



GUIDANCE NUMBER: SECZ/LSS 21/09/2022

Subject: Anti-Money Laundering, Combating Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF) Guidelines on Customer Acceptance Process Flow, 2022

Scope: All Securities Market Intermediaries (SMIs)

Circulated: 21 September 2022

A handwritten signature in black ink, appearing to read "Any", is written over a horizontal dashed line.

Signed: Anymore Taruvinga
(Chief Executive Officer)

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS	2
DEFINITIONS	3
1. INTRODUCTION.....	4
2. RISK ASSESSMENT APPLYING A RISK -BASED APPROACH.....	5
3. GOVERNANCE AND COMPLIANCE.....	6
4. CUSTOMERS ONBOARDING PERSONNEL.....	8
5. KNOW YOUR CUSTOMER (KYC) PROCESS.....	9
6. RECORD KEEPING; CUSTOMER DUE DILIGENCE RECORDS	22
7. DECISION OUTCOME-OPEN ACCOUNT OR DENY APPLICATION	23
8. ONGOING MONITORING DUE DILIGENCE	23
9. ANNUAL AML/CFT/CPF REVIEW	24
10. REFERENCE	24
APPENDIX 1: EXAMPLE OF SUSPICIOUS TRANSACTIONS IN THE SECURITIES SECTOR	25

ACRONYMS AND ABBREVIATIONS

AML	Anti-Money Laundering
BO	Beneficial Ownership
CDD	Customer Due Diligence
CFT	Counter Financing of Terrorism
CPF	Counter Proliferation Financing
CIP	Customer Identification Program
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ID	Identification
KYC	Know Your Customer
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
PEPs	Politically Exposed Persons
PF	Proliferation Financing
SECZ	Securities and Exchange Commission of Zimbabwe
SOF	Source of Funds
SMIs	Securities Market Intermediaries
SOW	Source of Wealth
TF	Terrorist Financing

DEFINITIONS

For purposes of this Guideline:

Act- means the Money laundering and Proceeds of Crime Act [Chapter 9:24]

Beneficial owner - has the meaning given to it in terms of the Money Laundering and Proceeds of Crime Act [Chapter 9:24].

Business relationship - means any business, professional or commercial arrangement or proposed arrangement where the purpose or effect of the arrangement is to facilitate a transaction on an occasional, frequent, habitual, or regular basis between a customer and Securities Market Intermediary.

Customer - has the meaning given to it in terms of the Money Laundering and Proceeds of Crime Act [Chapter 9:24].

Competent Supervisory Authority - has the meaning given to it in terms of the Money Laundering and Proceeds of Crime Act [Chapter 9:24].

Customer Due Diligence (CDD) - means the measures taken to know and understand a customer and a beneficial owner of a customer which measures includes the process of collecting, analysing, and verifying information in order to identify and verify the identity of the customer or beneficial owner.

Enhanced Due Diligence (EDD) – is the additional analysis and cautionary measures aimed at identifying customers & confirming that their activities and funds are legitimate. It is additional level of risk identified at the time of performing customer due diligence checks and is associated with high-risk customers.

Know Your Customer (KYC)- means a process of being able to identify whom your customer is before entering into a new relationship.

Money Laundering Reporting Officer (MLRO) – is the first point of contact if you suspect money laundering or terrorist financing from a client in your sector. A compliance professional who oversees the SMI's AML/CFT/CPF framework.

Politically Exposed Person - has the meaning given to it in terms of the Money Laundering and Proceeds of Crime Act [Chapter 9:24].

Securities Market Intermediaries - refers to persons licensed in terms of section 38 of the Securities and Exchange Act [Chapter 24:25].

Serious Offence means - any offence referred to in section 2 of the Money Laundering and Proceeds of Crime Act [Chapter 9:24].

Unlawful activity - means any act or omission that if committed in Zimbabwe or any other country would constitute a criminal offence.

1. INTRODUCTION

- 1.1 This guideline is issued pursuant to:
 - a) Section 3(3) of the MLPC Act which empowers the Commission to supervise SMIs to comply with AML/CFT/CPF requirements;
 - b) FATF Recommendation 34 which requires supervisors to establish guidelines which will assist SMIs in applying AML/CFT/CPF measures in detecting and reporting suspicious and unusual transactions; and
 - c) Paragraph 21 of the First Schedule of the Securities and Exchange Act [Chapter 24:25] which authorises the Commission to formulate guidelines and notices.
- 1.2 This guideline is aimed at clarifying and explaining the KYC, CDD, and EDD requirements to help Securities Market Intermediaries ("hereinafter called SMIs") to understand and apply these requirements in compliance with AML/CFT/CPF laws and regulations.
- 1.3 This guideline is expected to be read in conduction with sections 15 to 23 of the Money Laundering and Proceeds of Crime Act [Chapter 9:24] and FATF Recommendations 9 to 23.
- 1.4 Further, the guideline is consistent and reflects on the Recommendations and guidance papers issued by the Financial Action Task Force ("FATF") and relevant international best practices.
- 1.5 To ensure preparedness for money laundering, terrorist financing, and proliferation risks, SMIs, particularly their front-line, customer-facing, relationship management, customer engagement, and customer support employees, as well as compliance/Anti-money laundering officers must take appropriate steps to identify, understand and assess the risks of money laundering, terrorist financing, and proliferation financing.
- 1.6 There is a need to conduct ongoing monitoring of customer transactions and accounts, taking into consideration risk factors, including those relating

to their customers' geographic areas, products, services, transactions, or delivery channels.

- 1.7 SMLs must also have in place policies, controls, and procedures to mitigate and effectively manage these risks of money laundering, terrorist financing, and proliferation financing.

2. RISK ASSESSMENT APPLYING A RISK BASED APPROACH

- 2.1 FATF Recommendation 1 requires SMLs to put in place appropriate processes to identify, assess, monitor, manage and mitigate ML/TF/PF risks affecting their businesses. The risk assessments should be documented as they serve as a basis for developing the SMI's AML/CFT/CPF Risk Management and Compliance Program. When identifying aspects of business that make SMLs susceptible to ML/TF/PF risks the following factors should be considered:

- a) the nature, size, and complexity of the business;
- b) type of customers and communities with whom they do business;
- c) countries or jurisdictions from where customers come from;
- d) products and services offered;
- e) delivery channels and business practices; and
- f) type of institutions the SMLs have business dealings with.

- 2.2 On the onboarding stage, the customer needs to be risk rated and SMLs should have an in-house risk rating tool. Customers may be given a risk rating in accordance with the risk he or she may present to the institution. Risk ratings can be in the form of a category, such as "low risk", "medium risk" or "high risk", or a numeric value derived from a risk matrix based on a pre-defined set of criteria. This will should be inbuilt into the compliance manual of the SMI.

- 2.3 A risk rating helps an SMI in deciding how and when to apply the appropriate checks, treatment, and controls that are commensurate to the level of risk. The following is an example of risk assessment scoring that SMLs can use to risk rate their customers.

0, <3	Low Risk
=>3, <5	Moderate Risk
5 or above 5	High Risk

- 2.4 In compliance with FATF Recommendation 15, SMIs must identify and assess ML/TF/PF risks that may arise in relation to the development of new products, business practices, new delivery channels, and the use of new or developing technologies for both new and pre-existing products.

3. GOVERNANCE AND COMPLIANCE

Role of the Board

- 3.1 The Board of Directors of an SMI has oversight accountability for approving policies and procedures and monitoring the effectiveness of the AML/CFT/CPF Risk Management and Compliance Program on a regular basis. It is the responsibility of the Board to ensure compliance by SMI and its employees with the provisions of the MLPC Act and the SMI's AML/CFT/CPF Risk Management and Compliance Program.

Role of Senior Management

- 3.2 Senior Management is responsible and accountable for exercising oversight on the day-to-day implementation of the AML/CFT/CPF Risk Management and Compliance Program to ensure that it is adequate to mitigate ML/TF/PF risks and that it is implemented effectively in all relevant business areas.
- 3.3 Senior Management should ensure that:
- a) an appropriately qualified person of sufficient competence appointed as an MLRO/Compliance Officer to be responsible for the implementation of, and ongoing compliance with, this Act by the institution;
 - b) the Commission is notified in writing of the appointment of an MLRO and furnished with a detailed curriculum vitae of the MLRO and a full description of the duties of the MLRO;
 - c) the MLRO is resident in Zimbabwe;
 - d) the Commission is informed in writing of the termination of services of an MLRO and provided with an explanation of the reasons for the termination, within 15 days of such termination;

- e) the MLRO is a member of Senior Management or reports directly to Senior Management or the Board of Directors and does not report to the internal auditor to avoid potential conflicts of responsibilities;
 - f) the MLRO has clear and documented responsibility and accountability for designing the AML/CFT/CPF Risk Management and Compliance Program ensuring that the SMLs assess the risk of ML/TF/PF it may expect to face during its business and uses the results of the risk assessment in designing the AML/CFT/CPF Risk Management and Compliance Program.
 - g) the MLRO and the internal auditor have adequate resources in terms of people, data management systems and budget to implement and administer the AML/CFT/CPF Risk Management and Compliance Program effectively and to offer objective advice to the Board and Senior Management; and
 - h) any recommendations made by the MLRO, the internal auditor, and Senior Management in respect of the AML/CFT/CPF Risk Management and Compliance Program are acted upon in a timely manner.
- 3.4 Senior Management should further ensure that they receive sufficient pertinent information from the MLRO, the internal auditor, and other sources, as appropriate, to enable them to ensure the overall adequacy and effectiveness of the AML/CFT/CPF Risk Management and Compliance Program.

Responsibilities of the MLRO

- 3.5 The responsibilities of MLRO should, among others, include the following:
- a) ensuring that the AML/CFT/CPF risk assessment of the entity is developed, documented, and approved by the Board;
 - b) developing a risk-based AML/CFT/CPF Risk Management and Compliance Program;
 - c) keeping a register of all reports received from staff and a separate register of all reports made to the FIU;
 - d) ensuring a speedy and appropriate reaction to any matter in which ML/TF/PF is suspected; advising and training management, the Board

- (where relevant) and staff on the development and implementation of internal policies, procedures, and controls on AML/CFT/CPF;
- e) carrying out, or overseeing the carrying out of, ongoing monitoring of the business relations and reviewing a sample of records and transactions for compliance with this Guideline and the MLPC Act;
 - f) promoting compliance with this Guideline, including observation of the underlying principles on AML/CFT/CPF, and taking overall charge of all AML/CFT/CPF matters within SMIs;
 - g) acting as a liaison officer between the SMI, the SECZ, and the FIU; and
 - h) developing and implementing a self-assessment of controls.
- 3.6 The reports from the MLRO should include information on significant patterns or trends, self-assessment of controls and material changes thereto, as well as remedial action plans or recommendations, if any, with milestones and target dates for completion.
- 3.7 Where appropriate, the MLRO should draw conclusions, offer advice, and make recommendations about the overall structure and scope of the AML/CFT/CPF Risk Management and Compliance Program.

4. CUSTOMERS ONBOARDING PERSONNEL

- 4.1 The customer onboarding personnel is the person(s) who are responsible for initiating the SMI-customer relationship. These people are the face of the organization and gatekeepers against criminal activities. The SMIs personnel or staff responsible for the customers' onboarding and KYC verification are key in ML/TF/PF risks mitigation and prevention. These individuals should be well trained and have a better experience, as they must undertake the KYC process for all types of institutions and customers.
- 4.2 The SMIs should apply an in-house risk rating tool before onboarding customers. Further, signoffs of new customers must involve management and the Compliance Officer.
- 4.3 Staff facing customers should understand and be experienced in:
- a) Services or products the institution is offering;
 - b) Verification of high-risk customers such as PEPs and High net worth customers;

- c) Verification of customers from high-risk countries;
- d) Tools and technology used for data handling and whether it is safe enough to prevent document loss and loss of customer confidentiality;
- e) Verification of beneficial ownership for corporate customers;
- f) Reporting suspicious or large cash transactions;
- g) AML/CFT/CPF policies and procedures;
- h) Understand sector red flags, and
- i) AML/CFT/CPF laws, rules and, regulations in the country.

5. KNOW YOUR CUSTOMER (KYC) PROCESS

- 5.1 Know your customer is a process that involves getting a customer's data before starting a business relationship.
- 5.2 Initiating the AML/CFT/CPF KYC process is the first phase of the customer acceptance process. This should involve a notification being sent to the AML/CFT/CPF responsible team (or other KYC-related personnel), giving them an alert to the commencement of the AML/CFT/CPF review process as per KYC company requirements.
- 5.3 At this stage, SMLs should collect and verify the new customer's information and the forms of proof of identity that they provided along with the KYC form.
- 5.4 At this stage SMLs should know that there is no transaction that can occur or is allowed to happen.
- 5.5 As mandated by the laws and regulations of money laundering in the country, all SMLs are required to have a written and well-documented customer identification program (CIP) incorporated into their AML/CFT/CPF compliance program.
- 5.6 know-your-customer is about performing customer due diligence (CDD), i.e., identifying and verifying the identity of a customer.

Customer Due Diligence (CDD)

- 5.7 A SML shall ascertain the identity of a customer or beneficial owner based on any official identifying document and shall verify the identity of the customer based on reliable and independent source documents, data or information, or other evidence which is reasonably capable of verifying the

identity or the customer or beneficial owner before starting a business relationship.

- 5.8 In line with the requirements of FATF Rec 10, reporting entities are required to know their customers and the different types of risks associated with such customers.

Anonymous or Fictitious persons/business

- 5.9 SMI should know its customers and shall not deal with any person on an anonymous business, or any person using a fictitious name and should give special attention to the risks arising from new or developing technologies that may favour the anonymity of customers.
- 5.10 Whenever an SMI engages with a prospective customer to enter a transaction or to establish a business relationship, the institution must, while establishing that business relationship and in accordance with its AML/CFT/CPF Risk Management and Compliance Program –
- establish and verify the identity of the customer; and
 - if the customer is acting on behalf of another person, establish and verify the identity of that other person and the authority to establish the business relationship or to conclude the transaction on behalf of that other person; and
 - if another person is acting on behalf of the customer, establish and verify the identity of that other person and that other person's authority to act on behalf of the customer.

Reasonable suspicion prior to the establishment of business relations

- 5.11 If, prior to establishing business relations with a customer, an SMI has reasonable grounds to suspect that the funds of a customer are proceeds related to the facilitation or carrying out the offence defined in the MLPC Act, the SMI shall -
- a) not establish business relations with, or undertake a transaction with the prospective customer; and
 - b) file a suspicious transaction report to the FIU.

When CDD measures are to be performed

- 5.12 SMI shall perform CDD measures in accordance with this Guideline when:
- 1) establishing business relations with a customer;

- 2) carrying out occasional transactions: above the applicable designated threshold by the FIU;
- 3) dealing with a customer as part of an existing business relationship;
- 4) there is a suspicion of ML or TF or PF;
- 5) the SMI has doubts about the veracity or adequacy of previously obtained customer identification data.

5.13 SMIs should carefully assess the specific background and other conditions and needs of the customer. To achieve this, the SMI should collect relevant information, for example, the type and background of the customer or beneficial owner, income, and details of sources of funds. This will lead to a customer risk profile, which could serve as a reference to establish the purpose of the transaction and monitor subsequent transactions and events.

CDD measures when business relations are being established

5.14 Factors to be considered when creating a customer risk profile include but are not limited to:

- 🏠 type and background of the customer or beneficial owner;
- 🏠 geographic sphere of the activities of the customer and/or beneficial owner;
- 🏠 nature of the business activities;
- 🏠 sources of funds;
- 🏠 sources of wealth;
- 🏠 customer's and/or beneficial owner's geographical base;
- 🏠 frequency and scale of activity;
- 🏠 whether or not payments will be made to third parties;
- 🏠 type and complexity of the business relationship; and
- 🏠 size and pattern of transactions.

Identification of Customers

5.15 SMIs are required to identify and verify the identity of each customer who applies to them to establish business relations using reliable and independent source documents data and information.

Natural Persons

5.16 Where a customer is a natural person, the SMIs should obtain and record information regarding the customer, including but not limited to the following:

- 🏠 full legal name (s) used, including any aliases;
- 🏠 occupation, public position held and name of employer (if self-employed, the nature of the self-employment);
- 🏠 specimen signature;
- 🏠 residential address and contact telephone number;
- 🏠 nationality (non-Zimbabwe passport with photograph and resident alien card for non-citizens);
- 🏠 date and place of birth;
- 🏠 national identity card; and
- 🏠 parental consent form (where the individual is a minor)

Legal Persons

5.17 For customers who are legal persons such as companies, partnerships, trusts, associations, or other legal arrangements, CDD will require identification of the natural persons who comprise the mind and management of the legal person. This means that the SMI should understand the ownership and control structure of the customer.

5.18 Apart from identifying the customer, the following should also be identified:

- 🏠 each natural person who independently or together with a connected person has a controlling ownership interest in the legal person or who otherwise exercises control over the management of the legal person including the capacity in which the natural person is representing the legal person;
- 🏠 the beneficial owner of the customer;
- 🏠 tax identification number of the customer;
- 🏠 founding instruments in terms of which the legal person is created;
- 🏠 place of incorporation or registration;
- 🏠 date of incorporation or registration;
- 🏠 registered address of the legal person or address from which the entity operates;

- 🏠 shareholders or persons having executive authority in the legal person; and
- 🏠 residential address and contact particulars of each shareholder, partner, trustee, beneficiary, or person having executive authority in the legal person.

5.19 In the case of a partnership or similar arrangement, the SMI should further identify and establish the natural person purporting to enter a transaction or to establish a business relationship on behalf of the partnership. Furthermore, the name of the partnership, the identity of every partner, and the person who exercises executive control over the partnership should also be established.

5.20 In the case of a trust or similar arrangement, the SMI should further identify and establish the name of the trust, the identity of the founder, and each trustee and natural person who purports to be authorized to enter a transaction or to establish a business relationship on behalf of the trust. Each beneficiary is referred to in the trust deed or other founding instrument and the particulars of how the beneficiaries are determined should also be established by the SMI.

5.21 Where the customer appoints one or more natural persons to act on its behalf in establishing business relations with the SMI, or the customer is not a natural person, the SMI should:

- 🏠 Identify the natural person(s) that act or are appointed to act on behalf of the customer, as if such persons were themselves, customers.
- 🏠 verify the identity of these persons using reliable, independent source documents;
- 🏠 retain copies of all reference documents used to verify the identity of these persons; and
- 🏠 verify the authority of such persons to act on behalf of the customer by obtaining appropriate documentary evidence of their appointment, for example. e.g., power of Attorney, letters of administration for appointment as executor, and court orders for appointment as curators.

5.22 Where the customer is a Zimbabwean Government entity, the SMI is required to obtain such information as may be required to confirm that the

customer is a Zimbabwean Government entity as asserted, for example, a confirmation letter from the responsible ministry with an official seal/stamp.

Non-Face-to-Face Verification

- 5.23 SMIs should put in place policies and procedures to address specific risks associated with non-face-to-face business relationships or transactions, which should be implemented when establishing business relations and transacting through instructions conveyed by customers over the post, telephone, or internet.
- 5.24 Where there is no face-to-face contact, the SMI should use equally effective identification procedures as those available for face-to-face customer acceptance, supplemented with specific and adequate measures to mitigate the higher risk.
- 5.25 The following measures should be considered to mitigate the heightened risk associated with not being able to have face-to-face contact when establishing business relations:
- 🏠 telephone contact with the customer at a residential or business number that can be verified independently.
 - 🏠 confirmation of the customer's address through an exchange of correspondence or another appropriate method.
 - 🏠 subject to the customer's consent, telephone confirmation of the customer's employment status with the customer's employer at a listed business number of the employer.
 - 🏠 confirmation of the customer's salary details by requiring the presentation of recent bank statements.
 - 🏠 requiring the customer to make an initial payment using a cheque or RTGS drawn from the customer's personal account; and
 - 🏠 other reliable verification checks adopted by the SMI for non-face-to-face business.

Identification and Verification of Identity of Beneficial Owner

- 5.26 SMIs are required to inquire if any beneficial owner exists in relation to a customer. Where there is one or more beneficial owners in relation to a customer, the SMI should take reasonable measures to obtain information sufficient to identify and verify the identity of the beneficial owner.

- 5.27 When an SMI establishes and verifies the identity of the beneficial owner of a legal person the institution must –
- a) identify and verify each natural person who, independently or together with a connected person, has a controlling ownership interest or ultimately owns the legal person; and
 - b) if there is doubt as to whether a natural person contemplated in a) is a beneficial owner of the legal person in question or where no natural persons ultimately own the legal person, identify each natural person who ultimately controls the legal person or who otherwise exercises executive control or management or similar position in the legal person.
- 5.28 The Beneficial Owner in relation to a customer of an SMI means, the natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a person or a legal arrangement.
- 5.29 For legal persons, the primary source for verification of ultimate beneficial ownership is the Register of Ultimate Beneficial Ownership which is compiled and kept by the Registrar of Companies Office.
- 5.30 For complex structures, foreign entities, or foreign-owned entities, SMIs are required to develop and have the necessary knowledge to correctly identify and verify such customers and their beneficial owners using information and data publicly available on the internet or request information from the jurisdiction where the customer is registered.
- 5.31 Identifying beneficial ownership of a customer is an obligation that must be satisfied, upon the risk assessment of the customer.
- 5.32 SMIs should assess different levels of ML/TF/PF risks posed by their customers' beneficial owners. For example, SMIs should consider whether a beneficial owner is a high-risk customer.
- 5.33 If an SMI has doubts about the veracity or adequacy of the information provided, it should not start a business relationship, or provide a financial service, and should consider making a suspicious transaction report to FIU. There is also the risk of tipping off.

Online Accounts

- 5.34 SMIs are now allowing some of the customers to open accounts online without needing to appear in person. This entails Customer Identification Program (CIP) rules that recognize a convenience used in today's digital age, so they offer flexibility in this area.
- 5.35 SMIs should apply a risk-based approach to using Digital ID systems for customer identification. According to the FATF Guidance On Digital ID, this requires:
- a) Understanding the assurance levels of the Digital ID system's technology main components to determine its reliability/independence; and
 - b) Making a broader, risk-based determination of whether, given its assurance levels, the Digital ID system provides an appropriate level of reliability and independence considering the potential AML, CFT, CPF, fraud, and other illicit financing risks at stake.
- 5.36 However, SMIs must still adhere to KYC requirements. This may be through the upload of a scanned driver's licence and other necessary verification documents.

Simplified Customer Due Diligence

- 5.37 Where the risks of ML/TF/PF are lower, SMIs may apply simplified CDD measures. The simplified measures must have been identified through a risk assessment and should be commensurate with the lower risk factors having regard to the circumstances of each case. This means that the SMI must have a basis for applying simplified CDD measures.
- 5.38 Some examples of possible simplified measures are:
- 🌐 reducing the frequency of customer identification updates;
 - 🌐 reducing the degree of ongoing monitoring and scrutinizing transactions based on a reasonable money threshold; and
 - 🌐 not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.
- 5.39 Some examples of when an SMI might apply reduced CDD measures are where:

- reliable information on the customer and beneficial owner is publicly available or where adequate checks and controls exist elsewhere in the national system;
 - the SMI is dealing with another SMI whose AML/CFT/CPF controls it is familiar with by virtue of previous dealings; or
 - the customer is a financial institution that is subject to and supervised for compliance with AML/CFT/CPF requirements consistent with standards set by the FATF;
 - the customer poses a lower risk of ML/TF/PF because of the nature of the product that the customer has bought or intends to buy.
- 5.40 Where simplified CDD measures have been performed in relation to a customer, the SMI should document:
- 1) the details of its risk assessment; and
 - 2) the nature of the simplified CDD measures.
- 5.41 Simplified CDD measures are not allowed where there is a suspicion of ML/TF/PF or where specific higher-risk scenarios apply.

Enhanced Customer Due Diligence

- 5.42 SMIs shall implement appropriate internal risk management systems, policies procedures, and controls to determine if business relations with or transactions for any customer present a higher risk for ML/TF/PF.
- 5.43 Enhanced CDD measures refer to additional due diligence measures that must be applied where the customer has not been physically present for the identification or where the customer is politically exposed or in any situation that by its nature can present a higher risk of ML/TF/PF. These measures should apply to all higher-risk business relationships, customers, and transactions.
- 5.44 Entities should examine the background and purpose of all complex or unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. They should increase the nature and intensity of monitoring of the business relationship, to determine whether those transactions or activities appear suspicious.

When must EDD be conducted for new customers?

5.45 SMIs must conduct enhanced CDD when taking on certain types of new customers. This includes establishing a business relationship with a customer or if a customer seeks to conduct an occasional transaction or activity.

5.46 Customers that must have enhanced CDD are:

- (a) A trust or another vehicle for holding personal assets
- (b) A non-resident customer from a country that has insufficient AML/CFT/CPF systems or measures in place
- (c) A company with nominee shareholders or shares in bearer form
- (d) A politically exposed person (PEP)
- (e) High Net Worth customer
- (f) A customer seeking to conduct a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose
- (g) Any other customer or circumstances that you assess (based on your risk assessment and standard CDD) to be of high ML/TF/PF risk
- (h) A business relationship with a customer that involves new or developing technologies, or new or developing products, that might favour anonymity
- (i) A customer seeking to conduct an occasional transaction or activity through the reporting entity that involves new or developing technologies, or new or developing products, that might favour anonymity.

5.47 In cases where a customer is deemed to pose a high risk, the case is escalated to the MLRO. The SMI is required under its EDD process to ascertain the riskiness level of the customer. EDD is the third phase in the AML/CFT/CPF KYC process flow. When performing EDD, the following need to be considered:

- 1) Verification of customers' details, their beneficial ownership structure, and the details of representatives and other key persons. You must take reasonable steps to do this according to the level of risk involved.
- 2) Should usually obtain and verify information relating to the source of wealth (SoW) and/or source of funds (SoF) of the customer.






- 3) Determine whether complex beneficial ownership structures are legitimate and intended to facilitate business or if they are deliberately complicated to hinder the investigation and conceal the identity of the beneficial owners.
 - 4) Determine whether a customer's SoW or SoF are legitimately derived, or intended for legitimate use, or whether there are reasonable grounds to suspect it may be the proceeds of crime.
 - 5) Where possible visit or identify the business in which the customer is operating and further visit the said customers to ensure they really buy from the customers' business.
 - 6) Distinguish between a customer that has a higher risk profile but is not involved in ML/TF/PF, as opposed to a customer whose transactions or activities may be linked to ML/TF/PF.
- 5.48 When conducting EDD on high-risk entities, SMLs need to identify all beneficial owners of each legal entity customer at the time of account opening.
- 5.49 Legal entity customers include the following entities created by filing with the country's registration office or Deeds Office:
- (a) corporations (Private and Public limited companies)
 - (b) limited partnerships
 - (c) general partnerships
 - (d) business trusts
 - (e) any other entity created by a filing with a registration office
 - (f) any similar entities formed under the laws of a non-Zimbabwean jurisdiction.
- 5.50 When conducting EDD, SMLs should review the elements in 5.51 during the onboarding phase and throughout the life of the relationship. The know your customer requirement does not stop after the account is opened.
- 5.51 KYC requirements to review for high-risk customers:
- (a) The purpose of the account
 - (b) Source of their funds and wealth
 - (c) Individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors

- (d) Occupation or type of business (of the customer and/or other individuals with account ownership or control)
- (e) Financial statements
- (f) Banking references
- (g) Domicile (where the business is organized or incorporated)
- (h) The proximity of the customer's residence, place of employment, or place of business to the bank or other financial institution
- (i) Description of the customer's primary trade area and whether there will be routine international financial transactions
- (j) Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers
- (k) Explanations for changes in account activity.

Politically Exposed Persons and other high-risk customers

5.52 The FATF Recommendations require additional due diligence measures in relation to Politically Exposed Persons (PEPs).

5.53 SMLs should take note that PEPs can be foreign, domestic, or may be persons who are or have been entrusted with a prominent function by international organizations. Therefore, in addition to performing CDD measures, SMLs should perform enhanced CDD measures in relation to such customers. For this purpose, SMLs should:

-  put in place appropriate risk management systems, internal policies, procedures, and controls to determine if a customer or beneficial owner is a politically exposed person;
-  establish a board-approved customer acceptance policy regarding PEPs, taking account of the reputational and other risks involved;
-  obtain approval from senior management to establish or continue business relations with such customers;
-  establish, by appropriate and reasonable means, the source of wealth and source of funds of such customers; and
-  conduct enhanced ongoing monitoring of the business relations with the customer.

5.54 SMLs are also required to give particular attention to business relations and transactions with persons from countries that have inadequate

AML/CFT/CPF measures. For this purpose, they may take a range of steps, including the adoption of measures like those applied to PEPs and other high-risk categories.

- 5.55 Determining whether an individual is a PEP may not always be straightforward. In the circumstances, the Authority considers it acceptable for SMLs to refer to databases of PEPs (available in a jurisdiction) or use open sources like the internet. However, the Commission also expects SMLs to exercise a measure of discretion and sound judgment in deciding whether an individual who is not on such a database should nevertheless be treated as a PEP, having regard to the risks and the circumstances of each case.
- 5.56 Enhanced CDD measures must also be applied to immediate family members and known close associates of PEPs. An immediate family member includes a spouse, previous spouse, life partner, children and stepchildren, and their spouses or life partners, parents, siblings, and stepsiblings, and their spouses or life partners.
- 5.57 SMLs should take reasonable measures to determine whether the beneficiaries and the beneficial owners of the beneficiaries if any, are PEPs. Where higher risks are identified SMLs should:
- 1) require that senior management be informed before transaction is made;
 - 2) conduct enhanced scrutiny of the whole business relationship with the customer; and
 - 3) consider making a suspicious transaction report.
- 5.58 Other high-customers that the SMLs should conduct enhanced due diligence include high-net-worth individuals, non-residents customers, trusts, non-governmental organizations, professional intermediaries (lawyers, accountants), customers with criminal records, or past supervisory actions against them, customers with business links to known high-risk jurisdictions, and other high-risk Customers as identified by the FATF.

Reliance On Third Parties

- 5.59 SMLs are allowed to rely on intermediaries or other third parties to perform some elements of the CDD process, provided that the following requirements are met:

- 1) the SMI must be satisfied that the third party it intends to rely upon is subject to and is supervised for compliance with AML/CFT/CPF requirements consistent with the standards set by the FATF, and has adequate AML/CFT/CPF systems in place to comply with those requirements;
 - 2) the third party is able and willing to provide to the SMI without delay, any identification data, documents, or information obtained by the third party relating to CDD measures applied to customers and beneficial owners;
 - 3) the third party commits in writing that it shall perform CDD measures, grant the SMI access to CDD documentation in its custody, and report to the FIU and the SMI in the case of a suspicious or unusual transaction;
 - 4) the SMI undertakes and completes its own verification of the customer and beneficial owner if it has doubts that appropriate due diligence was performed by the third party.
- 5.60 For the avoidance of doubt, notwithstanding the reliance on a third party, the ultimate responsibility for the customer and beneficial owner identification and verification remains with the SMI relying on a third party. However, third parties are responsible for the validity of all information obtained.

6. RECORD KEEPING: CUSTOMER DUE DILIGENCE RECORDS

- 6.1 SMIs must keep all records obtained or generated by CDD measures, including account files, business correspondence, and results of any analysis undertaken. Other records are the risk profile of each customer and beneficial owner and copies of identification documents.
- 6.2 In the case of a business relationship, the records must reflect the information obtained by the SMI describing the nature of the business relationship concerned, the intended purpose of the business relationship and the source of the funds which the prospective customer is expected to use in concluding transactions during the business relationship. Records must be kept for a period of five years from the date on which the business relationship is terminated.

7. DECISION OUTCOME-OPEN ACCOUNT OR DENY APPLICATION

- 7.1 The process is completed when the MLRO/Compliance officer/senior management has approved or denied the account opening. Only after CDD/EDD has been approved, should an account be opened in accordance with legal requirements.
- 7.2 If after completing the process of KYC and AML/CFT/CPF evaluation of the customer, Management will decide whether to proceed further or not.
- 7.3 However, declining to establish a business relationship may be counter-productive, and can lead to tipping off and the risk of de-risking a segment of customers.

8. ONGOING MONITORING DUE DILIGENCE

- 8.1 SMIs should pay attention to all requested changes that occur after the business relationship has been established. They should monitor on an ongoing basis their business relations with customers and should observe and assess the activity in respect of the customer and scrutinize transactions undertaken to ensure that they are consistent with the SMI's knowledge of the consumer, its business, risk profile and where appropriate, the sources of funds.
- 8.2 SMIs should pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent economic or lawful purpose. To the extent possible, SMIs should inquire into the background and purpose of all such transactions and document their findings with a view to making this information available to the FIU should the need arise.
- 8.3 Periodic reviews of customer identification information obtained should be done to ensure that the information is kept up to date, particularly for higher-risk categories of customers.
- 8.4 For ongoing monitoring, an SMI should put in place and implement adequate systems and processes, commensurate with the size and complexity of the SMI, to; –
 - 1) monitor its business relations with customers; and
 - 2) detect and report suspicious, complex, unusually large, or unusual patterns of transactions.

9. ANNUAL AML/CFT/CPF REVIEW

- 9.1 The AML/CFT/CPF review does not end after onboarding a customer. There should be an ongoing/annual review of the customer's transactional activities if you want to properly adhere to the AML/CFT/CPF requirements.
- 9.2 Customers shall be classified according to the level of ML/TF/PF risk they pose, that is, either high or medium or low. The SMLs are required to perform an ongoing review of KYC documents and customer activities utilising timeframes as indicated beneath:
- (a) Low Risk: **Within 24 months**
 - (b) Medium Risk: **Within 12 months**
 - (c) High Risk: **Within 6 months**

10. REFERENCE

FATF (2020). Guidance on Digital Identity. Paris, www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

FATF (2013-2021), Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems. Paris, http://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf_methodology.html

Financial Services Regulatory Authority Eswatini (2016). Money Laundering and Financing of Terrorism (Prevention) Guideline (AML/CFT). Number: 01

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

Securities and Exchange Act [Chapter 24:25]

APPENDIX 1: EXAMPLE OF SUSPICIOUS TRANSACTIONS IN THE SECURITIES SECTOR

SMLs that are involved in the business of dealing in securities, or any other financial instruments, including asset managers and custodians, should consider the following indicators of potentially suspicious transactions;

- 🏦 Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the customer or the customer's financial ability;
- 🏦 Any dealing with a third party when the identity of the beneficiary or counterparty is undisclosed;
- 🏦 Customer attempts to purchase investments with cash;
- 🏦 Customer uses securities or broking firm as a place to hold funds that are not being used in the trading of securities for an extended period and such activity is inconsistent with the normal investment practice of the customer or the customer's financial ability.
- 🏦 Customer washes money received through the sale of shares to be deposited into a bank account rather than a trading account which is inconsistent with the normal practice of the customer;
- 🏦 Customer frequently makes large investments in stocks, bonds, ETFs, or other securities in cash within a short period, inconsistent with the normal practice of the customer;
- 🏦 Customer makes large or unusual settlements of securities in cash;
- 🏦 Transfers of funds or securities between accounts not known to be related to the customer;
- 🏦 Several customers open accounts within a short period of time to trade the same stock;
- 🏦 Customer is an institutional trader that trades large blocks of small stock on behalf of an unidentified party;
- 🏦 Unrelated customers redirect funds toward the same account;

- 🚧 Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity;
- 🚧 Customer is willing to deposit or invest at rates that are not advantageous or competitive; or
- 🚧 Third-party payments.