Guidance to Authorised Dealers with Limited Authority on the Risk-based Approach to Implementation of Anti-money Laundering / Counter-terrorism Financing /Combating Financing of Proliferation of Weapons of Mass Destruction Obligations

FINANCIAL SURVEILLANCE DIVISION

2025

Preamble

In accordance with FATF Recommendation 34 on Guidance and Feedback, competent supervisors and regulatory bodies are required to establish guidelines and provide feedback to assist Financial Institutions and Designated Non-Financial Businesses and Professions (DNFBPs) in implementing national measures to combat money laundering and terrorist financing.

This Guidance Manual is issued by the Financial Surveillance Division to aid Authorised Dealers with Limited Authority (ADLAs) in understanding and fulfilling their statutory obligations regarding Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing (AML/CFT/CPF). Section 12(B) of the Money Laundering and Proceeds of Crime (MLPC) Act mandates that every Financial Institution must identify, assess, and understand the ML/TF risks they face and implement appropriate measures to mitigate these risks.

It is therefore essential for the Competent Supervisory Authority to issue this Guidance Manual to ensure that ADLAS comply with FATF Recommendation 1: Assessing Risk and Applying a Risk-Based Approach. This recommendation is fundamental to the FATF standards due to its impact on other standards. By adhering to the measures outlined in this Guidance Manual, ADLAs will enhance their AML/CFT frameworks, ensuring they are robust and the financial system remains resilient against manipulation by criminals and terrorists seeking to move illicit funds or finance terrorism.

The implementation of the measures in this Guidance Manual will result in an effective AML/CFT system, characterized by its ability to detect, deter, prevent, disrupt, and punish illegal financial activities and hence achieve the overarching objective of financial integrity.

Any enquiries regarding this Guidance Manual should be channelled to:-

The Director
Financial Surveillance Division
Reserve Bank of Zimbabwe
80 Samora Machel Avenue
P. O. Box 1283
HARARE

Contents

List of abbreviations

ADLA	Authorized Dealers with Limited Authority
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Counter-Financing of Terrorism
CPF	Combating Financing of Proliferation of Weapons of Mass Destruction
CSA	Competent Supervisory Authority
CTR	Cash Transaction Reports
EDD	Enhanced Due Diligence
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know Your Customer
MIS	Management Information System
ML	Money Laundering
MLPC	Money Laundering and Proceeds of Crime Act [Chapter 2: 24]
MTA	Money Transfer Agency
MTO	Money Transfer Operator
PEPs	Politically Exposed Person
PF	Proliferation Financing
RBA	Risk-Based Approach
RBZ	Reserve Bank of Zimbabwe
SDD	Simplified Due Diligence
STR	Suspicious Transaction Reports
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UBO	Ultimate Beneficial Owners
UNSR	United Nations Security Council Resolution

Definition of key terms

For this AML/CFT/CPF Risk Based Guideline, the following definitions and interpretations apply. These definitions must be read together with the definitions set out in Section 2, Section 13 and Section 16 of the Money Laundering and Proceeds of Crime Act [Chapter 9:24]. In the event of conflict between a definition in this guidance and that in the Act, the later prevails.

TERM	DEFINITION
ADLA	Authorised Dealer with Limited Authority (ADLA) shall be a financial services provider not necessarily licensed under the Banking Act [Chapter 24:20] but authorized by the Reserve Bank of Zimbabwe in terms of the Exchange Control Act [Chapter 22:05] to buy and sell foreign currency and carry out small value person to person cross border remittances through money transfer systems. Types of ADLAs include: **Tier One (1)**: Includes locally incorporated money transfer operators (MTOs) that partner with approved international money transfer organizations (MTOs) or use own systems to carry out both inward and outward international remittances. They also buy and sell foreign exchange on a spot basis. **Tier Two (2)**: Includes locally incorporated money transfer operators (MTOs) operating as money transfer agencies (MTAs) by either partnering with approved international money transfer operators or use own systems to carry out inward international remittances only. They also buy and sell foreign exchange on a spot basis. **Tier three (3):** These are locally incorporated financial services providers *(Bureau de Change)* which only buy and sell foreign currency on a spot basis.
Financial Surveillance Division	This is a Division of the Reserve Bank of Zimbabwe responsible for compliance monitoring and enforcement and is a designated Competent Supervisory Authority (CSA) for Authorized Dealers with Limited Authority, in terms of Section 2 of MLPC Act.
Money Laundering (ML)	Means the conversion or transfer of proceeds of crime for the purpose of (a) disguising the illicit origin of such property; or (b) assisting any person involved in the commission of a serious offence to evade the consequences of his/her illegal act or omission.[1]

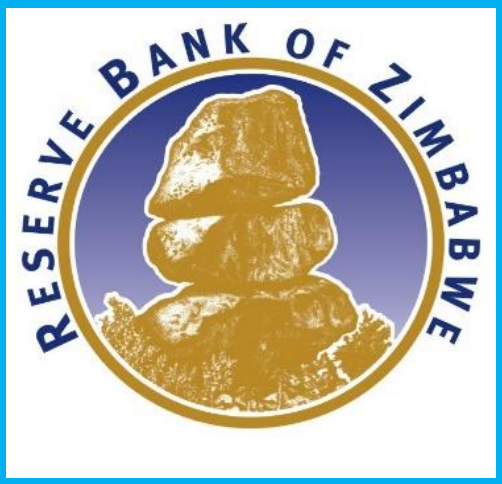
[1] Refer to Section 9 of the MLPC Act.

TERM	DEFINITION
	There are three distinct stages in which money laundering is deemed to be accomplished: ❖ **Placement**- this is the primary stage in the money laundering process, which involves placing cash in the formal financial system. ❖ **Layering**- process of disguising source of the funds through layers of complex financial transactions, designed to disguise audit trail and provide anonymity. ❖ **Integration**- Once the funds are layered and can no longer be tracked back to their criminal origins, they are integrated into the financial system and now appear clean and available for use by criminals. Funds re-enter the financial system appearing as normal business funds.
Terrorist Financing (TF)	Terrorist Financing involves the solicitation, collection and the provision of funds and other assets with the intention that the funds/other assets may be used to support terrorist organisations and their activities.
Proliferation Financing (PF)	Proliferation Financing is defined as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
Money Laundering risk	The risk that a country, financial institution or business unit could be used for money laundering.
Terrorist Financing risk	The risk that a country, financial institution or business unit could be used for terrorism financing.
Proliferation Financing Risk	Refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial obligations referred to in Recommendation 7 of FATF.
MLPC Act	An ACT to suppress the abuse of the financial system and enable the unlawful proceeds of all serious crime and terrorist acts to be identified, traced, frozen, seized and eventually confiscated.
Financial Action Task Force (FATF)	It is the global money laundering and terrorist financing watchdog. It sets international standards that aim to prevent

TERM	DEFINITION
	Money Laundering/Terrorist Financing/ Proliferation Financing of Weapons of Mass Destruction risks.
Financial Intelligence Unit (FIU)	Refers to the Financial Intelligence Unit, established under Section 6A of the MLPC Act.
Beneficial Owner (or Ultimate Beneficial Owner)	Refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Reference to "ultimately owns or control" or "ultimate effective control" refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.
Financial Institution	Means a financial institution as defined in Section 2 of the MLPC Act.
High risk countries	Refers to countries listed in a circular or directive issued by the FIU in terms of Section 26A. These are normally countries that would have been identified by the FATF as non-compliant for AML/CFT/CPF purposes. ADLAs are required to exercise enhanced due diligence, proportionate to the identified risks, when conducting business relationships with persons or institutions in such countries.
Compliance Risk (CR)	This refers to the current and prospective risk of damage to the organisation's business model or objectives, reputation and financial soundness arising from non-adherence to regulatory requirements and expectations. Compliance risk is an institutional-level concern and revolves around non-adherence to AML/CFT/CPF regulatory requirements.
Financial exclusion risk	This refers to the risk of excluding significant portions of population (mostly low-income customers as well as semi-formal and informal institutions serving the low-income customers) from the financial system. This exclusion opens up opportunities for money laundering.
Financial Inclusion	Financial inclusion refers to the access to, and usage of, a range of financial products and services provided by formal financial service providers to specific target groups or all segments of the population, as well as the quality of these products and services.

TERM	DEFINITION
Inclusive integrity	Refers to implementation of AML/CFT/CPF in a way that aligns with financial inclusion.
Proportionate measures	Refers to AML/CFT/CPF measures that are aligned with the level of risks. Enhanced measures are required for identified higher risk customers / transactions / situations while simplified measures may be implemented for lower risk situations.
Board of Directors (BoD)	Refers to a governing body or a group of directors. A director includes any person who occupies a position of a director, however styled, of a body corporate or unincorporated.
Senior management	Refers to any person(s) having authority and responsibility for planning, directing or controlling the activities including the management and administration of a financial institution.
Legal arrangements	Refers to express trusts or other similar legal arrangements.
Legal persons	Any entities, other than natural persons, that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations and other relevant similar entities.
Politically Exposed Person (PEPs)	Refers to: (a) Domestic PEPs – i.e. individuals who are or have been entrusted domestically with prominent public functions. For example, Heads of State or of government, senior politicians, senior government officials, judiciary or military officials, senior executives of state-owned corporations and senior political party officials; (b) Foreign PEPs – individuals who are or who have been entrusted with prominent public functions by a foreign country. For example, Heads of State or of government, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations and senior political party officials; (c) Persons who are or have been entrusted with a prominent function by an international organisation which refers to members of senior management. For example, directors, deputy directors and members of the board or equivalent functions.

TERM	DEFINITION
	(d) Immediate family members (such as parents, children, siblings or spouses) or associates of persons referred to in (a) to (c) above.
Customer	Refers to both account holder and non-account holder, and the term also refers to a client.
Customer Due Diligence (CDD)	Refers to any measures undertaken pursuant to Section 15 and 16 of the MLPC Act.



SECTION ONE (1)

INTRODUCTION AND BACKGROUND

1.1 Background

1.1.1 Money Laundering, Terrorism Financing and Proliferation Financing (ML/TF/PF) continue to be a dynamic threat which has the potential of adversely affecting the country's reputation and investment climate. The globalisation of financial services and advancement in technology has posed challenges to regulators and law enforcement agencies as criminals have become more sophisticated in utilising financial institutions including Authorised Dealers with Limited Authority (ADLAs) to launder illicit funds and use them as conduits for moving funds meant for terrorist activities.

1.1.2 In terms of Section 2 of the Money Laundering and Proceeds of Crime Act [Chapter 9:24] (MLPC), Financial Surveillance Division,[2] is designated as a Competent Supervisory Authority (CSA).

1.1.3 In line with Memorandum of Understanding (MoU) between the Financial Surveillance Division and Financial Intelligence Unit (FIU) of 10 December 2013, and in terms of Section 3(3) of the MLPC Act, Financial Surveillance Division, in its capacity as a CSA, has the obligation to cooperate with the FIU in ensuring that ADLAs, comply with their statutory Anti-Money Laundering/ Combating Financing of Terrorism/Countering Proliferation Financing of Weapons of Mass Destruction (AML/CFT/CPF) obligations.

1.1.4 This Guidance Manual, as issued by Financial Surveillance Division is meant to assist ADLAs understand and implement their statutory obligations on AML/CFT/CPF.

1.1.5 The Guidance Manual reflects the shift from a previous rule based, "tick-box" approach, to a risk-based approach (RBA) to combating money laundering and financing of terrorism.

1.1.6 Section 12B of the MLPC Act requires every financial institution to (a) identify, assess and understand the money laundering (ML) and terrorism financing (TF) risks to which the financial institution is exposed; and to (b) put in place and implement effective measures to mitigate the risks.

1.1.7 Implementation of most of the AML/CFT/CPF requirements under the MLPC Act, therefore, starts with an assessment and understanding of the money laundering risks to which the institution is exposed.

1.1.8 The rule-based approach, which was enforced prior to 2012, required financial institutions to implement AML/CFT/CPF obligations uniformly in respect of all customers, to all transactions and to all situations, regardless of the level of money laundering or terrorism financing risk.

[2] Formerly Exchange Control Inspectorate in the Exchange Control Division.

1.1.9 This "tick box" and "one-size-fits-all" approach resulted in unfocused and inefficient deployment of resources. Resources were wasted on customers, transactions and financial products/services that presented little ML/TF/PF risks. This rigorous uniform enforcement of AML/CFT/CPF requirements on all customers, all transactions and all situations also resulted in the exclusion of a significant segment of the population who failed to meet the stringent requirements to access financial services.

1.1.10 The risk-based approach seeks to strike a balance between protecting the integrity of the financial system, through implementation of measures to deter, detect and report ML and TF, on the one hand, and promoting financial inclusion, on the other hand.

1.1.11 This balanced approach is sometimes referred to as "inclusive integrity". The risk-based approach achieves this balance by giving ADLAs the leeway to assess the different levels of ML/TF risks presented by different types of customers and by different financial products or services.

1.1.12 Having thus identified and assessed the ML/TF risks, ADLAs are required to apply enhanced due diligence in respect of all high-risk customers and products/services. Conversely, ADLAs are permitted to implement reduced or simplified customer due diligence on low-risk customers and low risk financial products/services.

1.2 Purpose of the Guidance Manual

1.2.1 This Guidance Manual is formulated in accordance with the Money Laundering and Proceeds of Crime Act [Chapter 9:24) and Financial Action Task Force 40 Recommendations and is intended to ensure that ADLAs understand and comply with the requirements and obligations imposed on them.

1.3 Scope of the Guidance Manual

1.3.1 The Guidance Manual sets out the following:-

(i) Obligations of ADLAs with respect to the requirements imposed under the MLPC Act;

(ii) Requirements imposed on ADLAs in implementing a comprehensive risk-based approach in managing ML/TF/PF risks; and

(iii) Roles of ADLAs' board of directors, senior management and staff in putting in place relevant AML/CFT/CPF measures.

1.4 Legal Provisions

1.4.1 This Guidance Manual is issued in line with the provisions of:-

(i) The Money Laundering and Proceeds of Crime Act [Chapter 9.24];

(ii) Exchange Control Statutory Instrument 104 of 2015;

(iii) Statutory instrument 76 on Suppression of Foreign and International Terrorism (Application of UNSCR 1267 of 1999, UNSCR 1373 of 2001 and Successor UNSCRs) Regulations, 2014;

(iv) Statutory Instrument 56 on Suppression of Foreign and International Terrorism (Application of UNSCR 1540 (2004) 1673, 1810, 1887, 1977 (On non-state actor proliferation), 1695, 1718, 1874 on Democratic People's Republic of Korea and1696, 1737, 1747, 1803 and 1929, UNSCR 2094 (2013), 2231 (2015) UNSCR 2270 (2016), UNSCR 2321 (2016), UNSCR 2371 (2017), of UNSCR 2375 (2017) UNSCR 2397 (2017)and Successor UNSCRs) Regulations, 2019.

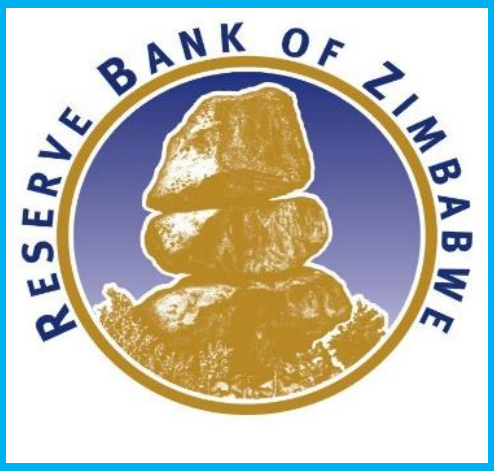
1.5 Applicability of the Guidance Manual

1.5.1 This Guidance Manual is applicable to:-

(i) Banking ADLAs
(ii) Non-Banking ADLAs and
(iii) Branches and subsidiaries of ADLAs

1.5.2 The requirements of this Guidance Manual are applicable to Zimbabwean licensees operating as foreign branches, subsidiaries and offices, wherein they are required to comply with the policies and procedures as implemented by their head offices.

1.5.3 However, if policies and procedures as implemented by their head offices are inconsistent with the requirements of this document or less stringent than stated in this document, the requirements prescribed herein in this document shall prevail.



SECTION TWO (2)

THE RISK BASED APPROACH
(ASSESING RISK AND APPLYING RBA)

2.1 Overview

2.1.1 This part of the Guidance Manual focuses on the principles that should help ADLAs to implement the AML/CFT/CPF obligations requirements effectively. The Financial Action Task Force (FATF) Recommendation One (1), compels Financial Institutions to identify, assess their ML/TF/PF risks and take effective action to mitigate these risks in their businesses.

2.1.2 This is where the risk-based approach (RBA) to AML/CFT/CPF comes in. The risk-based approach requires ADLAs to identify, assess and understand the money laundering risks to which they are respectively exposed, and to take commensurate measures to mitigate such risks.

2.1.3 The risk-based approach is premised on the assumption that one cannot effectively combat that which one has not properly identified and understood. It is also based on a recognition that resources to combat ML and TF are invariably finite and the limited resources can be deployed more efficiently and effectively if ADLAs focus more on the high-risk customers or products and services and devote less resources to lower risk situations. The RBA, therefore, enables ADLAs to save compliance resources (human, financial and material resources, etc) by focusing on higher risk situations.

2.1.4 In practice, an ML and / or TF risk assessment by ADLAs involves an assessment of the following types of risks, in a risk matrix format:-

(i) Customer risk;
(ii) Financial product/services risk;
(iii) Delivery channel risk; and
(iv) Geographic risk;

2.1.5 Thus, in respect of customer risk, the ADLA would assess and classify its customers by risk levels, i.e. **Low Risk, Medium Risk and High Risk** (or any similar risk scoring method).

2.1.6 The financial institution will do the same for the various products/services it offers to its customer. It has to identify those products/services that are most likely to be abused to launder proceeds of crime (high risk products/services) and those that are less likely to be favoured by launderers.

2.1.7 Having assessed the ML/TF risks to which the business is exposed, an ADLA must then come up with appropriate and effective measures to mitigate those risks, i.e. applying enhanced measures for high-risk customers, products or situations, and simplified measures for low risk customers, products or situations.

2.1.8 ADLAs should have the flexibility to construct and tailor their risk management frameworks for the purpose of developing risk-based system controls and mitigation strategies in a manner that is proportionate to their business

structure, resources, customers, geographical locations, staff, products and the services they offer.

2.1.9 The results of the financial institution's risk assessment must lead to the design and implementation of a risk-based compliance program.

2.2 Risk Identification, Assessment and Mitigation: The Process

2.2.1 Section 12 B of the MLPC Act provides that:-

1. *Every Financial institution and DNFBPs shall assess its money laundering risk and Terrorist financing risks to which it is exposed and shall maintain adequate records thereof.*
2. *Based on the risk assessment, the financial institution or designated non-financial business or profession shall implement prescribed anti-money laundering and anti-financing of terrorism measures, commensurate with the identified risks, that is to say—*
   a. *shall implement enhanced measures for high risk customers, products, services or situations, as appropriate; and*
   b. *may implement simplified or reduced measures for low risk customers, products, services or situations, as appropriate:*
3. *Every financial institution or designated non-financial business or profession shall review and update its risk assessment regularly to take into account material changes in risk factors and shall maintain records of such reviews and updates.*

2.2.2 The law does not prescribe a particular method or process of carrying out the ML/TF risk assessment process. What is important is for the ADLA to choose or come up with its own methodology, provided the chosen methodology incorporates the principles[3] explained in the Guidance Manual of 2021 and achieves the end objective i.e. to ensure that the institution has identified and assessed the ML/TF risks it faces and, based on that assessment, has put in place effective mitigating measures commensurate with the identified risk levels.

2.2.3 The diversity of ADLAs in terms of the services they offer (Inward international remittances, outward international remittances, domestic transfers, currency switches, etc), the types of customers they serve, the ML/TF risks to which they are exposed as well as the different sizes and different levels of complexities of businesses will necessarily demand different approaches and different methodologies to assessing and mitigating the risks.

[3] These principles are:-
(i) Risk identification
(ii) Risk assessment/measurement
(iii) Risk mitigation, and
(iv) Risk Monitoring and evaluation

2.2.4 A registered ADLA operating under Tier 1 and 2 would, naturally be expected to invest in an equally sophisticated and appropriate IT-based risk assessment tool. On the other hand, a small-sized domestic MTA may not require a sophisticated IT-based risk assessment tool but may just need to demonstrate that:-

(i) It is aware of the different money laundering risk factors (customer risk, product risk, geographic risk and delivery channel risk) and how they apply to its specific business;

(ii) The ADLA has capacity to identify type of customers, transactions and services offered by the business, which present higher risks;

(iii) The ADLA applies enhanced due diligence in respect of the higher risk customers / transactions (e.g. seeking more in depth information on the nature of business or source of funds / wealth of the customer). [4]

(iv) The ADLA is able to identify and report suspicious transactions.

2.2.5 Irrespective of any methodology adopted, there are four key steps involved in implementing the risk-based approach by an ADLA, namely:

(i) Step 1: Risk identification;
(ii) Step 2: Risk assessment/measurement;
(iii) Step 3: Risk mitigation and
(iv) Step 4: Risk Monitoring and evaluation.

Step 1: Risk identification

2.2.6 This involves identifying the inherent risks to which the ADLA is exposed. Inherent risk refers to the ML/TF risks faced by the ADLA before one considers the controls and other measures already in place to mitigate the risk.

2.2.7 There are 4 main types of risks that an ADLA would normally face, and which, in most cases, would be covered in a risk assessment, namely:-

(i) Customer risk;
(ii) Products/services risks;
(iii) Geographic risk;
(iv) Delivery channel risk

[4] Source of wealth differs from source of funds. Source of funds refers to the origin of the specific funds or assets that will be used for a transaction or to establish a business relationship. Source of wealth is a broader concept that refers to the origin of the entire body of the customer's wealth that is total assets, even if those assets will not necessarily be the same assets used for one of these purposes. In essence, source of wealth refers to the origin of a customer's total financial standing.

Step 2: Risk assessment/measurement/profiling

2.2.8 This involves measuring the magnitude of the risk and each of the risk types identified under Step 1, above.

2.2.9 In relation to each risk type, the ADLA must assign risk-rating score. Tier 3 ADLAs may not need an elaborate/complex risk scoring model as would be expected of ADLAs under Tier 1 & 2.

2.2.10 Most Domestic Money Transfers (DMT) in Zimbabwe that are involved in straightforward occasional transactions may apply a simple risk scale that distinguishes between high and low risk situations, while other bigger ADLAs may, depending on size and complexity of business have a risk scale with three or more categories, e.g. **Low risk, Medium risk, Medium-Low risk, Medium-High risk, High-Risk, etc**.

(a) Customer risk

2.2.11 Under customer risk, the ADLA assesses the likelihood that a particular customer or type of customer will make use of the products or services of the business to commit money laundering or to finance/support terrorism.

2.2.12 Some customers present higher risks than others. The following types of customers would, in most cases, pose a high inherent risk:-

(i) Politically exposed persons (PEPs);
(ii) High net worth individuals;
(iii) Legal persons and legal arrangements with unnecessarily complex structures or opaque ownership;
(iv) Shelf companies;
(v) Non-resident customers in general; and
(vi) Non-resident customers connected with countries known to present high ML or TF risks;

(b) Products/services risk

2.2.13 Assessment of this risk factor looks at the services/products offered by the institution/business and estimates the likelihood that a particular product would be abused to launder proceeds of crime or to finance terrorism.

2.2.14 Examples of products or services that are normally considered as high risk in the ADLA sector include:-

(i) Cash;
(ii) Wire transfers;
(iii) International inward and outward remittances and
(iv) Products and services or transaction methods that allow a degree of anonymity of the customer, e.g. crypto assets, nominee accounts, complex and opaque corporate structures, etc.)

2.2.15 ADLAs are required to identify and assess the ML/TF/PF risks that may arise in relation to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products.

2.2.16 ADLAs are required to:-

(i) undertake the risk assessment prior to the launch or use of such products, practices and technologies and
(ii) take appropriate measures to manage and mitigate the risks that may arise through the use of such products and practices.

(c) Geographic/country risk

2.2.17 Geographic and country risks looks at the ML/TF risks associated with the country or geographic location of the ADLA as well as the ML/TF risks associated with a customer or a transaction.

2.2.18 Thus, the ADLA must always have regard to the ML/TF types and level of risks to which the country is exposed and which could impact on the ADLAs own ML/TF risks.

2.2.19 In this regard, the ADLA may be guided by the national ML/TF risk assessment, if any, done by the authorities, as well as the ADLA own understanding of the national ML/TF risks.

2.2.20 Similarly, when dealing with customers or transactions associated with a foreign country, the ADLA should pay regard to the ML/TF risks associated with the particular country, e.g. countries that are known to present high terrorism or terrorism financing risks, countries that are associated with high levels of corruption, or countries that are identified by the FATF as not sufficiently implementing AML/CFT/CPF requirements.

(d) Delivery channel risk

2.2.21 Delivery channel risk refers to the method of delivering a financial or other product or service to a customer. This is closely associated with, and can be assessed as part of products/services risks.

2.2.22 Assessment of delivery channel risk normally looks at whether a service/ product is delivered to a customer face-to-face i.e. where the ADLA directly interfaces with a customer, or whether it is delivered through a non-face-to-face medium, such as the internet or through agents (DMT mostly).

2.2.23 Some types of non-face-to-face methods of delivering services present higher ML/TF risks:-

(i) Where business relationship can be established online and
(ii) Where an ADLA relies on agents to identify and verify identities of customers or to deliver services to customers.

Step 3: Risk mitigation

2.2.24 Having identified the different types of risks and assessed the inherent risks, the institution/business should implement controls and measures to mitigate the identified risks, with more focus on the higher risks.

2.2.25 Enhanced controls and measures are required for higher risk customers and situations, while simplified/reduced measures may be implemented for lower risk situations.

2.2.26 Every ADLA is required to have in place an AML/CFT/CPF compliance program that takes into account and addresses the identified risks and the risk levels.

Step 4: Risk Monitoring and evaluation.

2.2.27 Risk assessment is not a once-off event but an ongoing process. ADLAs must, therefore, ensure that the risk assessment is kept current and up to date with the evolving risks.

2.2.28 An ADLA risk assessment should be reviewed at intervals determined by it, usually annually.

2.2.29 A review may be triggered by lapse of the set time period or, at any other time, if there are material events or changes that have a bearing on the entity's ML/TF risks.

2.2.30 Some trigger events/changes may affect only some parts or components of the assessment and may not always require a review of the whole assessment.

2.2.31 As with the original assessments, the risk assessment updates and any adjustments to the controls and measures necessitated by such review should be documented.

2.2.32 ADLAs compliance officers' shall timely report the risk assessment findings, ML/TF risk profiles and the effectiveness of risk control and mitigation measures to the Board and senior management. The frequency of reporting shall be commensurate with the level of risks involved and the ADLA's operating environment.

2.2.33 The Board report referred above (2.2.32) should include, the following:

(i) Results of AML/CFT/CPF monitoring activities carried out by the ADLA such as level of the institution's exposure to ML/TF risks, break-down of ML/TF risk exposures based on key activities or customer segments, trends of suspicious transaction reports and trends of orders received from law enforcement agencies;

(ii) Details of recent significant risk events, that occur either internally or externally, modus operandi and its impact or potential impact to the institution and

(iii) Recent developments in AML/CFT/CPF laws and regulations, and its implications to the institution.

2.2.34 ADLAs are also required to ensure that the identified ML/TF risks, are well understood by staff and proposed controls are implemented and maintained using the RBA.

2.2.35 ADLAs are expected to demonstrate to Financial Surveillance Division their AML/CFT/CPF risk based systems are robust and show that controls are adequate and consistent with international best practice. In assessing ML/TF risks, ADLAs are required to establish internal policies and procedures by having the following processes:-

(i) Documenting their risk assessments and findings; considering all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

(ii) keeping the assessment up-to-date through a periodic review; and

(iii) having appropriate mechanisms to provide risk assessment information to the Financial Surveillance Division.

2.2.36 ADLAs are required to conduct additional assessment as and when required by Financial Surveillance Division.

2.2.37 ADLAs may be guided by the results of the National Risk Assessment disseminated by Financial Surveillance Division in conducting their own risk assessments.

SECTION THREE (3)

SPECIFIC AML/CFT/CPF OBLIGATIONS IN THE CONTEXT OF THE RBA

3.1 AML/CFT/CPF Compliance Program

3.1.1 The various obligations imposed by the MLPC Act require every financial institution to have in place an AML/CFT/CPF compliance program, which must be continuously reviewed and developed to respond to the evolving ML/TF risks.

3.1.2 Section 25 of the MLPC Act sets out and prescribes that:-

(1) Financial institutions and designated non-financial businesses and professions shall develop and implement programmes for the prevention of money laundering and financing of terrorism taking into account the money laundering and terrorist financing risks and size of the business, which programmes shall include the following—

(a) internal policies, procedures and controls to fulfil obligations pursuant to this Act; and

(b) adequate screening procedures to ensure high standards when hiring employees; and

(c) ongoing training for officers and employees to make them aware of this Act and other laws relating to money laundering and the financing of terrorism, with a view to assisting them to recognise 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; and

(d) policies and procedures to prevent the misuse of technological developments including those related to electronic means of storing and transferring funds or value; and

(e) independent audit arrangements to review and verify compliance with and effectiveness of the measures taken in accordance with this Act.

(2) Financial institutions and designated non-financial businesses and professions shall designate a compliance officer at management level to be responsible for the implementation of, and ongoing compliance with, this Act by the institution, business or profession.

3.1.3 AML/CFT/CPF policies, procedures and controls are part of an entire ADLA's AML/CFT/CPF Compliance Program.

3.1.4 AML/CFT/CPF Policy is a document that sets out the entity's high level commitment to implementing measures to combat money laundering and terrorism financing in line with the requirements of the MLPC Act.

3.1.5 The procedures, on the other hand, detail the processes to guide staff on the implementation of the various key AML/CFT/CPF obligations set out in the MLPC Act, including the following:-

(i) Risk assessment;
(ii) Customer due diligence, including Customer identification and verification, Ongoing monitoring;
(iii) Enhanced customer due diligence and transaction monitoring for high-risk customers, including Politically Exposed Persons and
(iv) Detection and reporting of suspicious transactions.

3.1.6 Controls relate to internal systems put in place to combat AML/CFT/CPF risks.

3.2 Customer Due Diligence

3.2.1 Aside from the overarching AML/CFT/CPF obligation to identify, assess and mitigate ML/TF risks, one of the most basic and critical measures to combat ML/TF is the implementation of Customer Due Diligence (CDD) requirements.

3.2.2 CDD also referred to as Know Your Customer (KYC) consists of a number of distinct but connected elements, namely:-

(i) Identifying and verifying a customer's identity;
(ii) Establishing the nature of business and source of funds/wealth of the customer and
(iii) Undertaking ongoing due diligence and monitoring.

3.2.3 This Guidance Manual demonstrates the important interplay between risk assessment and CDD. The ADLA assessment and understanding of the risks presented by different customers and financial products and services, informs the level of due diligence required for each customer category or product type.

❖ Customer identification and identity verification (Section 15 – 23 of the MLPC Act)

3.2.4 The starting point for CDD is for the ADLA to identify and verify the identity of a customer.

3.2.5 Section 15(1) of the MLPC Act obliges financial institutions to identify and verify the identity of their customers by means of an official identification document. To identify a customer and to verify the customer's identity are two separate but related requirements under this provision.

- To identify a customer is to establish and record the name of the customer.

- To verify the identity is to confirm the customer's details by obtaining the official identification document of the customer, i.e. national identity document, or passport, in the case of individuals, or certificate of incorporation or other document evidencing the creation and legal status of the entity.

3.2.6 The obligation to identify and verify the identity of a customer arises in each of the following circumstances:-

(i) Where a financial institution intends to open an account for, or establish a business relationship with a customer; or

(ii) In the case of a proposed occasional once-off transaction, which does not involve the opening of an account or establishment of an ongoing business relationship, if the proposed transaction is valued at US$5,000 or more; or

(iii) In every case where the customer intends to carry out a wire transfer, whether domestic or international, valued at US$1,000 or more; or

(iv) Regardless of the amount involved, if doubt exists regarding the correctness of previously obtained customer identification information; or

(v) Regardless of the amount involved, where there is suspicion of ML/TF.

❖ Requirement to identify ultimate beneficial owners of legal entities: S. 15(3) of MLPC Act.

3.2.7 Over and above the obligation to identify and verify the identity of a customer who is a legal person, ADLAs are also required to identify and verify the identity of the ultimate beneficial owner of the entity.

3.2.8 Beneficial owner(s) refers to the natural person(s) who ultimately owns or exercises effective control over a legal person, including the person who ultimately enjoys the fruits or dividends of the legal entity.

3.2.9 A beneficial owner is not necessarily the same person/entity listed as legal owner (shareholder) in official company documents. In the context of money laundering/terrorism financing, criminals may use nominees and proxies (individuals, trusts or corporate vehicles) as shareholders in an effort to disguise or conceal the true ownership of ill-gotten assets.

3.2.10 To establish who the beneficial owner(s) is/are, the financial institution is required to "pierce the veil" of the entity. Where the corporate entity has a number of corporate shareholders, it may not be practical or beneficial to try to establish the beneficial owners of all the corporate shareholders. As a general guide, it would be sufficient to identify the beneficial owners of only those entities that hold 10% or more shareholding in the company.

3.2.11 Ownership of a legal entity, such as a company, may be either direct or indirect, that is, through one or more controlled entities, such as subsidiaries. It includes ownership that is exercised alone or jointly with one or more other persons.

3.2.12 In determining effective control of a legal entity customer, an ADLA should take steps to identify any person or persons:-

(i) Who can elect a majority of the board of directors, supervisory board, or any equivalent body, of a legal entity; or

(ii) Who can exert a "dominant influence" over the financial, economic, or management policies of the entity regardless of the amount, if any, of share ownership or voting rights in that entity.

3.2.13 In determining "dominant influence", ADLAs should take particular note of any situation in which a majority of the members of the board of directors, supervisory board, or any equivalent body, of a legal entity are accustomed or are obliged to act in accordance with a given person's directions, instructions, or wishes in conducting the affairs of the entity. Such an obligation may be formal or informal.

3.2.14 In some cases, it may not be possible based on the above criteria to identify a natural person who ultimately owns or exerts control over a legal entity. In such cases, ADLAs may deem one or more senior management officials (such as the chief executive officer) to be the beneficial owner(s) of the entity. This,

however, should be done after the ADLA is satisfied that it has exhausted all other means of identification, and that there is no reason to suspect "hidden" or concealed beneficial ownership. The ADLA should keep records of the actions taken to identify the beneficial ownership.

3.2.15 ADLAs need to ensure that they clearly understand the ownership and control structure of any legal entity customer with multiple layers of ownership. This means, among other things, that any intermediate layers of the company's ownership structure should be fully identified.

3.2.16 The ADLA, through its internal procedures, should determine the manner in which this is accomplished. A very effective way to gather this information is to obtain a declaration from an authorised representative, such as a senior official, director, or majority shareholder, and an ownership chart clearly showing the intermediate layers with the respective ownership amounts.

3.2.17 The amount and degree of detail of the information can be determined on a case-by-case basis depending on the perceived degree of risk, but in all cases should include certain basic information.

3.2.18 The name of each company in the group, its jurisdiction of incorporation, and the amount of ownership (direct and indirect) held by other persons, should all be included.

3.2.19 If the institution believes the ownership structure to be needlessly complex, it should inquire about the rationale for the structure. The goal should always be to trace the chain of ownership and actual effective control "all the way to the top," i.e., to the individuals who are the ultimate beneficial owners of the direct customer, and to verify the identity of those individuals.

3.2.20 ADLA does not necessarily need to verify the details of intermediate entities in an ownership chain, unless the structure arouses suspicion.

3.2.21 However, ADLAs should be aware that extremely complicated ownership structures (for example, numerous layers, cross-ownership, companies and controlling shareholders located in different jurisdictions, trusts, and so forth) without an obvious business purpose are often tools for illegitimate activities and should prompt further inquiry.

3.2.22 In some cases, ownership is purposely set up in a confusing manner to hide the actual beneficial owners and their illicit business activities. In such cases, further steps may be necessary to ensure that the institution is satisfied with

the identity of the beneficial owners and that their business activities are legitimate.

3.2.23 Beneficial ownership information can be obtained from a variety of sources, including:

(i) The entity customer itself (the one seeking to transact or open an account) should be asked to disclose its beneficial owners. But such information may still need to be verified through other independent means;

(ii) The deeds and companies' registry. Companies in Zimbabwe, are by law, required to maintain beneficial ownership information and file same with the Registrar of Companies. Similarly trustees of registered trusts are required to maintain and file with the Registrar of Deeds information identifying all the trustees, founder/settlor and beneficiaries;

(iii) Open information sources from the internet concerning the entity, including from the entity's own website, if any.

3.2.24 Identifying the ultimate beneficial owners of legal entities can be a difficult exercise especially where the entity has a complex shareholding structure and even more so where some of the shareholders of the entity are incorporated in offshore jurisdictions.

3.2.25 The extent and expense to which an ADLA should go to identify the ultimate beneficial owner should be guided by its assessment of the ML/TF risk involved.

3.2.26 Where an ADLA has failed to get sufficient reliable information identifying the beneficial owner(s) of a legal entity, and does not have sufficient confidence as to who the customer is, it is not advisable to proceed with the business relationship/occasional transaction, especially where the risk of money laundering appears to be high.

❖ Timing of customer identification and verification (S. 16 of MLPC Act)

3.2.27 As a general rule, identification and identity verification of a customer as required under Section 15 of the MLPC Act, must be undertaken prior to the opening of the account or establishment of the business relationship.

3.2.28 The law, however, recognizes that there are exceptional instances where it may not be possible or practical from a business continuity point of view to

undertake the customer verification before establishing the business relationship.

3.2.29 Financial institutions are thus permitted to allow a customer to utilize a business relationship subject, strictly, to meeting the following conditions:-

(a) Where a delay in verification is unavoidable in the interest of not interrupting the normal conduct of business and

(b) The financial institution adequately manages the ML/TF risk through adoption of risk management procedures under which the customer may utilize the business relationship pending identity verification.

3.2.30 Both conditions (a) and (b) above, must be met, before a financial institution avails itself of this exceptional dispensation.

3.2.31 Possible risk management measures would be for a financial institution to impose restrictions on the nature of transactions that may be undertaken before full identity verification, e.g. allowing inflows into an account and restricting any outflows.

❖ Particulars of customer identification (S. 17 of MLPC Act)

3.2.32 Section 17 lays down the minimum information required as part of customer identification and verification, both for individual and corporate customers.

3.2.33 Over and above identifying a customer and verifying his/her identity by means of an identity document, the following customer identification particulars are required;-

(a) For a customer who is an individual, his or her full name and date and place of birth;

(b) For a legal person the corporate name, head office address, identities of directors, proof of incorporation or similar evidence of legal status and legal form, provisions governing the authority to bind the legal person, and such information as is necessary to understand the ownership and control of the legal person;

(c) For legal arrangements, the names of every trustee, settlor, and beneficiary of an express trust, and of any other party with authority to manage, vary or otherwise control the arrangement;

(d) In addition to the identity of the customer, the identity of any person acting on behalf of a customer, including evidence that such person is properly authorised to act in that capacity;

(e) Information on the intended purpose and nature of each business relationship and

(f) Sufficient information about the nature and business of the customer to permit the financial institution or designated non-financial business or profession to fulfil its obligations under the MLPC Act.

3.2.34 For higher risk customers and situations, in line with the risk-based approach, more information would need to be obtained.

3.2.35 Similarly, for low-risk customers and financial products, the Financial Surveillance Division is empowered to grant exemptions to dispense with some of the identification requirement, although a person's official identification document is normally a non-negotiable minimum requirement.

3.2.36 The ADLA should have clear written AML/CFT/CPF procedures, detailing how it implements the different levels of CDD, in respect of low risk, medium risk and high-risk customer categories.

3.2.37 The procedures should set out which customers are subject to simplified customer identification requirements, based on their low risk status, and what those requirements would be. The procedures should similarly set out enhanced identification requirements for the higher risk customers.

❖ Reliance on customer identification by third parties/intermediaries (S. 18 of MLPC Act)

3.2.38 The obligation to comply with customer identification and verification requirements prescribed by the Act rests squarely with the ADLA concerned.

3.2.39 It is permissible for an ADLA to rely on customer identification and verification performed by third parties or intermediaries/agents, but only under the following conditions:-

(a) only where there is no suspicion of ML/TF, and

(b) provided that information on the identity of each customer or beneficial owner is obtained immediately on opening the account or establishing the business relationship, and

(c) the financial institution is satisfied that the third party is:-

(i) in a position to provide, without delay, copies of the relevant identification and other required documents;
(ii) is established, domiciled or ordinarily resident in a compliant jurisdiction;
(iii) has an adequate CDD process and
(iv) is properly regulated and supervised by the respective authorities.

3.2.40 The ADLAs relying on a third party for customer identification remains ultimately responsible for any non-compliance with the identification and verification requirements set out by the MLPC Act.

3.2.41 Some ADLAs rely on agents to recruit/onboard customers. In such cases, it is the ADLA's responsibility to ensure that every such agent is adequately trained on, and complies with the identification/verification requirements of the MLPC Act and should have written procedures on conducting the process.

❖ Identification and identity verification of non-face-to-face customers

3.2.42 An ADLA may find itself in a situation where it is necessary or expedient to establish a business relationship with a customer who is not or cannot be physically present for purposes of identification and identity verification.

3.2.43 Such a situation presents a heightened ML/TF risk and the ADLA must take reasonable and adequate measures to satisfy itself that the customer is who he/she/it presents itself to be.

3.2.44 Section 19 of the MLPC Act provides that:-

(1) designated non-financial businesses and professions shall take adequate measures to address the specific 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.
(2) Such measures shall ensure that the due diligence is no less effective than where the customer appears in person, and may require additional

documentary evidence, or supplementary measures to verify or certify the documents supplied, or confirmatory certification from financial institutions or other documentary evidence or measures, as may be prescribed in directives.

3.2.45 ADLAs may obtain an attestation from the third party to satisfy themselves that the requirements have been met.

3.2.46 ADLAs are required to be vigilant in establishing and conducting business relationships via information communication technology.

3.2.47 When dealing with non-face to face customers, ADLAs are required to establish appropriate measures for the identification and verification of such customers' identity that shall be as effective as that for face-to-face customers and implement monitoring and mechanisms to identify potential ML/TF/PF activities.

3.2.48 ADLAs may use the following measures to verify the identity of non-face -to-face customer:-

(i) requesting additional documents to complement those which are required for face-to-face customer;
(ii) developing independent contact with the customer; or

(iii) verifying customer information against any database maintained by the authorities.

❖ Enhanced Identification and due diligence requirements for high risk customers

3.2.49 Section 20 (1) (a) of the MLPC Act requires financial institutions to put in place risk management systems:-

"to identify customers whose activities may pose a high risk of money laundering and financing of terrorism and shall exercise enhanced identity verification and ongoing due diligence procedures with respect to such customers".

3.2.50 This provision should be read in conjunction with Section 12B of the MLPC Act which requires financial institutions to identify, assess and mitigate the ML/TF risks to which their businesses are exposed.

3.2.51 The obligations in Section 12B are wider, encompassing assessment of all ML/TF risk factors, including customer risk, product risk, delivery channel risk and geographic risk.

3.2.52 Section 20, on the other hand, emphasizes customer risk, i.e. the need to identify which customers present the highest ML/TF risk and the need to exercise enhanced customer identification, verification and ongoing due diligence and monitoring.

❖ Identification and due diligence requirements for politically exposed persons

3.2.53 Section 20 (1) (b) requires ADLAs to put in place risk management systems to determine if a customer or beneficial owner of an account/transaction is a politically exposed person (PEP).

3.2.54 If a customer or beneficial owner is identified as a PEP, an ADLA is required to:-

(a) Obtain senior management approval before establishing a business relationship with the customer; or, if the customer is identified as a PEP after a business relationship had already been established, senior management approval is required to continue with the business relationship; and

(b) Take all reasonable measures to identify the source of wealth and funds and other assets of the customer or beneficial owner of the customer.

3.2.55 A politically exposed person is defined under Section 13 of the MLPC Act as –

(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 of 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 of 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, including the position of director, deputy director, member of the board or equivalent functions; or

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

3.2.56 PEPs are a special class of customers, who are deemed, by law, as presenting a high ML/TF risk, arising from the power and influence they wield, which can, potentially be abused for personal enrichment through corruption and embezzlement. However, they can be disaggregated as follows:-

- **Foreign PEPs**

3.2.57 ADLAs are required to put in place a risk management system to determine whether a customer or a beneficial owner is a foreign PEP.

3.2.58 Upon determination that a customer or a beneficial owner is a foreign PEP, the requirements of enhanced CDD must be conducted.

- **Domestic PEPs.**

3.2.59 ADLAs are required to take reasonable measure to determine whether a customer or beneficial owner is a domestic PEP or a person entrusted with a prominent function by an international organization.

3.2.60 If the customer or beneficial owner is assessed as a domestic PEP or a person entrusted with a prominent function by an international organization, ADLAs are required to assess the level of ML/TF risks posed by business relationship with the domestic PEP or person entrusted with a prominent function by an international organization.

3.2.61 The assessment of the ML/TF risks shall take into account the profile of the customer on Risk Profiling.

3.2.62 The requirements of enhanced CDD must be conducted in respect of domestic PEPs who are assessed as high risk.

3.2.63 ADLAs may apply standard CDD measures similar to other customer for domestic PEPs if the ADLA is satisfied that the domestic PEPs or person

entrusted with a prominent function by an international organization are low risk.

3.2.64 For non-PEP customers, ADLAs have the obligation to assess the ML/TF risk and decide each customer's risk category, e.g. low, medium or high risk. PEPs, especially all foreign ones, however are, by law, automatically deemed as high risk and ADLAs do not have the discretion to assess the risk differently.

❖ What to do if customer identification obligations cannot be fulfilled

3.2.65 Section 22 of the MLPC Act prohibits a financial institution from establishing or continuing a business relationship with a customer, if the identification and verification requirements set out above cannot be fulfilled.

3.2.66 In addition to declining or discontinuing the business relationship/transaction, the ADLA is required to immediately report the matter to Financial Surveillance Division and/or FIU.

3.2.67 Section 22 of the MLPC Act provides as follows:-

> *"A financial institution or designated non-financial business and profession that cannot fulfil the requirements of this Part with respect to any customer or beneficial owner shall not establish an account for or maintain the business relationship with that customer and shall immediately make a report on the matter to the Unit".*

❖ Ongoing Due Diligence and Monitoring (Section 26 of the MLPC Act)

3.2.68 CDD is not a once-off exercise, confined only to customer identification and identity verification at the time of establishing a business relationship with the customer.

3.2.69 Customer identification and verification requirements only represent the first stage of an ongoing process that continues for the entire duration of the business relationship.

3.2.70 Just as is the case with the initial customer identification and verification stage, the level of ongoing due diligence and monitoring depends on the risk category of the customer.

3.2.71 For low-risk customers and low risk financial products, only simplified/reduced due diligence and monitoring is required, while for higher risk customers and/or

higher risk products and services, enhanced due diligence (EDD) and monitoring is mandatory.

3.2.72 An ADLA should have written AML/CFT/CPF procedures that detail how the business entity implements risk-based CDD. The procedure should set out and describe the different levels of due diligence for each customer risk category.

3.2.73 It should be noted that the law does not allow a financial institution to dispense with CDD and monitoring requirements for any customer or for any financial product on the grounds that the ML/TF risk is nil. ML/TF risk can never be zero, but can only be low, hence the need for reduced level of monitoring for low-risk situations.

3.2.74 A customer's risk profile can change when there are some material changes in the customer's or other relevant circumstances, e.g., if there are changes in the customer's line of business, source of funds, volume/value of transactions etc. It is thus important for ADLAs to not only monitor each customer's activities and circumstances on an ongoing basis, guided by the customer's risk category, but also to undertake periodic risk assessment reviews for the entire customer base.

3.2.75 Section 26 of the MLPC Act sets out the obligations of financial institutions in relation to ongoing due diligence. It provides thus:-

> *(1) Financial institutions and designated non-financial businesses and professions shall exercise ongoing due diligence with respect to business relationships that are or may become subject to the requirements of customer identification and verification, including – (a)maintaining current information and records relating to the customer and beneficial owner concerned; and (b) closely examining the transactions carried out in order to ensure that such transactions are consistent with their knowledge of their customer, and the customer's commercial or personal activities and risk profile; and 27 (c) ensuring the obligations pursuant to Sections 19, 20 and 21 relating to high risk customers, politically-exposed persons, and correspondent banking relationships are fulfilled.*
>
> *(2) Financial institutions and designated non-financial businesses and professions shall – (a) pay special attention to all complex, unusual large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose; and (b)pay special attention to business relations and transactions with persons, including legal persons and arrangements, from or in non-compliant or*

insufficiently compliant jurisdictions; and (c) examine as far as possible the background and purpose of transactions under paragraphs (a) and (b) and set forth in writing their findings; and (d)take such specific measures as may be prescribed by directive from time to time to counter the risks with respect to business relations and transactions specified under paragraph (b).

(3)The findings referenced in subsection (2)(c) shall be maintained as specified in Section 24, and be made available promptly if requested by the Unit or by a foreign counterpart agency, a competent supervisory authority or other authority prescribed by the Minister.

❖ Higher risk countries (Section 26A) of the MLPC Act

3.2.76 Financial institutions are required to conduct enhanced due diligence, proportionate to the risk towards business relationships and transactions with any natural or legal person from countries identified as non-cooperative in implementing AML/CFT/CPF standards.

3.2.77 The lead agency FIU is mandated to communicate such list, as updated from time to time, to financial institutions, including ADLAs. The list may include non-compliant countries identified and listed by the FATF or identified by the FIU on its own initiative.

3.2.78 With respect to some of the countries on the FATF "black list", ADLAs may be required to take specified counter-measures as set out in Directives issued by FIU from time to time. For transactions involving other non-compliant countries where no FATF countermeasures are specified, ADLAs are simply required to implement EDD, having regard to the nature of the AML/CFT/CPF shortcomings and risks of each specified country.

3.2.79 In addition to the enhanced CDD requirements, ADLAs are required to, on a continuous basis, apply appropriate countermeasures, proportionate to the risk, for high risk countries listed as having on-going or substantial ML/TF risks, as follows:-

(i) limiting business relationship or financial transactions with identified jurisdictions or persons located in the country concerned;

(ii) review and amend, or if necessary terminate, relationships with financial institutions in the country concerned and

(iii) conduct enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the institution or financial group, located in a jurisdiction of concern.

3.3 Suspicious Transaction Report (STR)

3.3.1 This is another fundamental obligation key to combating ML/TF. An ADLA is required to report every suspicious transaction, in prescribed form through the GoAML platform, to the FIU.

3.3.2 In terms of timing, the obligation is to submit the report to the FIU promptly, but in any case, not later than three (3) working days from the time when the suspicion arises.

3.3.3 A suspicious transaction includes an attempted transaction, i.e. where the transaction was not completed, but was nevertheless suspicious.

3.3.4 Section 30(1) of the MLPC Act provides that –

(1) Subject to subsections (2) and (3), financial institutions, designated non-financial businesses and professionals, and their respective directors, principals, officers, partners, professionals, agents and employees, that suspect or have reasonable grounds to suspect that any property or any transaction or attempt to effect a transaction –

(a) involves or is the proceeds of crime; or

(b) is related or linked to, or is to be used for, terrorism, terrorist acts or by terrorist organisations or those who finance terrorism; shall submit promptly, but not later than three working days after forming the suspicion, a report setting forth the suspicion to the Unit.

3.3.5 **Annexure "C"** gives a non-exhaustive list of indicators or red flags that are useful in helping an ADLA identify and report suspicious transactions.

3.3.6 Some suspicious transaction red flags/indicators are business-type specific. It is thus important for ADLAs and their staff to be familiar with the common ML/TF red flags associated with their respective types of businesses.

3.3.7 ADLAs are required to ensure that its designated branch or subsidiary compliance officer is responsible for channelling all internal suspicious transaction reports received from employees of the respective branch or

subsidiary to the Compliance Officer at the head office. In the case of employees at the head office, such internal suspicious transaction reports shall be channelled directly to the Compliance Officer.

3.3.8 Upon receiving any internal suspicious transaction report whether from the head office, branch or subsidiary, the Compliance Officer must evaluate the grounds for suspicion. Once the suspicion is confirmed, the Compliance Officer must promptly submit the suspicious transaction report to the FIU.

3.3.9 In the case where the Compliance Officer decides that there are no reasonable grounds for suspicion, the Compliance Officer must document and file the decision, supported by the relevant documents.

3.3.10 The Compliance Officer must submit the STR in the specified suspicious transaction report form through the GoAML system.

3.3.11 ADLAs must ensure that in the course of submitting the STR, utmost care must be undertaken to ensure that such reports are treated with the highest level of confidentiality. The Compliance Officer has the sole discretion and independence to report suspicious transactions.

3.3.12 ADLAs must provide additional information and documentation as may be requested by the FIU and to respond promptly to any further enquiries with regard to any report received under Section 30 of the MLPC Act.

3.3.13 Institutions must ensure that the STR mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy.

3.3.14 Where an STR has been lodged, institutions are required to make a fresh STR on the same, when a new suspicion arises.

3.3.15 ADLAs are required to establish internal criteria ("red flags") to detect suspicious transactions. ADLAs must consider submitting STR when any of its customer's transaction or attempted transaction fits the institution's list of "red flags."

3.3.16 ADLAs must ensure that the Compliance Officer maintains a complete file of all internally generated reports and any supporting documentary evidence regardless of whether such reports have been submitted. In cases where an STR is not reported to the FIU, the internally generated reports on such

transactions and the relevant supporting documentary evidence must be made available to supervisory authorities upon request.

3.4 Prohibition against tipping-off

3.4.1 Except where required by law, an ADLA shall not disclose to its customer or to a third party that an STR has been submitted or will be submitted to the FIU.

3.4.2 Such disclosure has the effect of tipping-off the customer and afford him/her the opportunity to take steps to defeat or undermine any subsequent investigations by law enforcement agencies.

3.4.3 Section 31(2) of the MLPC Act provides that :–

"No financial institution or designated non-financial business or profession, nor any director, partner, officer, principal or employee thereof, shall disclose to any of their customers or a third party that a report or any other information concerning suspected money laundering or financing of terrorism will be, is being or has been submitted to the Unit, or that a money laundering or financing of terrorism investigation is being or has been carried out, except in the circumstances set forth in subsection (3) or when otherwise required by law to do so."

3.5 Submission of Large Cash Transaction reports

3.5.1 In addition to the obligation to report suspicious transactions to the FIU as required under Section 30(1) of MLPC Act, the FIU may, in terms of Section 30(6) of MLPC Act require ADLAs to submit threshold-based transaction reports.

3.5.2 Under this requirement, the FIU issues directives from time to time requiring financial institutions to submit returns in respect of all cash transactions of or above a specified threshold, otherwise referred to as "large cash transaction" reports.

3.5.3 It is important to note the difference between STRs and threshold-based cash transaction reports (CTRs).

(i) STRs must be submitted in terms of Section 30 (1) of the MLPC Act, regardless of the value involved as long as the transaction is a suspicious one.

(ii) CTRs must be submitted in compliance with any applicable Directive issued by the FIU, regardless of whether or not the transaction is suspicious.

(iii) If a transaction is suspicious and also meets the CTR reporting threshold, it must be reported separately, both as an STR and as a CTR.

3.6 Management Information System

3.6.1 ADLAs must have in place adequate management information systems (MIS), either electronically or manually, to complement its CDD processes. The MIS is required to provide the institution with timely information on a regular basis to enable the ADLA to detect irregularities and any suspicious activity.

3.6.2 The MIS shall be commensurate with the nature, scale and complexity of the ADLA's activities and ML/TF/PF risk profile.

3.6.3 The MIS shall include, at a minimum, information on multiple transactions over a certain period, large transactions, transaction patterns, customer's risk profile and transactions exceeding any internally specified thresholds.

3.6.4 The MIS shall be able to aggregate customer's transactions from multiple accounts and from different systems. It should also be used to monitor transactions and flag out any suspicious transactions.

3.6.5 The MIS may be integrated with the ADLA's information system that contains its customer's normal transactions or business profile, which is accurate, up-to-date and reliable.

3.7 Independent Audit Functions

3.7.1 ADLAs should ensure regular independent audits of the AML/CFT/CPF measures are undertaken to determine their effectiveness and compliance with the MLPC Act, AML/CFT/CPF directives, policies, and circulars.

3.7.2 The Board is required to ensure that the roles and responsibilities of the auditors are clearly defined and documented. The roles and responsibilities of the auditors shall include, at a minimum:-

(i) checking and testing compliance with, and effectiveness of the AML/CFT/CPF policies, procedures and controls and

(ii) assessing whether current measures are in line with the latest developments and changes of the relevant AML/CFT/CPF requirements.

3.7.3 The scope of independent audit shall include, at a minimum:-

(a) compliance with MLPC Act;

(b) compliance with the institution's internal AML/CFT/CPF policies and procedures;

(c) adequacy and effectiveness of the AML/CFT/CPF compliance programme and

(d) reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.

3.7.4 The auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of AML/CFT/CPF measures and any inadequacy in internal controls and procedures.

3.7.5 ADLAs are required to ensure that independent audits are carried out at least on an annual basis.

3.7.6 ADLAs must ensure that such audit findings and the necessary corrective measures undertaken are submitted to the Financial Surveillance Division within one (1) month after the completion of the internal audit.

3.8 Employee Training and Awareness Programmes

3.8.1 ADLAs are required to conduct awareness and training programmes on AML/CFT/CPF practices and measures for their employees. Such training must be conducted regularly.

3.8.2 Employees must be made aware that they may be held personally liable for any failure to observe the AML/CFT/CPF requirements and for tipping off.

3.8.3 The ADLA must make available its AML/CFT/CPF policies and procedures to all employees.

3.8.4 The training conducted for employees must be appropriate to their level of responsibilities in detecting ML/TF/PF activities and the risks of ML/TF/PF faced by the institutions.

3.8.5 Employees who deal directly with customers receive prior training on AML/CFT/CPF before dealing with customers.

3.8.6 Training for all employees may provide a general background on ML/TF, the requirements and obligations to monitor and report suspicious transactions to the Compliance Officer and the importance of CDD.

3.8.7 In addition, training may be provided to specific categories of employees:-

(a) Front-Line Employees

3.8.8 Front-line employees may be trained to conduct effective on-going CDD, detect suspicious transactions and on the measures that need to be taken upon determining a transaction as suspicious. Training may also be provided on factors that may give rise to suspicion, such as dealing with occasional customer transacting in large amount of transaction, PEPs, higher risk customers and the circumstances where enhanced CDD is required.

(b) Employees that Establish Business Relationships

3.8.9 The training for employees who establish business relationships may focus on customer identification, verification and CDD procedures, including when to conduct enhanced CDD and circumstances where there is a need to defer establishing business relationship with a new customer until CDD is completed satisfactorily.

(c) Supervisors and Managers

3.8.10 The training on supervisors and managers may include overall aspects of AML/CFT/CPF procedures, in particular, the risk-based approach to CDD, risk profiling of customers, enforcement actions that can be taken for non-compliance with the relevant requirements pursuant to the relevant laws and procedures related to the financing of terrorism.

3.9 Record Keeping Requirements

3.9.1 Section 24 of the MLPC Act sets out the record-keeping obligations of financial institutions, prescribing what must be covered by such records as well as the minimum length of time for which such records should be kept.

3.9.2 The record-keeping obligations are meant to assist Financial Surveillance Division, FIU and law enforcement agencies should the need arise to investigate a customer or a transaction.

3.9.3 Section 24 of the MLPC Act provides that –

(1) Financial institutions and designated non-financial businesses and professions shall maintain all books and records with respect to their customers and transactions as set forth in subSection (2), and shall ensure that such records and the underlying information are available on a timely basis to the Unit and such other competent authorities as are prescribed by the Minister.

(2) Such books and records shall include, as a minimum—

a. account files, business correspondence, and copies of documents evidencing the identities of customers and beneficial owners obtained in accordance with this Act, all of which shall be maintained for not less than five years after the business relationship has ended; and

b. records on transactions sufficient to reconstruct each individual transaction for both account holders and non-account holders which shall be maintained for not less than five years from the date of the transaction; and

c. the findings set forth in writing pursuant to Section 26(2)(c) and related transaction information which shall be maintained for at least five years from the date of the transaction; and

d. copies of all suspicious transaction reports made pursuant to Section 30, including any accompanying documentation, which shall be maintained for at least five years from the date the report was made.

3.10 IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS PURSUANT TO UNITED NATIONS SECURITY COUNCIL RESOLUTIONS

3.10.1 Countries are required to implement the requirements of United Nations Security Council Resolutions (UNSCRs) that are issued in terms of Chapter VII of the United Nations Charter.

3.10.2 Under these Chapter VII powers, the United Nations has various resolutions in force requiring countries to enforce targeted financial sanctions to combat financing of terrorism and financing of proliferation of weapons of mass destruction.

3.10.3 The resolutions identify (and require countries to identify) persons and entities involved in financing terrorism or in financing proliferation of weapons of mass destruction.

3.10.4 Pursuant to its international obligations, Zimbabwe passed the following statutory instruments:-

(i) Statutory Instrument 76 of 2014, requiring financial institutions, and other persons, to identify, freeze and report funds or other assets of individuals and entities identified by or under the authority of the United Nations Security Council for financing or supporting international terrorism and

(ii) Statutory Instrument 110 of 2021 and Statutory Instrument 164 of 2023, requiring financial institutions, and other persons to identify, freeze and report funds or other assets of individuals and entities identified by or under the authority of the United Nations Security Council for financing or promoting proliferation of weapons of mass destruction.

3.10.5 The FIU issues Directives and guidance, from time to time, on the implementation of the requirements of the two UN sanctions regimes.

3.10.6 ADLAs are required to submit an STR when there is an attempted transaction by any of the persons listed in the Consolidated List.

3.10.7 ADLAs are required to ascertain potential matches with the Consolidated List to confirm whether they are true matches to eliminate "false positives". ADLAs are required to make further inquiries from the customer or counter-party (where relevant) to assist in determining whether the match is a true match.

3.10.8 ADLAs are required to confirm receipt and communicate the outcome of the name search in its database to the FIU, within three (3) days of receiving the directive.

3.10.9 ADLAs may also scan their database against other recognised lists of designated persons or entities issued by other jurisdictions and organisations such as the European Union.

3.10.10 The same process on terrorist financing should be implemented for customers linked to PF.

3.11 Corporate Governance

(a) Board of Directors

3.11.1 Board of Directors must understand their roles and responsibilities in managing ML/TF/PF risks faced by the institution.

3.11.2 Board members must be aware of the ML/TF/PF risks associated with business strategies, customers, delivery channels and geographical coverage of its business products and services.

3.11.3 They must understand the AML/CFT/CPF measures required by FATF, the provisions of the MLPC Act and other international best practices.

3.11.4 Board of Directors have the following roles and responsibilities:-

(i) maintain accountability and oversight for establishing AML/CFT/CPF policies and minimum standards;

(ii) approve policies regarding AML/CFT/CPF measures within the institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions, combating the financing of terrorism and proliferation financing;

(iii) establish appropriate mechanism to ensure the AML/CFT/CPF policies are periodically reviewed and assessed in line with changes and developments in the institution's products and services, technology as well as trends in ML/TF;

(iv) establish an effective internal control system for AML/CFT/CPF and maintain adequate oversight of the overall AML/CFT/CPF measures undertaken by the ADLA;

(v) define the lines of authority and responsibility for implementing the AML/CFT/CPF measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;

(vi) ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF;

(vii) ensure regular assessment of ML/TF/PF risks and application of the risk-based approach (RBA) to the compliance programme;

(viii) assess the implementation of the approved AML/CFT/CPF policies through regular updates by the senior management and Audit Committee and

(ix) establish MIS that is reflective of the nature of the ADLA's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered and geographical coverage.

(b) Senior Management

3.11.5 Senior management must be accountable for the implementation and management of AML/CFT/CPF compliance programmes in accordance with policies and procedures established by the Board, requirements of the law, regulations, Guidance Manual and international best practices.

3.11.6 Senior management have the following roles and responsibilities:-

(i) be aware of and understand the ML/TF/PF risks associated with business strategies, customers, delivery channels and geographical coverage of its business products and services offered and to be offered including new products, new delivery channels and new geographical coverage;

(ii) formulate AML/CFT/CPF policies to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by the institution;

(iii) establish appropriate mechanism and formulate procedures to effectively implement AML/CFT/CPF policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;

(iv) undertake review and propose to the Board necessary enhancements to the AML/CFT/CPF compliance programme;

(v) Approve business relationships with high-risk customers and PEPs;

(vi) provide timely updates to the Board on the level of ML/TF risks facing the institution, strength and adequacy of risk management and internal

controls implemented to manage the risks and the latest development on AML/CFT/CPF which may have an impact on the institution;

(vii) allocate adequate resources to effectively implement and administer AML/CFT/CPF compliance programmes using the RBA;

(viii) appoint a compliance officer at management level at Head Office and designate a compliance officer at each branch or subsidiary;

(ix) provide appropriate levels of AML/CFT/CPF training for employees at all levels throughout the institution;

(x) ensure that there is a proper channel of communication in place to effectively communicate the AML/CFT/CPF policies and procedures to all levels of employees;

(xi) ensure that AML/CFT/CPF issues raised are addressed in a timely manner and

(xii) ensure the integrity of employees by establishing appropriate employee assessment system.

(c) Compliance Management Arrangements

3.11.7 The Compliance Officer acts as the reference point for AML/CFT/CPF matters within the institution.

3.11.8 The Compliance Officer must have sufficient authority and seniority within the institution to participate and be able to effectively influence decisions relating to AML/CFT/CPF.

3.11.9 The Compliance Officer is required to be "fit and proper" to carry out his AML/CFT/CPF responsibilities effectively. The "fit and proper" test relates to:-

(i) probity, personal integrity and reputation and
(ii) competency and capability.

3.11.10 The Compliance Officer must have the necessary knowledge and expertise to effectively discharge his roles and responsibilities, including being informed of the latest developments in ML/TF/PF techniques and the AML/CFT/CPF measures undertaken by the ADLA industry.

3.11.11 ADLAs should require their Compliance Officers to pursue professional qualifications in AML/CFT/CPF so that they are able to carry out their obligations effectively.

3.11.12 Institutions are required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.

3.11.13 The Compliance Officer has a duty to ensure the following:-

(i) the institution is in compliance with AML/CFT/CPF requirements;

(ii) proper implementation of the AML/CFT/CPF policies and procedures; including, CDD, record-keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism and proliferation financing;

(iii) the AML/CFT/CPF programme is regularly assessed to ensure that it is effective and sufficient to address any change in ML/TF/PF risk trends;

(iv) the channel of communication from the respective employees to the branch or subsidiary compliance officer and subsequently to the Compliance Officer is secured and that information is kept confidential;

(v) all employees are aware of the institution's AML/CFT/CPF programme;

(vi) internally generated STRs by the branch or subsidiary compliance officers are appropriately evaluated before submission to the FIU and

(vii) the identification and assessment of ML/TF/PF risks associated with new products or services or arising from the institution's operational changes, including the introduction of new technology and processes.

3.11.14 ADLAs are required to inform, in writing the Financial Surveillance Division within thirty working days, on the appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, fax number, e-mail address and such other information as may be required.

3.11.15 The Compliance Officer or any designated person should ensure that customers are screened against Sanctions lists.

(d) Employee Screening Procedures

3.11.16 The screening procedures shall apply upon hiring the employee and throughout the course of employment.

3.11.17 ADLAs are required to establish an employee assessment system that is commensurate with the size of operations and risk exposure of ADLAs to ML/TF.

3.11.18 The employee assessment system shall include an evaluation of an employee's personal information, including criminal records, employment and financial history.

3.12 Enforcement of AML/CFT/CPF Obligations to ADLAs Foreign Branches and Subsidiaries

3.12.1 The requirements of this Guidance Manual are applicable to Zimbabwean licensees operating as foreign branches, subsidiaries and offices, wherein they are required to comply with the policies and procedures as implemented by their head office. However, if policies and procedures as implemented by their head office are inconsistent with the requirements of this document or less stringent than stated in this document, the requirements prescribed herein in this document shall prevail.

3.12.2 ADLAs are required to closely monitor their foreign branches, subsidiaries and offices operating in jurisdiction with inadequate AML/CFT/CPF laws and regulations as highlighted in the FATF Standards or in MLPC Act.

3.12.3 ADLAs are required to ensure that their foreign branches, subsidiaries and offices apply AML/CFT/CPF measures consistent with the home country requirements. Where the minimum AML/CFT/CPF requirements of the host country are less stringent than those of the home country, the institution must apply the home country requirements, to the extent that the host country laws and regulations permit.

3.12.4 If the host country does not permit the proper implementation of AML/CFT/CPF measures consistent with the requirement in Zimbabwe, ADLAs are required to apply appropriate additional measures to manage the ML/TF risks, and report to Financial Surveillance Division on the AML/CFT/CPF gaps and additional measures implemented to manage the ML/TF/PF risks arising from the identified gaps.

3.12.5 In addition, ADLAs may consider ceasing the operations of the said branch, subsidiary or offices that is unable to put in place the necessary mitigating control measures. These shall include the following measures:-

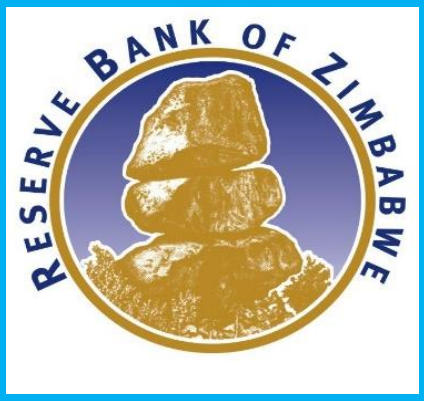
(i) framework for AML/CFT/CPF Compliance programme at the group level;
(ii) appoint a group compliance officer at management level;
(iii) policies and procedures for sharing information required for the purposes of CDD and ML/TF/PF risk management;
(iv) the provision of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT/CPF purposes;
(v) safeguards on the confidentiality and use of information exchanged and
(vi) A group compliance officer is responsible for creating, coordinating and making a group-wide assessment for the implementation of a single AML/CFT/CPF strategy, including mandatory policies and procedures and the authorization to give orders to all branches and subsidiaries.

3.13 Duty to Familiarise with Core Issues Under Immediate Outcomes Relating to Private Sector Financial Institutions

3.13.1 Immediate Outcomes (IOs) which measure **effectiveness** for the private sector, seeks to assess the adequacy of the implementation of the FATF Recommendations. These IOs identify the extent to which private sector achieves a defined set of outcomes that are central to a robust AML/CFT/CPF system.

3.13.2 ADLAs, together with their Boards, Senior management and Staff are required to be fully conversant with the provisions (core issues) of the FATF IOs in particular IO1, IO2, IO3, IO5, IO6, IO10 and IO11,[5] relating to financial institutions.

[5] Immediate Outcome 1 – Risk, Policy and Coordination
Immediate Outcome 2 – International Co-operation
Immediate Outcome 3 – Supervision and Preventive Measures for Financial Institutions (Fis) and VASPs
Immediate Outcome 5 – Legal Persons and Arrangements
Immediate Outcome 6 – Financial Intelligence ML/TF
Immediate Outcome 10- Terrorism Financing preventive measures and financial sanctions
Immediate Outcome 11- Proliferation Financing Sanctions



SECTION FOUR (4)

PENALTIES FOR NON-COMPLIANCE WITH AML/CFT/CPF OBLIGATIONS

4.1 PENALTIES

4.1.1 Non-compliance by an ADLA with any of the AML/CFT/CPF obligations under the MLPC Act or the obligations relating to the implementation of Targeted Financial Sanctions under statutory instruments 76 of 2014 and 110 of 2021, can attract either criminal sanctions or civil penalties (or both).

4.1.2 Section 5(3) of MLPC Act empowers the FIU to issue a directive to Competent Supervisory Authorities (CSAs) to impose civil and administrative penalties on financial institutions (and/ or the directors, employees and agencies) specifying the conditions under which CSAs may impose such penalties.

4.1.3 On 6 January 2022, FIU issued AML/CFT/CPF Directive PFIU1/2022, empowering and authorizing CSAs to impose civil and administrative penalties in respect of institutions, businesses or authorities under their respective supervisory jurisdiction, for breach of any of the obligations imposed under MLPC Act.

4.1.4 Based on this, Financial Surveillance Division is empowered to impose criminal and civil penalties which are enforceable against the ADLA or any of its employees, directors or agents, as the case may be or against both the institution/business and the responsible individuals.

4.1.5 In addition, administrative penalties are enforceable by the FIU under Section 5 of the MLPC Act. Under this provision, the FIU can, among other enforcement measures:-

(i) Impose a financial penalty against the institution/business or any of its employees, directors or agents; and/or

(ii) Order the removal of any employee, director or shareholder; and/or

(iii) Require the ADLA to take specified remedial action.

4.1.6 Financial Surveillance Division is guided by the Civil Penalties Enforcement Manual of December 2021, issued by the FIU, as read with AML/CFT/CPF Directive No. 2 of 2014 in relation `to the charges and penalty levels.

4.1.7 **Annexure ''D''** provides a non-exhaustive list of regulatory risk subject to imposition of monetary penalties.

SECTION FIVE (5)

ANNEXURES

Annexure A: Varying Degrees of Customer Due Diligence

(a) Simplified Customer Due Diligence

- ✓ Simplified due diligence is the least ranking of due diligence that can be applied on a customer especially where there is low probability of ML/FT risk posed by a customer to an entity.
- ✓ In most instances simplified customer due diligence requires customers to submit certain basic information such as name, national identity card, address, as well as passport-size picture.

(b) Standard Due Diligence

- ✓ Most customer relationships can be handled through standard due diligence. Standard due diligence should be applied when a new business relationship is established or certain occasional transactions are to be conducted.

(c) Enhanced due diligence

- ✓ Enhance Due Diligence is required where the customer and product or service combination is considered to be of greater risk. This higher level of due diligence is required to mitigate the increased risk. High risk situation poses high probability of money laundering or terrorist financing through the service and product which is being provided or through customer.
- ✓ Enhanced due diligence may entail gathering additional information to verify the customers' identity or source of income or perhaps an adverse media checks. The checks should be relative and proportionate to the level of risk identified and provide confidence that any risk has been mitigated and that the risk is unlikely to be realized.
- ✓ Situations that may be considered as high risk are cases where you may not meet the customer face to face or where you are dealing with a politically exposed person. Being a high-risk customer does not necessarily mean one is involved in money laundering or other criminal activity but there is high probability of such occurrences.
- ✓ In order to determine the appropriate due diligence (standard, simplified, or enhanced due diligence) ADLAs shall consider the following:-

    a) The customer's residence or location of the customer's business;

    b) The customer's occupation or nature of business;

    c) The purpose of the business transactions;

d) The anticipated pattern of transaction activity, including monetary amounts, and frequency;

e) The anticipated origin and methods of payments;

f) Basic founding documents of legal entity customers, such as articles of incorporation, partnership agreements, and business certificates;

g) Basic information about the customer's own customers;

h) Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner,;

i) Basic information about the customer's other significant personal and business relationships;

j) Approximate annual income or business revenue;

k) AML policies and procedures in place;

l) Third-party documentation;

m) The customer's reputation in the local market, through review of media and other publicly available sources.

Annexure B: Basic Contents of a Suspicious Transaction Report

(a) Reporting Institution Information

(i) Name and address of institution;
(ii) Name and address of Branch where the activity occurred

(b) Suspect Information

(i) Full Names or Name of Entity;
(ii) Address, Phone Number, Residence, Work;
(iii) Occupation/Type of business, Date of birth;
(iv) Forms of identification - National registration number - Valid Passport Number - Zimbabwean Driver's License and
(v) Relationship to financial institution (Employee, Director, Officer, Shareholder, Customer etc.)

(c) Description of the suspicious activity

(i) Type of transaction;
(ii) Amount involved;
(iii) Other details necessary to understand the transaction

(d) Action already taken

(i) If an insider is involved what action has been taken?
(ii) Has any law enforcement agency been advised? If yes, provide name of agency, name and telephone number of person(s) contacted, and by what method (telephone, written communication, etc)

(e) Contact person

(i) Full names;
(ii) Title / Designation;
(iii) Contact telephone number

(f) Date of suspicious transaction and date of preparation of report

Annexure C: non exhaustive Indicators/ Reflags of Suspicious Transactions Examples of suspicious transactions red flag, i.e., ways in which money may be laundered.

(a) Unusual Transactions

(i) Buying and selling of foreign exchange with no discernible purpose or in circumstances which appear unusual.

(ii) The intensity of transactions for an inactive trading account suddenly increases without plausible reason.

(iii) Frequent selling of currencies at significant losses.

(iv) Structuring transactions to evade reporting.

(v) Simultaneous transfer of funds to a group of recipients

(vi) Request to exchange large quantities of low denominations for higher denominations.

(vii) Transactions for which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

(b) **Large Cash Transactions**

(i) Exchanging large foreign exchange cash amounts in the reporting institution's on the same day.

(c)Transactions Incompatible with Customer's Financial Standing

(i) A customer who suddenly starts remitting funds in large amounts when it is known to the Reporting Institution that the customer does not have the capacity to do so.

(ii) Transactions that cannot be matched with the investment and income levels of the customer.

(iii) Source of the funds is unclear or not consistent with the customer's apparent standing.

(d) Suspicious Behaviour/Demeanour

(i) A customer for whom verification of identity proves unusually difficult and who is reluctant to provide details.

(ii) A group of unconnected customers who share a common correspondence address.

(iii) A client who shows unusual concern for secrecy e.g. in identifying beneficial owner of the account, his employment/business or assets or fails to indicate a legitimate source of funds.

(iv) The excessive or unnecessary use of nominees.

(v) The unnecessary granting of wide ranging Powers of Attorney

(vi) An unwillingness to disclose the sources of funds

(e) Dealing with High-Risk Jurisdictions

(vii) Sending and/ or receiving international remittances from/to countries where production of drugs or drug trafficking may be prevalent.

(viii) Funds credited into customer remittance accounts from and to countries associated with the production, processing or marketing of narcotics or other illegal drugs; or other criminal conduct; or transfer to or from a banking secrecy-haven country or country generally known for money laundering and terrorist financing.

(ix) The sending or receipt of frequent or large volumes of transfers to and from offshore humanitarian institutions.

(x) Customers transferring large sums of money to or from overseas with specific requests for payment in cash.

(xi) International transfers for accounts with no history of such transfers or where the stated business of the customer does not warrant such activity.

(f) Suspicious Behaviour/Demeanour by an Employees of the Reporting Institution

(i) There may be circumstances where the money laundering may involve employees of Reporting Institution. Hence, if there is a change in the employees' characteristics e.g. lavish lifestyles, unexpected increase in performance, etc. the Reporting Institution may want to monitor such situations.

Annexure D: Risk Assessments and Regulatory Risk Synopsis

- ✓ ADLAs are required to take appropriate steps to identify, assess and understand their ML/TF risks in relation to their business and regulatory risks.
- ✓ Business risk include the assessment of customers, countries or geographical areas and products, services, transactions or delivery channels.
- ✓ In addition to assessing business risks highlighted above ADLAs are required to assess their regulatory risks. Regulatory risk is associated with failure to meet the requirements of the MLPC Act and AML/CFT/CPF regulations (including all amendments) and instructions issued by the FIU and Financial Surveillance Division. Examples of these risks are:-

  (i) lack of Board oversight;

  (ii) customer/beneficial owner identification and verification not done properly;

  (iii) Inadequate policies and procedures;

  (iv) Inadequate internal controls;

  (v) failure to keep record properly;

  (vi) failure to vet staffs on recruitment;

  (vii) failure to train staff adequately;

  (viii) not having an AML/CFT/CPF program;

  (ix) failure to implement Sanction lists requirements;

  (x) failure to report suspicious transactions;

  (xi) not submitting required reports (CTRs) to FIU regularly;

  (xii) not having an AML/CFT/CPF Compliance Officer/function;

  (xiii) failure of doing Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs,)

  (xiv) not complying with any order for freezing or suspension of transaction issued by FIU;

  (xv) not submitting accurate information or statement requested by Financial Surveillance Division and

  (xvi) lack of independent testing of the AML/CFT/CPF program.

Annexure E: ADLAs Compliance Rating System

- ✓ In determining AML/CFT/CPF compliance rating on the part of ADLAs, Financial Surveillance Division will use the risk-based approach.
- ✓ The AML/CFT/CPF rating shall be established through a weighted assessment of the technical compliance (20%) and effectiveness (80%) of the institution.
- ✓ Prior to going onsite, inspectors will engage in a desk reviews where AML/CFT/CPF policies and procedures, as well as the Institutional Risk Assessment will be assessed for technical compliance. Technical compliance in this context refers to adequacy of such documentation in line with MLPC Act, relevant Guidance Manual and directives issued by the FIU and Financial Surveillance Division, as well as available guidance on AML/CFT/CPF best practices.
- ✓ The onsite reviews will be key to determining each institution's level of effectiveness, being the extent to which AML/CFT/CPF policies and procedures and the institutional risk assessment are being implemented to produce expected results.
- ✓ A weighted risk-rating tool will be used to assess technical compliance and effectiveness of the ADLAs implementing AML/CFT/CPF requirements**.**
- ✓ The technical compliance or effectiveness score would fall in one of the ''control strength range" levels given in Table 1 below, and be allocated the corresponding rating.

Table 1: Technical compliance and effectiveness rating key

CONTROL STRENGTH RANGE	TECHNICAL COMPLIANCE RATING	EFFECTIVENESS RATING
0.8-1	Compliant (Very minor shortcomings)	High (Expected results achieved to a very large extent. Minor improvements needed)
0.5-<0.8	Largely compliant (minor shortcomings)	Substantial (Expected results achieved to a large extent. Moderate improvements needed)
0.2-<0.5	Partially compliant (moderate shortcomings)	Moderate (Expected results achieved to some extent. Major improvements needed)
0-<0.2	Non- compliant (major shortcomings)	Low (Expected results not achieved or achieved to a negligible extent. Fundamental improvements needed)

- ✓ Technical compliance will be rated using a score range of 0 to 1, with 0 representing non-compliance and 1 representing compliance.
- ✓ A rating of ‘’compliant” means that for example the AML/CFT/CPF policy contains all the key AML/CFT/CPF elements required.
- ✓ Effectiveness will be rated using score range of 0 to 1, with a score close to 0 representing low level of effectiveness and a score close to 1 representing high level of effectiveness.
- ✓ A rating of ‘’High” effectiveness means that the AML/CFT/CPF control measure is achieving the expected results, for example, identifying suspicious transactions. Minor improvements can be undertaken to further enhance effectiveness.
- ✓ Each institution’s overall rating will be obtained by adding up all the weighted AML/CFT/CPF compliance or effectiveness levels.
- ✓ Each MVT/ADLAs AML/CFT/CPF rating (being the weighted technical compliance rating + effectiveness rating) will fall into one of four levels, each having a corresponding ML/TF risk vulnerability as tabulated below:

Table 2: Overall compliance and ML/TF vulnerability key

Risk Score Range	Rating	Level of ML/TF Vulnerability
< 45%	Non-Compliant	Very High
45%< 65%	Partially Compliant	High
65%< 85%	Largely Compliant	Moderate
85%< 100%	Compliant	Low

- ✓ On a risk sensitive basis, Financial Surveillance Division will select a sample of branches to visit, the area to focus on during the inspections and personnel to interview to assess the level of awareness and knowledge of AML/CFT/CPF Obligations.

REFERENCES

1. FATF (2012-2023), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, **www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatfrecommendations.html.**

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

3. The Money Laundering and Proceeds of Crime Act [Chapter 9: 24] (MLPC Act) **https://www.fiu.co.zw/amlcft-framework.**

4. Statutory Instrument 76 of 2014, requiring financing institutions, DNFBPs and other persons, to identify, freeze and report funds or other assets of individuals and entities identified by or under the authority of the United Nations Security Council for financing or supporting international terrorism.

5. Statutory Instrument 164 of 2023, requiring financial institutions, DNFBPs and other persons to identify, freeze and report funds or other assets of individuals and entities identified by or under the authority of the United Nations Security Council for financing or promoting proliferation of weapons of mass destruction.

6. Risk-Based Guidance Manual on Anti-Money Laundering and Combating Financing of Terrorism, of January 2021, issued by Financial Intelligence Unit to Financial Institution and Designated-Non-Financial Businesses and Professions.

Headquarters:
80 Samora Machel Avenue, Box 1283, Harare, Zimbabwe.
Tel: +2638677000477, +263242703000
Regional Branch:
93 Leopold Takawira Avenue, Box 399 Bulawayo, Zimbabwe.
Tel: +2638677002046, +26329272141-5

communications@rbz.co.zw
www.rbz.co.zw
@ReserveBankZim
@ReserveBankZim