority of an authorised officer or a supervisory body in terms of the Act.

24.15 FAILURE TO COMPLY WITH THE DIRECTIVES OF THE FIC: The Bank is guilty of an offence and are both noncompliant and subject to an administrative sanction should it fails to comply with the direction provided by the FIC.

24.16 FAILURE TO COMPLY WITH A MONITORING ORDER: The Bank is guilty of an offence should they fail to comply with an order by a judge in accordance with the requirements of the Act.

24.17 MISUSE OF INFORMATION : The Bank is guilty of an offence should they disclose confidential information held by or obtained from the FIC, wilfully destroy or in any other way tamper with information kept by the FIC for the purposes of the Act, use information obtained from the FIC otherwise than in accordance with any arrangements or safeguards made or imposed by the Director, disclose a fact or information or use such information, otherwise than as permitted in term of the Act.

24.18 FAILURE TO COMPLY WITH DUTIES IN RESPECT OF THE RMCP: The Bank is non-compliant and are subject to an administrative sanction should they fail to develop, document, approve, maintain, implement and review the RMCP in accordance with the requirements of the Act.

24.19 FAILURE TO REGISTER WITH THE FIC: The Bank is non-compliant and subject to an administrative sanction should it fails to register with the FIC or fail to provide the FIC with updated information.

24.20 FAILURE TO COMPLY WITH DUTIES REGARDING GOVERNANCE: The Boards of Directors and the compliance function of the Bank will be non-compliant and subject to an administrative sanction should they fail to comply with the governance requirements as detailed in the Act and this RMCP.

24.21 FAILURE TO PROVIDE TRAINING: The Bank non-compliant and subject to an administrative sanction should they fail to provide training to their employees as required in term of the Act and this RMCP.

24.22 OFFENCES RELATING TO INSPECTION: A person who fails to appear for questioning, fails to comply with an order, wilfully gives false information to an inspector, fails to comply with any reasonable request by an inspector in the performance of his or her functions; or wilfully hinders an inspector in the performance of his or her functions is guilty of an offence.

24.23 HINDERING OR OBSTRUCTING AN APPEAL BOARD: Any person who wilfully interrupts the proceedings of the appeal board or who wilfully hinders or obstructs the appeal board in the performance of its functions, is guilty of an offence.

24.24 FAILURE TO ATTEND AN FIC SUMMONS: Any person who, having been summoned to attend and give evidence or to produce any book, document or object before the FIC or a supervisory body or the appeal board, fails without sufficient cause to appear at the time and place specified or to remain in attendance until excused; or attends as required, but refuses to take an oath or to make affirmation; or fails to produce a book, document or other item as ordered, if it is in the possession of, or under the control of, that person, is guilty of an offence.

24.25 FAILURE TO ANSWER FULLY OR TRUTHFULLY: Any person who, having been sworn in or having made an affirmation before the FIC or a supervisory body or the appeal board fails to answer any question fully and to the best of that, person's ability; or gives false evidence, knowing or believing it to be false, is guilty of an offence.

24.26 FAILURE TO COMPLY WITH FIC DIRECTIVES OR THOSE OF SUPERVISORY BODIES: The Bank is non-compliant and subject to an administrative sanction should it fail to comply with a directive of the FIC or a supervisory body.

24.27 OBSTRUCTING OFFICIALS IN THE PERFORMANCE OF THEIR DUTIES: Any person who obstructs, hinders or threatens an official or representative of the FIC in the performance of their duties or the exercise of their powers in terms of the Act, is guilty of an offence

24.28 CONDUCTING TRANSACTIONS TO AVOID REPORTING DUTIES: 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 reporting duty under the Act, is guilty of an offence.

24.29 UNAUTHORISED ACCESS TO FIC COMPUTER SYSTEMS, APPLICATIONS OR DATA: Any person who, without authority to do so, wilfully accesses or causes any other person to access any computer system that belongs

to, or is under the control of, the FIC, or any application or data held in such a computer system, is guilty of an offence.

24.30 UNAUTHORISED MODIFICATIONS TO FIC COMPUTER SYSTEM CONTETS: Any person who, without authority to do so, wilfully causes a computer system that belongs to, or is under the control of, the FIC, or any application or data held in such a computer system, to be modified, destroyed, erased or the operation or reliability of such a computer system, application or data to be otherwise impaired, is guilty of an offence.

24.31 PENALTIES: A person convicted of an offence mentioned in the Act other than an offence mentioned in paragraphs below 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 of the Act is liable to imprisonment for a period not exceeding five years or to a fine not exceeding R10 million.

25. READ IN CONJUNCTION WITH OTHER POLICIES/FRAMEWORKS

25.1 This RMCP must be read in conjunction with the following:

- Fraud and Corruption Prevention Policy;
- Whistleblowing Policy;
- Supply Chain Management Policy;
- Compliance Policy;
- Compliance Framework;
- Compliance Manual;
- Credit Policies;
- Enterprise Risk Management Framework;
- Risk Appetite Framework;
- Code of Ethics and Business Conduct;
- Recruitment and Selection Policy;
- FIC Guideline 17.

26. RMCP REVIEW HISTORY

Date of review	Version	Details of review
October 2011	1	Internal Rules to comply with FICA
June 2018	2	Alignment to amendment to FICA
November 2019	3	Updated to include changes in the DOP
October 2021	4	Alignment to internal governance process and FICA
June 2023	5	Alignment to internal governance process and FICA
October 2023	6	Alignment to internal governance process and FICA

27. APPROVAL OF THE RMCP

27.1 This RMCP was recommended by the following committees:

a. The Policy and Process Change Committee (PPROCC) on 08 September 2023.

b. The Executive Committee (EXCO) on DD October 2023.

c. The Social and Ethics Committee (SEC) on DD October 2023.

27.2 This RMCP was approved by the Land Bank Board on DD October 2023.

Appendix 1:

The Land Bank FICA Checklists

Land Bank, in its capacity as an accountable institution, has a duty to verify the identity of all its clients in compliance with the Financial Intelligence Centre Act No 38 of 2001(FICA).

Know Your Client (KYC) documents are required for each client transaction. The requirements for each entity type are listed below:

I. Individuals

Required FICA documents	Checklist
Green, bar-coded Identity document or Smart ID Card (also used for PEPs/Sanctioned screening purposes) if not available valid reason why identity document could not be provided together with a valid Passport or valid driver's licence	
Valid Passport (for foreign nationals)	
Proof of physical residential address	
Authority to act (if applicable): power of attorney / letter of appointment from the court and Identity document, physical residential address and contact details of persons authorised to act	
Birth certificate (for minors under 18 years) and proof of authority (where minor is assisted by legal guardian)	

II. Unlisted South African Companies

Required FICA documents	Checklist
Certificate of Incorporation (CM1 or CoR 15.1/CoR 14.1)	
Certified copy of Change of Name, if applicable (CM9 or CoR 9.1 or 2)	
Notice of Registered Office and Postal Address (CM22 or CoR 21)	
Current list of Directors (CM29 or CoR 39) (also used for PEPs/Sanctioned screening purposes)	
Authority to act: Directors' Resolution and/or Delegation of Authority	
In respect of the Principal Executive Officer, each Director, each Authorised person, and each shareholder holding more than 25% of the voting rights of the company: - Certified copy of the Identity document - residential address and contact details	
Proof of physical business address and trading/operating name	
Beneficial ownership (warm body that owns the company) of the company. If the shareholder is another company, provide shareholder details and beneficial ownership. Process continues until we establish the ultimate beneficial owner. If the shareholder is a trust, the trust deed needs to be provided to identify and verify all trustees, founders and beneficiaries to the trust.	

III. Unlisted Foreign Companies

Required FICA documents	Checklist
Official Document of Incorporation (or CoR 17.1)	
Registration Certificate (CoR 17.3)	

If trading in RSA, documents for RSA unlisted companies	
Authority to act: Directors' Resolution	
Identity document/Passport, details of physical residential address and contact details of related parties and persons authorised to act (also used for PEPs/Sanctioned screening purposes)	
Proof of physical business address and trading/operating name	

IV. Listed Companies

Required FICA documents	**Checklist**
Registration Certificate (Registrar of Companies or equivalent regulator-foreign companies)	
Documentary evidence of listing (printout from the official website of the stock exchange on which the entity is listed is required)	
Authority to act: Directors' resolution	
Identity document proof of residence and contact details of persons authorised to act (also used for PEPs/Sanctioned screening purposes)	

V. Close corporations (CC)

Required FICA documents	**Checklist**
Founding Statement and Certificate of Incorporation (CK1)	
Amended Founding Statement (CK2), (If applicable)	
Authority to act: Members' Resolution	
Identity document, physical residential address and contact details of each member, persons authorised to act and of the Person Exercising Executive control over the CC. (also used for PEPs/Sanctioned screening purposes)	

Proof of physical business address and trade name	
Conversion of Close Corporation (If a Close Corporation converts to another entity type, the following forms are applicable)	
Form CoR 18.1 – Application to convert a Close Corporation	
Form CoR 18.3 – Registration Certificate	

VI. Trusts

Required FICA documents	**Checklist**
Trust Deed or other Founding Document and any other subsequent Deeds	
A Foreign Trust: an official document reflecting appointment of Trustees issued by an authority in the country where the Trust is created	
Authority to act: Letter of Authority from the Master of the High Court and Trustees' Resolution	
Identity document, physical residential address and contact details of each trustee, each beneficiary, the founder and the persons authorised to act (also used for PEPs/Sanctioned screening purposes)	
Proof of registered address of Master of High Court (stamp on letter of authority)	

VII. Partnerships

Required FICA documents	Checklist
Partnership Agreement	
Authority to act: Partners' Resolution	
Identity document, physical residential address and contact details of all the partners and persons authorised to act and of the Person Exercising Executive control of the partnership (also used for PEPs/Sanctioned screening purposes)	
Professional partnerships	
Partnerships consisting of more than (20) partners which are incorporated in terms of Section 30(2) of Company's Act 61 of 1963 which are recognized in terms of the relevant Government Gazettes examples are: Attorneys, Notaries and Conveyancers, Public Accountants and Auditors, Medical Practitioners, Pharmacists, Professional Engineers, Quantity Surveyors, Stockbrokers and Architect)	
Registration certificate (provide proof of registration of the partnership by a regulatory body)	
Partners Resolution (Authority to act)	
Identity document residential and contact details for Persons Authorised to Act and of the Person Exercising Executive control of the partnership (also used for PEPs/Sanctioned screening purposes)	
Proof of physical business address	

<u>Politically exposed person (PEPs)</u>

Politically exposed person or PEP is the term used for an individual who is or has in the past been entrusted with prominent public functions in a particular country. The principles issued by the Wolfsburg Group of leading international financial institutions give an indication of best banking practice guidance on these issues. These principles are applicable to both domestic and international PEPs.

The following examples serve as aids in defining PEPs:

- Heads of State, Heads of Government and cabinet ministers;
- influential functionaries in nationalised industries and government administration;
- senior judges;
- senior political party functionaries;
- senior and/or influential officials, functionaries and military leaders and people with similar functions in international or supranational organisations;
- members of ruling or royal families;
- senior and/or influential representatives of religious organisations (if these functions are connected to political, judicial, military or administrative responsibilities).

According to the Wolfsburg principles, families and closely associated persons of PEPs should also be given special attention by a bank. The term "families" includes close family members such as spouses, children, parents and siblings and may also include other blood relatives and relatives by marriage. The category of "closely associated persons" includes close business colleagues and personal advisers/consultants to the PEP as well as persons, who obviously benefit significantly from being close to such a person.

A bank should conduct proper due diligence on both a PEP and the persons acting on his or her behalf. Similarly, KYC principles should be applied without exception to PEPs, families of PEPs and closely associated persons to the PEP.

FICA defines a DPIP as the following:

A domestic prominent influential 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

<u>Source of Funds and Source of Wealth needs to be established for all PEP/DPIP/FPPOPEP/DPIP/FPPO.</u>

Proof of physical residential/business address

Any one of the following documents reflecting the physical/business address is acceptable

- Utility bill (must be less than 3 months old, unless otherwise specified)
- Current lease or rental agreement
- Bank statement
- Municipal rates and taxes invoice
- Valid television licence
- Mortgage statement
- Telkom account
- Valid motor vehicle licence
- Insurance policy
- Tax return (less than 1 year old)
- Letter from bank manager, medical practitioner, accountant, or attorney, on a formal letterhead, stating that they know the client for three years and confirming physical address
- Letter on letterhead, signed by board of trustees, directors' etc. confirming physical business address
- Correspondence from a body corporate or share block association ☐ Payslip or salary advice

All address verification documents must be valid and reflect the name and the current physical address of the client (legal property descriptions are also acceptable - e.g. erf/stand numbers).

Spouse/partner

Any of above documents for spouse, together with marriage certificate or if not available;

- Affidavit from person co-habiting with client, providing:
- Name, identity number and physical residential address of client and co-habitant
- Relationship between client and co-habitant
- Confirmation that residential address is shared

Parent:

- Any of above documents for parent
- Must be accompanied by the child's birth certificate (for a minor)

If above documentation not available:

Visit to physical address by a Land Bank employee, or

Affidavit from client (as a last resort), providing:

- Name, identity number and physical residential address
- Confirmation that client resides at physical residential address

Trade name (if this is not reflected on the proof of physical business address)

Any one of the following documents reflecting the Trade Name is acceptable

- An Original Company Letterhead
- Utility bill (less than three months old)
- Bank statement or financial statement from another financial institution (less than three months old)
- Valid lease or rental agreement (signed by all relevant parties)
- Municipal rates and taxes invoice (less than three months old)
- Mortgage statement from another financial institution (less than six months old)
- Telephone account i.e. a land-line or cell phone (less than three months old)
- An official tax return (less than one year old)
- An official tax assessment or official correspondence from the local revenue services (less than three months old)
- Valid television licence document
- A recent short-term insurance policy or a renewal letter (less than one year old)

DEFINITIONS

Principal Executive Officer

Refers to the principal executive officer such as the CEO, CFO, COO, MD, FD or any person who exercises executive control.

Authorised Persons

These are individuals who are authorised to act on behalf of the Company/Legal Entity and who are authorised to establish a relationship with Land Bank on behalf of the company/legal entity.

Authority of Individuals purporting to act on behalf of the Company/Legal Entity:

- Duly executed Board Resolution authorising the opening of an account/establishment of the business relationship/conclusion of the transaction and conferring authority on those who will establish the business relationship/conclude the single transaction; OR
- Certified extract of the minutes proving authority; OR
- Original letter signed by the company secretary on the official company letterhead

If a 3rd party is acting on behalf of the Client (Individual) the following is required:

- Proof of authority (i.e.) power of attorney, mandate, resolution, court order,
- Letters of appointment by the Master of the High Court
- Individual FICA above, for the person who is acting on behalf of the Client (together with all the FICA documentation of the Client)

Certified or Verified

We are required to hold originally certified/verified copies of the following documentation on record. Strictly, only clear, legible copies of identity and other documents will be accepted.

Please provide the original or certified copies of the following documentation for each shareholder holding 25% or more of voting rights at a general meeting of the company:

- South African (Pty) Company – Certificate of Incorporation and Notice of Registered Office and Postal Address, and a letterhead of the company;
- Listed Company – Latest Annual Report;
- Foreign Private Company: the official document reflecting the incorporation of the foreign company issued by the relevant registrar of companies or similar authority of the country of incorporation of the foreign company, reflecting the company's incorporation and bearing its name and number of incorporation and the address where it is situated for purposes of its incorporation, together with a letterhead of the company;
- Close Corporation – Founding Statement and Certificate of Incorporation and Amending Founding together with a letterhead of the close corporation.

Appendix 2:

AML Enhanced Due Diligence Template

Client

Mr X

Purpose

In terms of FICA, the Bank is required to screen all individuals/entities prior to entering into a transaction to establish if the individual/entity is a Politically Exposed Person (PEP)/Sanctioned.

Adverse media checks are also conducted to establish if the client poses any reputational risk to the Bank.

Methodology

The client was screened against the Dow Jones watch list to determine the PEP/Sanctioned status.

Further investigations were conducted (desk top Google search) to establish if there is any adverse media against the client.

Findings

Screening

List results

Adverse Media

State the adverse media findings

RECOMMENDATION

Due to there being no adverse media against Mr X there is a strong possibility that this client will/not expose the Bank to reputational risk and is therefore not considered a High-Risk client.

My recommendation is therefore to proceed/not proceed with xxxxx condition

Naweed Soofie

AML Compliance Officer

Date

Appendix 3:

STR Form

STR/TPR Report

Date: _____

Part A: Particulars of Person Making the report

Name and Surname: _____

Employee Number: _____

Contact Details: _____

BU: _____

Part B: Particulars of Transaction

Date of Transaction: _____

Type of Funds: _____

Client Account Number: _____

Client/Entity Name: _____

Client/Entity ID/Registration Number: _____

Amount of Transaction in Rand Value: _____

Part C: Particulars of Suspicious Activity

Please describe clearly and completely the events which led to the forming of the suspicion and the reasons thereof.

_____
_____

_____
_____

Kindly attach copies of all necessary documentation