CABS ANTI MONEY LAUNDERING MANUAL

Date Approved: AML Committee: **February 2024**

Date Approved: EXCO: **March 2024**

Date Noted at Board: **May 2024**

Related Information

CABS Anti Money Laundering Policy
CABS Sanctions Policy
CABS Compliance Policy

Policy Administration:

Contact person (Central Africa Building Society)

1. Farirayi Machawira
   Head, Compliance
   Central Africa Building Society
   Telephone +263 4 883823 ext. 1110
   Facsimile: +263 4 883804
   Email: FarirayiMachawira@cabs.co.zw

Document history

Revision Date	Doc Version	Summary of Changes	Author / Reviewer	EXCO Approval Date	Date noted at Board
16/03/14	1.0	Initial Draft	I. Musora	April 2014	April 2014
28/04/18	2.0	• New KYC requirements – added annexure 4 and inserted the SI No 23/2017 on Risk-based approach to KYC. • Sanctions screen • ing (refer to the new AML system) – see subsection. 10.3 • go AML regulatory reporting tool – see number 3 on duties of the compliance officer (pg. 18) • How we handle PEPS – Changed subsection 11.2 to include the approval process for account opening requests and cross-border transactions by PEPs. • Various provisions of the Money Laundering and Proceeds of Crime Act {Ch. 9:24}	I. Musora /F. Machawira		
17/08/18	3.0	• Incorporation of various provisions of the Money Laundering and Proceeds of Crime Act (Ch. 9:24)	I. Musora, F.Machawira	November 2017	November 2017
06/9/2019	3.1	• Removed S.I 23/2017 on a risk-based approach to money laundering. • Cosmetic changes to the document • Added responsibilities of the AML Committee (section 6)	I. Musora, F. Dzinoenda	September 2019	October 2019
26/06/20	4.0	Annual Policy Review	I. Musora,	9 July 2020	16 July 2020
07/08/21	5.0	Annual Policy Review	F. Dzinoenda I. Musora F. Machawira		
01/06/22	6.0	• Annual Policy Review • Amendment to s9 on Customer Due Diligence Requirements to increase the amount to USD 2,000. • Amendment to s 13 on Other High Customers to include Non-Governmental Organizations.	I. Musora F. Machawira T.Gunda.	June 2022	July 2022
01/01/24	7.0	• Annual Policy Review	J. Chikanga F.Machawira	March 2024	May 2024

Distribution List

Name	Position	Department
Machawira Farirayi	Head of Compliance	Compliance
CABS Compliance	Various	Compliance
AML Committee	Various	Various
All CABS Staff Members	All CABS Staff Members	Various
Phineas Calisto	Organization & Methods Manager	O & M
CABS EXCO	Members of the Executive Committee	Various

Mujekenjeki Eunice	Group Chief Risk Officer	Old Mutual Enterprise Risk management

1 Introduction

1.1 Central Africa Building Society, CABS (also referred to as the Society) is committed to upholding the highest standard of integrity and reputation concerning Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT).

1.2 CABS shall comply with relevant and applicable laws, rules and standards pertaining to Anti Money Laundering and Combating Financing of Terrorism (AML / CFT), considering the guidance provided by the:

1.2.1 Bank Use Promotion Act [Chapter 24: 24]

1.2.2 Money Laundering and Proceeds of Crime Act [Chapter 9: 24]

1.2.3 Banking Act [Chapter 24:20]

1.2.4 Suppression of Foreign and International Terrorism Act [Chapter 11:21]

1.2.5 Reserve Bank of Zimbabwe Anti-Money Laundering Guideline (2006)

1.2.6 Basel II Recommendations on KYC

1.2.7 FATF recommendations as incorporated in local legislation.

1.2.8 Financial Intelligence Unit Guidelines

1.3. CABS shall cooperate fully with local and international competent authorities and law enforcement agencies in combating money laundering and countering financing of terrorism.

1.4. CABS is committed to prevent its operations from being abused for money laundering or other financial crimes, including the financing of terrorism.

1.5. CABS values an impeccable reputation as a trustworthy financial institution and therefore will not enter relationships with individuals or organizations engaged in or suspected of illegal or unethical activities. New customers are accepted with due care and CABS operations shall be protected at all times from being abused by criminal organizations or individuals.

2 Scope and Applicability

2.1 This manual shall apply to all operations and departments under CABS including retail branches, agency banking and third-party service providers.

2.2 The manual also applies to all products and services offered by CABS. The approach towards the management of AML/CFT compliance within CABS shall be similar to the management of other types of risk, which is premised on three lines of defence as follows: -

2.2.1 First line of defence - Business Units

2.2.2 Second line of defence - Risk control units, Compliance Function and Risk Management

2.2.3 Third line of Défense –CABS Internal Audit; Group Internal Audit [GIA]

3. Overview of Money Laundering and Financing of Terrorism Risk

3.1 Definition of Money Laundering

3.1.1 Money laundering covers all activities and processes that change the identity of illegally obtained money so that it appears to have originated from a legitimate source.

3.1.2 The Money Laundering and Proceeds of Crime Act defines money laundering as 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 of assisting any person who is involved in the commission of a serious offence to evade the legal consequences of his or her acts or omission.

3.1.3 Financing of terrorism involves any transactions linked to terrorists' activities. The funds used may be legitimate and not necessarily owned by terrorists, but the focus is on the primary intention which is to assist terrorist activities. Essentially, financing terrorism involves providing or collecting property for carrying out an act of terrorism, providing services for terrorism purposes or arranging for retention or control of terrorist property.

3.1.4 Participation in, association with or conspiracy to commit, an attempt to commit, aiding, facilitating and cancelling the commission of money laundering offences by any person is an offence.

3.1.5 Any person who by any means, directly or indirectly, provides or collects funds, or attempts to do so with the intention that they should be used or in the knowledge that they are to be used in whole or part to facilitate terrorist actions commits an offence.

3.2 Stages of Money Laundering

3.2.1 **Placemen**t - The criminal introduces illegal profits and ill-gotten gains into the financial system. (This is the physical disposal or dealing of the initial proceeds derived from illegal activities)

3.2.2 **Layering** - In this phase, the criminal engages in a series of conversions or movements of the funds to distance them from the initial identifiable source. The illicit proceeds are separated from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide an appearance of legitimacy including anonymity.

3.2.3 **Integration** - Once layering succeeds, the criminal proceeds have been successfully laundered, "cleaned" and are regarded for all intent and purposes as legitimate funds and then reintroduced, i.e., brought back into the financial system through investment, purchase of assets, etc.

4. Anti-Money Laundering and Combating Financing of Terrorism Compliance Program.

4.1 Requirements of the AML/CFT program

The AML/CFT legislation stipulates that CABS develops and implements an AML/CFT program for the prevention of ML/TF risk. CABS therefore operates in line with a board-approved AML Compliance program which involves.

4.1.1 Internal policies, procedures and controls for customer due diligence, record keeping, on-going monitoring, reporting of suspicious transactions, records retention and co-operating with law enforcement requests for information, reviews, audits and investigations.

4.1.2 Ongoing training for officers and employees to make them aware of the MLPC Act and other laws relating to money laundering and the financing of terrorism, with a view to assisting them to recognize transactions and actions that may be linked to money laundering or financing of terrorism and to instruct them in the procedures to be followed in such cases.

4.1.3 Policies and procedures to prevent the misuse of technological developments including those related to electronic means of storing and transferring funds or value.

4.1.4 Independent audit arrangements to review and verify compliance with and effectiveness of the measures taken in accordance with the MLPC Act.

5. Roles and responsibilities

5.1 The CABS Board of Directors, through the Anti-Money Laundering Committee (AMLCOM) shall be responsible for overseeing the overall management of AML/CTF compliance risks, including the approval and implementation of AML/CFT measures.

5.2 The Board shall.

a. Ensure necessary steps are taken to rectify AML/ CFT issues effectively and expeditiously,
b. Determine the risk appetite with regards to AML/ CFT and
c. Approve and adopt AML policies and manuals.

5.3 The Board shall designate a Compliance Officer at the management level to be responsible for the fulfilment of and ongoing compliance with the provisions of the Act.

5.4 The Compliance Officer shall have ready access to all the books, records and employees of the institution as is necessary to fulfil his or her responsibilities which include:

a) Ensuring proper and accurate implementation and compliance with board approved AML/CFT Policies, procedures and controls.

b) Creating and retaining records as stipulated by legislation.

c) Responding to RBZ/ FIU enforcement requests.

d) Ensuring that requisite interpretation and training regarding the AML/CFT program is provided.

e) Reports are properly filed as required by the Reserve Bank of Zimbabwe (RBZ) and the Financial Intelligence Unit of Zimbabwe (FIU).

f) Reviews are carried out as needed and are as thorough as possible based on the CABS" risks profile and the RBZ/ FIU regulations.

g) Provide a risk view of AML/CTF compliance to the Board and Board Risk Committee on a quarterly basis.

5.5 Senior Management shall formulate a strategic direction to counter money laundering and terrorist financing activities. They shall:

a) Evaluate AML/CFT internal controls effectiveness and adequateness.

b) Approve business relationships with high-risk customers based on enhanced customer due diligence (CDD) process.

c) Develop clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher risk.

d) Ensure that these policies will consider factors such as customers" background, country of origin, public or high-profile position, linked accounts, business activities or other risk indicators that may be identified.

e) The level of the required due diligence should be related to the level of identified risks.

5.6 Business units shall be responsible for the day-to-day management of compliance with AML/CFT inherent in their operation and activities. The duty of vigilance consists mainly of the following:

a) Customer Due Diligence (CDD), including verification of identity.

b) Recognition and reporting of suspicious customers / transactions to the Money Laundering Reporting Officer. (Annexure 1 - STR Template).

c) Keeping of records.

5.7. Compliance Function shall be responsible for formulating and disseminating a Board approved AML/CTF Management Framework for CABS which involves:

a) Ensuring appropriate implementation of AML/CFT procedures regarding customer due diligence, Sanctions screening, record keeping, on-going monitoring, reporting of suspicious transactions, records retention and reporting.

b) Review the risk assessment process of money laundering and financing of terrorism with regard to new products or services including the introduction of new technology and processes.

c) Develop specific money laundering/ financing of terrorism indicators that assist in detecting money laundering/ financing of terrorism.

d) Co-operating with law enforcement requests for information, reviews, audits and investigations.

e) Assemble and distribute information, policy and procedure related to AML/CFT measures and channel of reporting to key personnel, front line staff, relevant department/ functional heads and branches.

f) Assist in the provision of AML/CFT training.

g) Ensure records concerning AML/CFT matters are properly kept including maintenance of the Politically Exposed client register.

h) Compliance monitoring of the effectiveness of processes for ongoing compliance with the Money Laundering and Proceeds of Crime Act, all subordinate legislation and guidance issued by the FIU through appropriate metrics.

i) Carrying out regular assessments of the adequacy of the systems and controls for effective ML/ TF risk management.

j) Bring to the attention of senior management the areas where the application of AML/CTF controls should be improved and provide guidance in that regard.

k) Reviewing, and updating the Compliance program as necessary due to changes in laws or regulations and ensuring that all affected employees have been advised of these changes.

5.8 Internal Audit shall be responsible for conducting independent reviews of the compliance framework and effectiveness of the AML/CFT measures undertaken on a periodical basis. Internal Audit will perform reviews to assure the design and effectiveness of the processes and controls implemented by CABS to discharge its obligations in terms of the AML/CFT Compliance Program.

6. The Anti-Money Laundering Committee ("AMLCOM").

The mandate to oversee the implementation and monitoring of Anti Money Laundering

("AML") legislation and Regulations and to ensure that oversight on the Bank's AML

compliance management is adequate.

The terms of reference of the AMLCOM set out the roles, responsibilities, and authority of the AMLCOM as delegated by the Board of Directors, and the rules of procedure that will guide the Committee in the performance of its functions.

6.1 General Purpose and Authority.

The AMLCOM is constituted for the following purposes:

a) To oversee and implementation of the Bank's Money Laundering and Terrorist Financing Prevention Program ("the Programme").

b) To oversee and recommend to the Board the adoption of a comprehensive and risk-based programme geared towards the promotion of high ethical and professional standards and the prevention of the Bank being used, intentionally, or unintentionally, for money laundering and terrorism financing.

c) Management of the implementation of the Programme shall remain the primary task of the CABS Compliance Function.

The AMLCOM shall have oversight over the following Compliance Functions:

d) It shall conduct periodic compliance monitoring which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in money laundering and terrorist financing prevention, reporting channels, effectiveness of the automatic money laundering transaction monitoring system and record retention system through sample testing and review of audit or examination reports. It shall also report compliance findings to the AMLCOM.

e) Ensure that breaches, discovered either by Audit or FIU are remediated.

f) Inform all responsible officers and employees of all resolutions, circulars and other issuances by the FIU, in relation to matters aimed at preventing money laundering and terrorist financing.

g) Alert the CABS EXCO, AMLCOM and the Board of Directors if it believes that the institution is failing to address anti-money laundering and terrorist financing issues; and

h) Organize the content of AML/CFT training of officers and employees including regular refresher training.

7. Assessment of Money Laundering and Terrorist Financing Risk

7.1 CABS is required to take appropriate steps to assess ML/TF risk in its day-to-day operations as per the requirements of the Money Laundering and Proceeds of Crime Amendment Act.

7.2 The Society will be expected to pay due regard to the findings of the National Risk Assessments and to implement applicable AML/CFT measures commensurate with the risks identified.

7.3 The Society will be required to carry out regular AML/CFT risk assessments and to keep records thereof. Based on the risk assessments, the Society will further be required to implement prescribed AML/CFT measures commensurate with the identified risks as per the Risk-Based Approach. The Society will be permitted to implement simplified or reduced measures for low-risk customers, products, services or situations provided that these simplified measures shall not be less than the prescribed AML/CFT measures

7.4. Before launching any new product, service, business practice, technological innovations new and existing products, the Society will be required to seek an AML/CFT assessment from Compliance. This assessment entails documenting the money laundering and terrorist financing risk posed by such products, services, business practices or technology and for the Society to put in place adequate measures to mitigate the risk.

7.5. The Society will be required to review and update its ML/TF risk assessment regularly to consider material changes in risk factors and shall maintain records of such reviews and updates.

7.6. The nature of these ML/TF risks in CABS relates to several aspects, including the:

a) Features of the intended target market of clients who are likely to use the range of products and services.

b) Geographic locations of CABS operations and clients.

c) Delivery channels through which persons become clients of CABS or through which clients access our products and services; and

d) Features of a particular product or service.

8. Risk Based Approach (RBA) to AML/CFT

8.1 The Money Laundering and Proceeds of Crime Act recommends CABS adopt the risk-based approach which involves.

a) identifying and assessing relevant money laundering and terrorist financing risks.

b) designing and implementing controls to manage and mitigate the assessed risks.

c) Monitoring and improving the effective operation of these controls.

8.2 The general principle of an RBA is that, where there are higher risks, CABS should take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted.

8.3 The key elements of the RBA approach to AML/CFT are:

a) Business, Product and Customer Risk Assessment.

b) Defining, documenting and evaluating inherent and residual risk.

c) Categorization of client risk, e.g., High, Medium, Low.

d) Allocation of risk categories to client types and products.

e) Designing risk reduction procedures, key controls and monitoring controls concerning client identification and verification, transaction monitoring and reporting; and ongoing monitoring of the client relationship during the client lifecycle (including termination of business relationship with a client).

9. Customer Due Diligence Requirements

9.1 Customer due diligence is a vital pillar in managing ML/TF risk in CABS. In terms of the Money Laundering and Proceeds of Crime Act, satisfactory evidence of the identity of customers, purpose and intention underlying the business relationship should be known. Know your client (KYC) requirements for the various CABS client types have been included in Annexure 2.

9.2 A Customer Includes:

a) The person or entity that maintains an account with CABS or those on whose behalf an account is maintained (i.e., beneficial owners).

b) The beneficiaries of transactions conducted by professional intermediaries.

c) Any person or entity connected with a financial transaction who can pose a significant reputational or other risk to CABS.

d) The person or entity that maintains an account with CABS or those on whose behalf an account is maintained (i.e., beneficial owners).

e) The beneficiaries of transactions conducted by professional intermediaries; and any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

9.3 CABS shall identify its customers and verify a customer's identity through identity document(s) in the following instances.

a) Opening an account for or otherwise establishing a business relationship with a customer.

b) Walk in non-customer carrying out a transaction in an amount equal to or exceeding the set reporting threshold, whether conducted as a single transaction or several transactions that appear to be linked.

c) Doubt exists about the veracity or adequacy of previously obtained identity documents.

d) There is suspicion of money laundering or financing of terrorism involving the customer or the customer's account.

9.4 The identification and verification of the identity of each customer and obtaining other information required above shall take place.

a) Before the establishment of an account, or of a business relationship.

b) Before the carrying on of further business, if money laundering or financing of terrorism is suspected; or

c) if doubts exist about the veracity or adequacy of previously obtained identity documents

9.5 The identification and verification requirements will apply on a risk-sensitive basis depending on the type and nature of the customer; Business relationship; Product and Transactions.

9.6 An Individual's identity comprises of full name, date of birth, current permanent residential address, the nature of business that the individual is involved in and normal financial transactions.

9.7 Whenever CABS is required to identify a customer, it must establish and verify the identity of the ultimate natural person who owns or controls the customer or its assets or on whose behalf the transaction is carried out or the business relationship is established.

9.8 In the case of non-residents making face-to-face contact, the Society is required to verify the identity and current permanent address of the applicant diligently.

9.9 Non-Residents applying from abroad are required to complete the standard application form, which should incorporate their accurate personal details as per the application form. The completed application must be accompanied by supporting KYC documents notarized by a notary public.

9.10 CABS may proceed with account opening for foreign and non-resident Zimbabweans on the understanding that all due diligence requirements are met.

9.11 CABS shall take adequate measures to address the risk of money laundering and financing of terrorism in the event they conduct business relationships or execute transactions with a customer who is not physically present for purposes of identification.

9.12 CABS may rely on intermediaries or other third parties to perform customer identification on condition that the third parties shall supply client data without delay and that CABS does not suspect any money laundering activities on the account. Please note that according to the Money Laundering and Proceeds of Crime Act compliance with this requirement does not relieve CABS from ultimate responsibility for compliance with all other stated due diligence requirements.

10. Risk-Based Approach to Customer Due Diligence.

10.1 A risk-based approach to Customer Due Diligence ("CDD") takes several discrete steps in assessing the most effective and proportionate way to manage the money laundering and terrorist financing risks faced by a Designated Institution. The risk assessment of a particular customer will determine:

a) Any additional information that needs to be requested

b) How that information will be verified and for whom; and

c) The extent to which the relationship will be monitored.

10.2 CDD information comprises both identification and relationship information. To enable a customer profile to be created , collect relevant CDD information on a risk-sensitive basis.

10.3 Where a customer poses a low risk, a set of Simplified Customer Due Diligence (SCDD) measures which reflects the accepted low risk of money laundering or terrorist financing that could arise from such business is adopted. Prior to applying SCDD, CABS must conduct and document appropriate testing to be satisfied that the customer or business qualifies for the simplified treatment under this policy.

10.4 CABS may apply enhanced due diligence (EDD) measures based on risk assessment, thereby requiring intensive „due diligence" for higher risk customers especially when.

the monies are to be paid out into an account other than one in the name of the original applicant particularly when the proceeds are to be paid to a third party. The examples of customers requiring higher due diligence include Politically Exposed Persons (PEPs), Correspondent banking institutions, and Car sale dealers.

10.5 Ongoing Customer Due Diligence (OCDD) means regularly reviewing customer information and having systems to conduct account monitoring. This is required for all existing customers. OCDD will help the Society to identify, mitigate and manage any money-laundering or terrorism-financing risks that may arise from providing one or more designated services to its customers. It complements the Society's KYC processes and allows it to minimize the risk of its products or services being used to facilitate money laundering or terrorist financing activities.

10.6 It will assist the Society to respond to any AML/CFT risks that may arise from the provision of any designated service(s) to customers at any stage after the initial customer identification.

11. High Risk Customers & Politically Exposed persons (PEPs)

11.1 CABS shall have an appropriate risk management system to identify customers whose activities might pose high risk of money laundering and financing of terrorism. It shall also exercise enhanced identification, verification and on-going due diligence procedures for such customers as well as determine if a customer or beneficial owner is a politically exposed person.

11.2 When dealing with a PEP, the institution shall.

a) Obtain approval from senior management and the AMLCOM before establishing a business relationship with the customer or later as soon as the existing customer or beneficial owner is identified as PEP.

b) Take all reasonable measures to identify the sources of wealth and or funds and other assets of the customer.

c) Provide increased monitoring and on-going monitoring of the customer and the business relationship to prevent money laundering or the commission of other offences.

11.3 Politically exposed persons include –

a) any person who is or has been entrusted in Zimbabwe with prominent public functions, including but not limited to, a Head of State or government, a senior government, judicial or military official, a senior executive of a state-owned corporation, or a senior official of a political party; or

b) any person who is or has been entrusted with prominent public functions by a foreign country, including but not limited to a Head of State or government, a senior government, judicial or military official, a senior executive of a state-owned corporation, or a senior official of a political party or

c) any person who is or has held a position as a member of senior management of an international organisation, holding the position of director, deputy director, member or board or equivalent functions; or

d) any close associate, spouse or family member of a person referred to in the paragraphs above.

11.4 All cross-border transactions belonging to PEPs should be referred to Compliance.

11.5 PEP status itself does not automatically mean that the individual is corrupt or they have been incriminated in any corruption. However, their office and position can leave them vulnerable to corruption. The risks increase when the person concerned is from a country with widely known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards, or where these do not meet international financial transparency standards.

11.6 Zimbabwe as a jurisdiction faces considerable reputational damage should any of its Designated Institutions have a business relationship with customers of this nature involving the proceeds of foreign corruption. CABS can reduce risk by conducting detailed CDD at the outset of the relationship and on an ongoing basis where it is known or suspected that the business relationship is with PEP.

11.7 CABS staff should be most vigilant where our customers are involved in those businesses which appear to be most vulnerable to corruption, such as, but not limited to, oil, construction or arms sales. New and existing customers may not initially meet the definition of PEP.

11.8 CABS staff should, as far as practicable, be Monitor public information and market intelligence for potential changes in the position of CABS customers due to political exposure. If an existing customer is later discovered to be PEP, senior management consent to maintain the relationship must be obtained.

11.9

11.10 Before a payout of the proceeds of an insurance policy, the Society will be required to take measures to determine whether the beneficiary/beneficial owner of the beneficiary is a politically exposed person where higher risks are identified, the Society will need to:

a) conduct enhanced scrutiny of the whole business relationship with the policyholder.

b) ensure that senior management is informed before paying out; and

c) Consider submitting a suspicious transaction report.

12. Customer Identification and account opening for cross Border Correspondent Banking Relationships.

12.1 When providing cross-border correspondent banking services, CABS shall be required to put measures in place that demonstrate that the Society has satisfied itself that where any of their accounts to be dealt with by the correspondent are adequately "KYC" verified and can provide on request all information obtained on such customers of banks.

12.2 CABS shall obtain senior management approval before establishing a correspondent banking relationship.

12.3 CABS shall verify the identity of respondent financial institutions with which it conducts correspondent banking relations.

12.4 CABS shall evaluate controls implemented by the respondent financial institution concerning money laundering and combating the financing of terrorism.

12.5 Persons engaged in business of purchasing and selling motor vehicles, whether new or second-hand , are categorized as a designated non-financial businesses or professions. Such clients are therefore treated as high-risk clientele.

13. Other high-risk clients.

Persons engaged in the following business activities are to be treated as high-risk customers; buying and selling motor vehicles whether new or used, Casinos, Real estate agents, Dealers in precious metals and precious stones, Money Service Business, Lawyers, Notaries, Other independent legal professionals, Non-Governmental organizations and accountants, Trust and service providers.

14. Forbidden business

Payable through accounts and relationships with shell banks are forbidden for CABS and its correspondent banks.

15. Source of Funds, Income and Wealth.

15.1 The source of funds refers to the activity that generates the funds for a particular business relationship or occasional transaction. This could be an insurance payout that a client decides to invest. CABS shall take the necessary measures to determine the source of funds when establishing any business relationships with a client or carrying out a once-off transaction per the requirements of the Money Laundering and Proceeds of Crime Act. The source of funds must be consistent with the risk profile of the client and their business.

15.2 This may also refer to an activity that provides a regular supply of money to a potential client. This can be a pension, employment or investment. Knowing the source of income is necessary in every case as this provides a basis upon which suspicious activities can be identified as well as establishing the risk profile of a customer.

15.3 The source of wealth describes the activities that have generated the total net worth of a person. This can be a significant inheritance coupled with savings from salary for 30 years. To establish the source of wealth one must look further into the history of the client . CABS must identify the source of wealth to ensure that the wealth originates from legitimate sources.

15.4 CABS must establish the source of funds of each transaction as well as the source of wealth of the underlying customer(s) to adequately assess the risk of exposure to money laundering or terrorist financing.

16. Client Account Monitoring

16.1 Ongoing monitoring of clients" accounts must be implemented to detect unusual/suspicious transactions.

16.2 Ongoing monitoring is essential to ensure effective and sound ML/TF risk management.

16.3 CABS can effectively manage its risks if It learns the usual and reasonable transactional patterns of its clients.

16.4 CABS is required to identify attempted and unusual transactions which fall outside the regular pattern of the client's expected activity.

16.5 Ongoing monitoring of business transactions and relationships will be carried out in a in accordance with the risk identified in the CABS risk assessment and its CDD efforts.

16.6 Enhanced monitoring will be adopted for higher-risk clients or transactions.

16.7 One component of OCDD is the Society's collection and verification of additional KYC information which shall be conducted annually for high-risk customers, every two years for medium risk customers and every three years for low-risk customers.

17. Sanctions

17.1 Sanctions are political trade restrictions placed against target countries by competent authorities. Examples are economic sanctions (e.g., a ban on trade); international sanctions (e.g., coercive measures adopted by a country or countries against another State to elicit a change in that State's behaviour); legal sanctions (e.g., penalties imposed by courts); sanctions imposed on financial institutions; embargoes on exporting or supplying arms, and associated technical assistance, training and financing to target countries.

17.2 The Compliance Function was constituted to give effect to CABS, its shareholders and other stakeholders‟ decisions on conducting business in embargoed/sanctioned jurisdictions and/or with sanctioned entities or individuals. CABS compliance function considers all relationships; transactions or activities involving sanctioned entities with new or existing customers/counterparties.

17.3 The main operational element of the CABS sanctions compliance programme is screening current and potential customers against sanctions lists embedded in the automated Anti Money Laundering system.

17.4 Where screening identifies a potential match (for example between a customer and a name on a sanctions list), CABS must investigate these thoroughly to determine whether the match is true (i.e., the customer and the sanctions list entry appear to be the same person/entity). If the match is true, CABS will either refuse to establish business relationships with the person (Legal or Natural)

17.5 Reserve Bank of Zimbabwe directive dated 15 August 2013 AML /CFT Directive 1 / 2013 Directive to Financial Institutions and Designated Non-Financial Business and Professions on Freezing of Assets of Designated Persons and Entities requires CABS to among other things, to freeze without delay the funds or other assets of any person or entity designated by or under the authority of the United Nations Security Council and further to ensure that no funds or other assets are made available, directly or indirectly to or for the benefit of such designated person or entity. Any decision taken by the compliance function is risk-based, final and binding on the business units concerned.

18. Suspicious and Unusual Transaction Reporting

18.1 CABS will report all confirmed suspicious transactions and unusual activities to the Financial Intelligence Unit (FIU) following the AML legislation and Guidelines. CABS undertake to cooperate with authorities to the extent permitted by applicable customer confidentiality obligations.

18.2 CABS will establish and maintain policies, procedures and controls to ensure that per regulatory requirements, all staff report information or matters which come to their attention during business activities and which give reasonable grounds for suspicion of money laundering activities.

18.3 Many factors are involved in determining whether transactions are suspicious including the amount, the location of the business, who the transactions involve and what the legislation and Guidelines state as being suspicious.

18.4 Zimbabwe AML legislation and Guidelines require CABS as a designated institution to file a Suspicious Transaction Report within 72 hours for any transaction or pattern of transactions where there is reason to suspect:

a) Involves funds or assets derived from illegal activity or is intended to hide funds derived from illegal activity.

b) Is structured to avoid recordkeeping or reporting requirements.

c) Has no business or apparent lawful purpose; or

d) Aids and abets criminal activity.

18.5 Suspicious Transactions Reporting Procedures - CABS staff shall unabatedly observe the Know Your Customer Principle. It should be noted that suspicion in the anti-money laundering framework is determined by context, that is; what is suspicious for one customer account may not necessarily be suspicious for another. Suspicion of potential money laundering may be based on timing, size, and quantity of transaction or cash involved.

a) The reporting officer is expected to diligently assess the transactions according to the circumstances. They are then expected to apply the "**know your customer** principle.

b) CABS staff is required to promptly report suspicious transactions directly to the compliance officer responsible for money laundering.

c) The suspicious transaction report (STR) should be reported no later than two days from the time the activity is detected following the AML legislation in the prescribed format **(see Annexure 1)**

d) The form must be completed in full giving all details of the basis of suspicion. The customer's KYC details and other relevant supporting documentation must be attached.

d) The reporting staff member is not allowed to discuss the suspicion raised on a customer with anyone else other than the compliance officer responsible for anti-money laundering or any other member of the CABS Compliance Function.

e) Staff members are not allowed to inform or tip off the concerned customers on the transactions being reported as suspicious.

18.6 Compliance officer will.

a) Analyse information submitted on suspicion of money laundering.

b) Acknowledge receipt of all submitted reports.

c) Report the suspicious activity or transaction within 72 hours from the time of detection. The details of the STR together with all the relevant supporting documents are then uploaded onto the GoAML regulatory reporting tool. An acknowledgement of receipt is then sent once the report has been successfully uploaded.

d) Compliance function serves as a point of reference within the in the bank as well as interface with law enforcement agencies and supervisory authorities on money laundering matters.

e) In terms of the Bank Use Promotion and Suppression of Money Laundering Act no employee shall be liable to any civil or employment-related sanction for making a report on a suspicious transaction, provided the same was made in good faith and believing that the information was substantially true.

f) Members of staff are not allowed to report suspicious transactions directly to law enforcement agencies outside the reporting chain provided above.

19. Training and Awareness

19.1 All CABS employees will be trained on the legislation, internal rules and business entity processes.

19.2 Anti-Money Laundering and anti-terrorist financing training must be included in induction training. Employees are to receive appropriate training concerning AML/CTF compliance requirements before facing clients or conducting transactions.

19.3 Refresher training will be provided when required.

19.4 Training should be documented, including the date of the training, name of the trainer/trainee and content of training.

19.5 Training shall be afforded to all staff members on an annual basis. Attendance registers shall be kept by compliance officer, head of unit/branch manager as well as training manager.

20. Record Keeping Obligations

Records must be kept of all transaction data and data obtained for identification and CDD measures; all documents related to money laundering topics (e.g., files on suspicious activity reports); account files and business correspondence; the results of any analysis undertaken; documents relating to business relations and executed transactions as well as correspondence with clients and other persons with whom CABS maintains a business relationship with.

These records must be kept for a minimum of five years. The five-year period is calculated following the carrying out of the transactions or the end of the business relationship.