BANK SUPERVISION, SURVEILLANCE & FINANCIAL STABILITY DIVISION

AML/CFT/CPF Guideline No. 01/2025/BSSFS

Guidance to Reporting Institutions on AML/CFT/CPF Obligations

Document No.	01-2025/BSSFS
Version	1
Issue Date	May 2025

Table of Contents

ACRONYMS

AML - Anti-money laundering

BSS&FS - Banking Supervision, Surveillance & Financial Stability Division

CDD - Customer Due Diligence

CFT – Countering Financing of Terrorism

CPF – Countering Proliferation Financing

CSA - Competent Supervisory Authority

EDD - Enhanced Due Diligence

EXCO – Executive Committee

FATF - Financial Action Task Force

FIU - Financial Intelligence Unit

IRA - Institutional Risk Assessment

KYC - Know Your Customer

ML - Money Laundering

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

NRA - National Risk Assessment

PEP - Politically Exposed Person

PF - Proliferation Financing

RBA - Risk Based Approach

RBZ - Reserve Bank of Zimbabwe

STR - Suspicious Transaction Report

TF - Terrorist Financing

TFS - Targeted Financial Sanctions

UNSCR - United Nations Security Council Resolution

WMD – Weapons of Mass Destruction

DEFINITIONS

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***] (hereafter referred to as the MLPC Act). In the event of conflict between a definition in this guideline and that in the Act, the latter prevails.

TERM	DEFINITION
Beneficial Owner	In the context of legal persons, *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 natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owners of a given legal person. In the context of legal arrangements, beneficial owner includes: (i) the settlor(s); (ii) the trustee(s); (iii) the protector(s) (if any); (iv) each beneficiary, or where applicable, the class of beneficiaries and objects of a power; and (v) any other natural person(s) exercising ultimate effective control over the arrangement. In the case of a legal arrangement similar to an Express Trust, beneficial owner refers to the natural person(s) holding an equivalent position to those referred above. When the trustee and any other party to the legal arrangement is a legal person, the beneficial owner of that legal person should be identified.
Cross Border Wire Transfer	Refers to any wire transfer where the ordering reporting institution and beneficiary reporting institution are in different countries.

TERM	DEFINITION
Domestic Wire Transfer	Refers to any wire transfer where the ordering reporting institution and beneficiary reporting institution are located in the same country.
Express Trust	Refers to a Trust clearly created by the settlor, usually in the form of a document for example a written deed of trust.
Financial Intelligence Unit (FIU)	Refers to the Financial Intelligence Unit, established under section 6A of the Money Laundering and Proceeds of Crime Act [*Chapter 9:24*].
High Risk Countries	Refers to countries with significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence (EDD), and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from these countries. These countries are often externally referred to as grey list and "black list" respectively.
Legal Arrangements	Refers to express trusts, a partnership of persons, or any person holding assets in a fiduciary capacity and any such arrangements.
Legal Persons	Any entity, other than natural person(s), that can establish a permanent customer relationship with a reporting institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations and other similar entities.

TERM	DEFINITION
Money Laundering	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.
Politically Exposed Persons (PEPs)	Domestic PEPs – (a) 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, directors, deputy directors and members of the Board or equivalent functions, senior executives of state-owned corporations and senior political party officials; Foreign PEPs – (b) 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 (senior management) of an international organisation. For example, directors, deputy directors and members of the Board or equivalent functions. (d) Immediate family members (such as parents, children, siblings or spouses) or associates of persons referred to in (a) to (c) above.
Proliferation Financing of weapons of mass destruction	The act of providing funds or financial services which are used, in whole or in part, 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

TERM	DEFINITION
	goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
Reporting Institution	A bank licenced and required to be registered under the Banking Act [*Chapter 24:20*], the Building Societies Act [*Chapter24:02*], development banks and microfinance institutions (Deposit-taking and Credit only) that are licensed or registered and supervised by the Reserve Bank of Zimbabwe as provided for by the Microfinance Act [*Chapter 24.30*].
Terrorist financing	Directly or indirectly, providing or collecting funds, or attempting to do so, with the intention that they should be used or in the knowledge that they are to be used in whole or in part in carrying out a terrorist act, or by a terrorist, or in part by a terrorist organisation.

LEGAL AUTHORITY AND APPLICATION

This guideline is issued in line with section 3(3) of the Money Laundering and Proceeds of Crime (MLPC) Act [Chapter 9:24], which gives the Reserve Bank of Zimbabwe, the mandate to supervise reporting institutions' compliance with the applicable requirements of the MLPC Act. It is also issued in line with section 6(1)(c) of the Reserve Bank of Zimbabwe Act [*Chapter 22:15*], which gives the Reserve Bank of Zimbabwe (Reserve Bank) the mandate to foster the stability and proper functioning of Zimbabwe's financial system.

The guidance applies to all banking institutions licensed by the Reserve Bank under the Banking Act [*Chapter 24:20*] and the Building Societies Act [*Chapter 24:02*], and microfinance institutions licensed under the Microfinance Act [*Chapter 24:30*] and all other institutions under the supervisory purview of the Reserve Bank.

Reporting institutions should employ the guidance in crafting their methodologies, incorporating principles explained to ensure adequate identification and assessment of the risk of money laundering, terrorist financing and proliferation financing, and put in place effective and proportionate mitigating measures based on that assessment.

For the avoidance of doubt, where the word "shall", "must" or "should", or other word having similar meaning, is used in the guidance with respect to an action, provision, consideration or measure, it is a mandatory requirement and reporting institutions are required to comply or implement the said action, provision, consideration or measure.

The Reserve Bank of Zimbabwe will monitor adherence to the guideline and failure to comply with its provisions will result in appropriate supervisory action taken against the institution.

In the event of any conflict between this guidance and any provision of law, the latter shall take precedence.

1. INTRODUCTION

1.1 Banks and microfinance institutions (reporting institutions) contribute to economic growth and development through their financial intermediation role. The banking sector is characterised by a large customer base, large volumes and values of transactions ranging from simple to complex transactions, large asset base as well as many products and services. These inherent characteristics open the financial sector to heightened money laundering, terrorist financing and proliferation financing risks.

1.2 Against this background, robust AML/CFT/CPF frameworks are pivotal in fostering financial stability, integrity, and ultimately economic growth.

1.3 To facilitate a consistent approach to implementation of AML/CFT/CPF obligations and the adoption of regional and international standards by reporting institutions, the Reserve Bank has prepared this set of guidelines to provide minimum requirements for an effective AML/CFT/CPF compliance programme.

1.4 The Reserve Bank is committed to promoting strong AML/CFT/CPF supervisory frameworks, through refining its supervisory processes & procedures and embracing the provisions of the Money Laundering and Proceeds of Crime Act [Chapter9:24] (MLPC Act) as aligned with Financial Action Task Force (FATF) Recommendations and other regional and international AML/CFT/CPF best practices.

1.5 Zimbabwe has a robust AML/CFT/CPF legal framework in place which is aligned to the FATF Recommendations and Standards to counter money laundering, terrorism financing and proliferation financing risks. The principal legislation is the Money Laundering and Proceeds of Crime Act [*Chapter 9:24*].

1.6 Effective 1 January 2023, the Financial Intelligence Unit appointed the Reserve Bank of Zimbabwe's Bank Supervision, Surveillance and Financial Stability Division (BSS&FS) as an AML/CFT/CPF Competent Supervisory Authority (CSA) to oversee the supervision of banks and microfinance institutions.

1.7 This guidance must, thus, be read together with The Money Laundering and Proceeds of Crime Act (https://www.fiu.co.zw/amlcft-framework) which sets out in detail the AML/CFT/CPF statutory obligations of reporting institutions in relation to:

(a) Risk based AML/CFT supervision;

(b) All current directives or circulars issued under Statutory Instruments 76 of 2014 and Statutory Instrument 110 of 2021 on the implementation of targeted financial sanctions to combat financing of terrorism and financing of proliferation of weapons of mass destruction, respectively;

(c) The Suppression of Foreign and International Terrorism Act [Chapter 11.21] (Application of UNSCR 1267 of 1999, UNSCR 1373 of 2001 and Successor UNSCRs) Regulations, 2014, Statutory Instrument 76 of 2014;

(d) The 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 and 1696, 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, 2021, Statutory Instrument 110 of 2021; and

(e) FATF guidelines on Targeted Financial Sanctions which are issued from time to time.

1.8 The relevant information and full listings of persons designated by UNSC is found on the UN website. https://www.un.org/securitycouncil/sanctions/information

1.9 A key aspect of section 12B of the MLPC Act is the application of a risk-based approach under which reporting institutions are expected to identify, assess and understand, their ML/TF/PF risks, take appropriate actions to mitigate those risks and allocate their resources efficiently by focusing on high risk areas.

2. RISK BASED APPROACH

Risk Identification, Assessment, Mitigation and Monitoring: The Process

2.1 Reporting institutions are required, in terms of section 12B of the MPLC Act, to apply a risk-based approach (RBA) to the implementation of the AML/CFT/CPF programmes.

2.2 A risk-based approach is a flexible set of measures that allows reporting institutions to conduct an institutional risk assessment which entails identification, assessment & understanding the ML/TF/PF risks to which they are exposed to and apply preventive measures that are proportionate to the nature of the risks i.e. enhanced measures should be applied to areas identified as high risk and simplified / reduced measures to lower risk areas in order to manage & mitigate them in an effective manner. It also allows the reporting institutions to target/ allocate their resources more effectively.

2.3 The expectation is that a reporting institution should undertake a ML/TF/PF institutional risk assessment (IRA) in the context of its enterprise-wide risk framework encompassing identification of the general & specific ML/TF/PF risks to which it is exposed and designing proportionate AML/CFT/CPF programs to mitigate the risks.

2.4 An effective enterprise-wide risk assessment can help reporting institutions identify gaps and opportunities for improvement in their internal AML/CFT/CPF policies, procedures, and controls, as well as make informed management decisions about risk appetite, AML/CFT/CPF resource allocation, and ML/TF/PF risk-mitigation strategies that are appropriately aligned with residual risks.

2.5 Reporting institutions have the latitude to select and develop their own methodologies for assessing ML/TF/PF risks provided that they incorporate the principles explained in this guidance and put in place effective mitigating measures based on the assessment.

2.6 The use of different methodologies emanates from the fact that, reporting institutions are heterogeneous in terms of business models, the services they provide, the types of customers they serve, the delivery channels they use, and the geographies in which they operate, as well as their varying sizes and levels of business complexities.

2.7 Reporting institutions should decide on the methodology of enterprise-wide ML/TF/PF risk assessments, including baseline and follow-up assessments, based on their specific circumstances, taking into account the nature of the inherent and residual ML/TF/PF risks to which they are exposed, as well as the latest National Risk Assessment (NRA) results.

2.8 Reporting institutions should conduct such risk assessments at least once a year. Further, reporting institutions are required to establish documented rules and procedures for the periodic review of their enterprise-wide risk assessment approach which should be approved by the Board.

2.9 The Risk Based Approach implementation process consists of four (4) key steps as follows:

Diagram 1: Risk-based Approach

Step 1: Risk Identification

2.10 The initial stage in the risk-based approach is risk identification. Reporting institutions should establish a process that identifies the nature and types of ML/TF/PF risks i. e. potential threats, vulnerabilities and consequences of the identified risks before any controls are applied. Effective ML/TF/PF risk identification and assessment processes are vital for reporting institution to understand their risk profiles and effectively focus risk management resources.

Step 2: Risk Measurement (Assessment)

2.11 Risk measurement is the process of quantifying the level of ML/TF/PF risk associated with an activity, business relationship, customer or products and jurisdictions which a reporting institution is exposed to. It involves measuring the magnitude of the risk for each of the risk types identified under Step 1, above.

2.12 In relation to each risk type, the reporting institution must design a risk rating scale which is informed by its size and complexity of business operations. Reporting institutions should also take into account the peculiarities, the risk degree or suspiciousness of a transaction or business relationship.

2.13 The different variables which can impact the potential risk posed by certain clients such as nature, scale, diversity and complexity of customer's business, target markets, internal audit and regulatory findings should all be considered in this risk measurement process.

2.14 Further, reporting institutions should develop and employ qualitative and quantitative risk scoring and rating methodologies. This entails assigning risk ratings to customers, delivery channels, geography and products based on defined criteria.

2.15 To ensure effective risk measurement and management, reporting entities are required to adopt a risk rating tool tailored to their operational needs. The risk rating tool should include weighting of the identified risk elements relative to their importance to the institution.

2.16 Reporting institutions should at all times maintain detailed records of such risk assessments and methodologies used.

Customer Risk

2.17 Customer risk assessment considers the likelihood that a particular customer or type of customer segment will make use of the reporting institution to launder/finance/support terrorism and proliferation financing using proceeds of crime/ illicit funds and/or legitimate funds, respectively. The reporting institution should exhibit understanding of customers' activities, transaction patterns, business operations, and other relevant factors. Further, the reporting institution should consider the size of a customer's asset base, capital outlay or the volume and size of transactions undertaken by a customer in respect of legal persons.

2.18 The basis for such risk assessment should be documented, as well as the criteria for customer classification and the assignment of a risk rating to each customer segment.

2.19 Reporting institutions should take into account the type of customer segments categorised as high risk by the latest AML/CFT/CPF National Risk Assessment when conducting customer risk assessment.

2.20 Reporting institutions are prohibited from offering financial services to individuals and entities on the UN-designated sanctions list and to individuals and entities owned or controlled directly or indirectly by these individuals and entities.

2.21 Reporting institutions should identify and verify the identities of all beneficial owners with 10% ownership and above and conduct enhanced due diligence to those classified as high risk.

2.22 Proliferation and terrorism networks often rely on shell and front companies to disguise end-users and payments, hence these companies should be regarded as high-risk due to their potential roles in TF and PF typologies.

2.23 Reporting institutions should consider applying enhanced measures for individual transactions of high-risk companies, such as requesting the customer to provide a valid export license or a reference to the export control requirements in the relevant jurisdiction showing that the exported goods are for legitimate use.

2.24 Special attention should be given to foreign PEPs, and high-risk non-governmental organisations when conducting customer risk assessment.

2.25 In relation to domestic PEPs or persons who have been entrusted with a prominent function by an international organisation, in addition to performing the CDD measures required, reporting institutions are required to:

(a) take reasonable measures to determine whether a customer or the beneficial owner is such a person; and

(b) in cases when there is higher risk business relationship with such a person, apply the measures under section 20(1) of the MLPC Act.

Products/Services Risk

2.26 This risk factor evaluates the institution's services or products and determines the likelihood that a particular product will be abused to launder criminal proceeds, finance terrorism and proliferation financing.

2.27 Reporting institutions should be aware of, and be capable of identifying, products and services that may pose higher ML/TF/PF risks. Legitimate products and services can be used to conceal the illicit origins of funds, move funds to finance terrorist attacks, or conceal the true identity of the product, service, or transaction's owner or beneficiary.

2.28 Products and services that facilitate the transfer and conversion of assets into, through, and out of the financial system may pose high ML/TF/PF risk. Further, products and services identified as potentially high risk for money laundering or terrorist financing in the latest National Risk Assessment, by other competent supervisory authorities, or other reputable sources should be assessed.

2.29 Various activities carried out by reporting institutions pose varied risks depending on their features. Some examples of ML/TF/PF vulnerabilities related with various reporting institutions activities include:

a) Retail banking including the supply of services to cash-intensive enterprises, the volume of transactions, high-value transactions, and the diversity of services.

b) Wealth management: a culture of secrecy, difficulty in identifying beneficial owners, concealment (use of offshore trusts), banking secrecy, the complexity of financial services and products, high-value transactions, and cross-border transactions.

c) Layering and integration in investment banking, entailing the transfer of assets between parties in exchange for cash or other assets, heightens ML/TF/PF risk. For purposes of TF/PF, reporting institutions should focus on cross-border wire transfers as these pose heightened TF/PF risk to reporting institutions. The reporting institutions should comply with the obligations under section 27 of the MLPC Act to effectively mitigate the risk associated with cross border wire transfers.

d) Reporting institutions offering correspondent banking services should comply with customer identification and account opening requirements under section 21 of the MLPC Act.

e) Trade finance transactions pose high risk of money laundering, terrorist and proliferation financing. Transactions in controlled goods and technology have been noted to heighten TF/PF risk as these transactions can allow individuals and entities to hide their intentions or underlying illicit activities.

Geography/Country Risk

2.30 Geography and country risks refers to the ML/TF/PF risks related with the reporting institution's country or geographic location, as well as the ML/TF/PF risks associated with a customer or a transaction. Reporting institutions must examine if the geographic areas in which they operate or conduct activities provide an increased risk of money laundering and terrorism funding. In this regard, reporting institutions should always consider the types and levels of ML/TF/PF risks to which the country is exposed and which may have an influence on the institution's level of ML/TF/PF risks.

2.31 Further, reporting institutions should be guided by the jurisdiction’s latest ML/TF/PF risk assessment, as well as the reporting institution’s own assessment of the national ML/TF/PF risks.

2.32 Similarly, when dealing with customers or transactions associated with a foreign country, the reporting institution should pay regard to the ML/TF/PF 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 Financial Action Task Force (FATF) as not sufficiently implementing AML/CFT/CPF requirements.

2.33 Countries that are known or strongly suspected to be developing weapons of mass destruction and have recorded many cases of terrorism present high jurisdiction risk to reporting institutions.

2.34 TF and PF risks are not solely tied to countries listed by FATF, but also those countries involved in terrorist financing and proliferation financing rely on transanational connections to procure and use illicit goods and services. These include countries which are insufficiently compliant with AML/CFT/CPF standards as well as those with weak export control laws. Such countries may allow shipment of sensitive or dual-use goods through their boarders to highly exposed countries.

2.35 Reporting institutions are therefore required to conduct enhanced due diligence, proportionate to the identified risk towards business relationships and transactions with any natural or legal person from countries identified as high-risk jurisdictions.

Higher Risk Countries

2.36 Section 26A of the MLPC Act requires reporting institutions to conduct enhanced due diligence, commensurate with the risk towards business relationships and transactions with any natural or legal person from countries identified as insufficiently compliant in implementing AML/CFT/CPF FATF standards.

2.37 High-risk countries include non-compliant countries identified and listed by the FATF or identified by the FIU.

2.38 Reporting institutions should make use of the list issued by the FIU which is updated from time to time.

2.39 The list may include non-compliant countries identified and listed by the FATF or identified by the FIU.

2.40 With respect to some of the countries on the FATF "black-list", reporting institutions may be required to take specified countermeasures as set out in the FIU directive(s). For transactions

involving other non-compliant [1]countries where no FATF countermeasures are specified, reporting institutions are required to implement EDD, having regard to the nature of the AML/CFT/CPF shortcomings and risks of each specified country.

Delivery Channel Risk

2.41 Reporting institutions should assess the channels through which their products or services are delivered. Due to technological developments many delivery channels in the digital space do not require customers to be in direct face-to-face contact with the reporting institution (for example, Internet, telephone, or mail), and are accessible 24 hours a day, seven days a week, from practically anywhere in the world. Some of these delivery channels' remoteness can be utilized to conceal the actual identity of a customer or beneficial owner thereby posing higher ML/TF/PF risks.

2.42 Delivery channel risk is closely associated with, and can be assessed as part of products /services risks. The assessment of delivery channel risk often looks at whether a service or product is offered face-to-face to a customer, i.e. where the business or institution directly interacts with the customer, or whether it is delivered through a non-face-to-face medium, such as the internet or through agents. Such types of non-face-to-face methods of delivering services present higher ML/TF/PF risks.

2.43 Reporting institutions should consider the channels used to onboard new customers as well as how customers access the products and services. Attention should be paid to channels that are not normally used by customers or are not in line with normal behavioural patterns of a customer.

Step 3: Risk Mitigation

2.44 Risk mitigation entails putting in place procedures to restrict potential money laundering and terrorist financing threats identified by the reporting institution. Following identification and

[1] Non-compliant Countries: Financial Action Task Force (FATF) identifies non-compliant countries in two main categories: the **"black list"** (officially known as High-Risk Jurisdictions subject to a Call for Action) and the **"grey list"** (Jurisdictions under Increased Monitoring)

assessment of inherent risks, the reporting institution should put in place adequate controls and procedures to minimize the identified risks.

2.45 The reporting institution should develop and implement policies and procedures designed to mitigate risks as part of its internal control environment. For higher-risk customers and scenarios, enhanced controls and procedures are required, whilst simplified / reduced measures may be used in lower risk situations.

Step 4: Monitoring of Risks and Review

2.46 On-going risk monitoring is an integral continuous process rather than a one-time event. As a result, reporting institutions should ensure that the risk profiles are kept up to date, taking cognisant of changes in the operating environment and emerging risks. In addition, reporting institutions should adopt on-going monitoring measures commensurate with the ML/TF/PF risks associated with their customers, products/services/ transactions, delivery channels and geographic area.

2.47 Section 26 of MPLC Act requires reporting institutions to conduct on-going 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;

(b) closely examining the transactions carried out in order to ensure that such transactions are consistent with their knowledge of the customer, and the customer's commercial or personal activities and risk profile; and

(c) ensuring that the obligations pursuant to sections 19, 20 and 21 of the MLPC ACT relating to high-risk customers, politically exposed persons, and correspondent banking relationships, respectively, are fulfilled.

2.48 Reporting institutions are required to:

(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;

(b) pay special attention to business relations and transactions with persons, including legal persons and arrangements, from non-compliant or insufficiently compliant jurisdictions;

(c) examine as far as possible the background and purpose of transactions under paragraphs (*a*) and (*b*) and set forth in writing their findings;

(d) take such specific measures as may be prescribed by the relevant directives from time to time to counter the risks with respect to business relations and transactions specified under paragraph (*b*); and

(e) develop and document risk mitigation measures and mitigation strategies. The risk mitigation methods should be clearly communicated to management and all staff.

2.49 As reporting institutions are required to maintain a risk rating framework and conduct continuous risk assessment of their customers to establish and update their risk profiles, the principle of proportionality to the risk assessment output of the customers/ product/ services/ transactions/ geographic area/ delivery channels will yield varying levels of ongoing monitoring requirements.

2.50 Once a business relationship has been risk rated, on-going monitoring measures that are commensurate with the level of risk associated with the relationship must be applied. Business relationships identified as posing a low risk would require simplified monitoring whereas those in the high-risk category would require enhanced due diligence measures.

2.51 Reporting institutions are expected to develop clear policies and procedures, especially on the frequency of periodic review or what constitutes a trigger event, to ensure continuous monitoring of their business relationships.

3. AML/CFT/CPF COMPLIANCE PROGRAMME

3.1 Section 25 of the MLPC Act requires every reporting institution to have an AML/CFT/CPF compliance programme in place, which must be evaluated and reviewed on a regular basis to adapt to developing ML/TF/PF risks. Further, Section 25(1) of the MLPC Act sets out and imposes a set of measures that are recognized as the five (5) pillars of an AML/CFT/CPF Compliance Programmes.

3.2 In this regard, reporting institutions are required to develop and implement effective compliance programmes taking into account the money laundering, terrorist financing and proliferation financing risks and size of the reporting institution, which programmes should include the following:

a. Board approved internal policies, procedures and controls to fulfil obligations pursuant to the MLPC Act;
b. maintain a robust internal control environment;
c. appointment of a money laundering reporting officer;
d. adequate screening procedures to ensure high standards when hiring employees;
e. on-going training for officers, employees and board members to make them aware of the MLPC Act obligations;
f. policies and procedures to prevent the misuse of technological developments including those related to electronic means of storing and transferring funds or value; and
g. independent audit arrangements to review and verify compliance with and effectiveness of the measures taken in accordance with the MLPC Act.

Internal Control Environment

3.3 Internal controls are a key component of a reporting institution's AML/CFT/CPF risk management framework. Internal controls consist of policies, procedures and governance structures to mitigate risk; and are characterised by preventive, detective and corrective measures.

3.4 Reporting institutions, through their board and senior management should have policies, processes, governance and procedures, in place to promote high ethical and professional

standards and prevent their institutions from being used, purposefully or unwittingly, by criminal elements. Reporting institutions must therefore establish clear responsibilities to ensure that policies, procedures, and internal controls are implemented and maintained ensuring that they comply with their legal obligations.

3.5 The board and senior management should establish a culture of compliance and ethical standards.

Policies and Procedures

3.6 Reporting institutions should have board approved policies and procedures that are consistent with the nature, complexity and scale of the institution's activities. The reporting institution should have a clear delineation of roles, responsibilities and accountability for the implementation of consistent policies across the institution.

3.7 Reporting institutions should establish appropriate procedures and processes to implement its policies, and these should be documented in procedure manuals. The procedures should detail the processes to guide staff on the implementation of the various key AML/CFT/CPF obligations set out in the MLPC Act. The manuals should be periodically reviewed at least annually to ensure that they reflect current developments. Deviations from such policies and procedures should be independently investigated, reported and addressed by the relevant parties.

3.8 At a minimum, the procedures should cover the following:

i. risk assessment;
ii. customer on-boarding procedures; customer due diligence, including customer identification, verification and on-going monitoring;
iii. enhanced customer due diligence and transaction monitoring for high-risk customers, including Politically Exposed Persons;
iv. detection and reporting of suspicious transactions; and
v. record keeping.

Policies and Procedures to prevent the Misuse of Technological Developments

3.9 Pursuant to section 12B (4) of the MLPC Act, every reporting institution shall assess and document the ML/TF/PF risk posed by such product, service, business practice or technology, and put in place adequate measures to mitigate the risk before launching any new product, service or business practice, and before the use of any new technological innovation, for both new and existing products.

3.10 Reporting institutions are required to undertake the risk assessments prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate the risks.

3.11 Pursuant to section 25(1) (d) of the MLPC Act reporting institutions should develop and implement programmes for the prevention of money laundering and financing of terrorism taking into account, the ML/TF/PF risks and size of the business, which programmes shall include policies and procedures to prevent the misuse of technological developments including those related to electronic means of storing and transferring funds or value.

Board and Senor Management Oversight

3.12 An effective risk-based approach to AML/CFT/CPF implementation requires board of directors and senior management that are committed to lead and oversee its development and implementation.

3.13 The ultimate responsibility and accountability of ensuring compliance with AML/CFT/CPF laws, regulations, guidelines, and directives rests with the reporting institution’s board of directors and senior management.

3.14 The board and senior management of reporting institutions should have a clear understanding of the ML/TF/PF risks to which the reporting institution is exposed, as well as how the reporting institution's AML/CFT/CPF control structure operates to mitigate such risks.

3.15 The board and senior management of reporting institutions should ensure effective implementation of rules, procedures, systems and processes that minimise ML/TF/PF risks. The AML/CFT/CPF programme of reporting institutions should be risk-based and proportionate to the nature, size, complexity and level of inherent risks.

3.16 Board and senior management should ensure that explicit responsibility is assigned within the reporting institution to enable effective management of processes and procedures. The board and senior management should establish a defined risk appetite and foster a compliance culture that prohibits criminals from abusing the reporting institution.

3.17 The board should ensure the establishment of appropriate mechanisms for the periodic review of the AML/CFT/CPF policies and procedures to ensure their continued relevance in line with changes in the reporting institution's products and services, and to address new and emerging ML/TF/PF risks.

3.18 Further, the board should ensure that information on ML/TF/PF risk assessment is delivered to the board in a timely, complete, clear, and accurate manner to enable making informed decisions. The following issues should at a minimum be included in the reports escalated to the board:

a) internal/external audit reports and supervisory reports on AML/CFT/CPF findings and remedial action plans, if any, to address the results of compliance testing and self-identified instances of non-compliance with AML/CFT/CPF requirements;
b) compliance reports and Executive Committee (EXCO) deliberations;
c) recent developments in AML/CFT/CPF rules and regulations, including any implications for the reporting institution;
d) Details of recent important risk incidents, including any consequences for the reporting institution;
e) statistics, including statutory reporting to the FIU and BSSFS, law enforcement agencies, orders, regulatory sanctions, denied or declined business, and de-risked relationships;
f) staff training completion rate; and
g) KYC compliance level.

3.19 Senior management is responsible for implementing, monitoring, and managing the reporting institution's AML/CFT/CPF programme, as well as ensuring compliance with established AML/CFT/CPF policies and procedures. senior management should, among other things, ensure that the policies and procedures are risk-based, proportional, and adequate to mitigate the reporting institution's ML/TF/PF risks.

3.20 In addition, senior management should:

a) ensure that the reporting institutions comply with the MLPC Act, all relevant AML/CFT/CPF laws, regulations, and this guidance; and that they are effectively implemented across relevant business lines; and

b) conduct a periodic review of the policies and procedures as appropriate or whenever regulation requires change, to ensure their continued relevance in light of internal and external developments such as changes in business model, new products/services, new and developing technologies, and regulatory and legislative changes.

3.21 It is senior management's responsibility to ensure that:

i) sufficient, regular and objective information and reports are in place to assess the ML/TF/PF risk to which the reporting institution is exposed through its activities and business relationships and the effectiveness of the AML/CFT/CPF controls;

ii) remedial actions are taken on a timely basis in response to recommendations made by internal and external auditors and regulators in respect of the AML/CFT/CPF programme;

iii) relevant, adequate and timely information regarding AML/CFT/CPF matters is provided to the board;

iv) training is provided to all relevant categories of staff, including compliance officers, on an on-going basis to enable them to effectively discharge their AML/CFT/CPF responsibilities; and

v) compliance and internal audit functions are provided with sufficient resources, including adequate staff and information technology resources, to execute their responsibilities effectively.

Compliance Function

3.22 In terms of section 25(2-6) of the MLPC Act, reporting institutions should designate a compliance officer at management level to be responsible for the implementation of the compliance programme, and on-going compliance with, the MLPC Act. Such compliance officer

shall have ready access to all books, records and employees of the institution concerned as is necessary to fulfil his or her responsibilities.

3.23 The compliance officer can be the Head of Compliance, cognisant of the institution's size and complexity of its activities.

3.24 The appointed compliance officer should ensure that the responsibilities of reporting institutions with respect to AML/CFT/CPF are being discharged as required under the MLPC Act and this guideline.

3.25 The appointment of a compliance officer should be in line with the requirements of the MLPC Act, regarding, amongst others, their fitness and probity.

3.26 The Compliance Officer should have the necessary authority within the reporting institution, such that, issues raised by him/her receive the necessary attention by the Board, Senior Management and business lines. He/she shall have a direct reporting line to the board and a relevant committee of the board.

3.27 The reporting institution should ensure that the Compliance Officer has sufficient resources, including adequate staff commensurate with the size and complexity of its business activities.

3.28 The responsibilities of the Compliance Officer should at a minimum include:

a) developing written AML/CFT/CPF policies and procedures that are approved by the board;
b) conducting or overseeing on-going monitoring of all AML/CFT/CPF obligations of the reporting institution. This includes sample testing of compliance and review of exception reports to alert senior management or the board of any non-adherence to AML/CFT/CPF procedures;
c) keeping the AML/CFT/CPF programme updated, relative to the reporting institution's identified inherent risks and giving consideration to local and international developments in ML/TF/PF;
d) conducting periodic reviews of AML/CFT/CPF control mechanisms to ensure their continued relevance and effectiveness in addressing changing ML/TF/PF risks;
e) conducting enterprise-wide risk assessments of ML/TF/PF risks including the timely assessments of new products and services as well as new technology and processes, as prescribed in this guidance;

f) ensuring transaction monitoring systems, including those required to identify and report suspicious transactions, are adequate, appropriate and effective in all relevant business areas of the institution;

g) ensuring that systems and other processes that generate information used in reports to senior management and the board are adequate & appropriate, use reasonably consistent reporting criteria, and generate accurate information;

h) promoting compliance with the MLPC Act, regulations and this guidance, and taking overall charge of all AML/CFT/CPF matters within the organisation;

i) informing staff promptly of regulatory and legislative changes and of revisions to policies and procedures;

j) ensuring a speedy and appropriate attention to any matter in which ML/TF/PF is suspected;

k) ensuring that on-going training and awareness programs on ML/TF/PF are current and relevant and are carried out for all employees, senior management and the board;

l) reporting to senior management on the outcome of reviews of the reporting institution's compliance with its AML/CFT/CPF obligations; and

m) reporting regularly on key AML/CFT/CPF risk management and control issues, and any necessary remedial actions, arising from audit, inspection, and compliance reviews, to the reporting institution's senior management and to the board.

3.29 The business interests of reporting institutions should not interfere with the effective discharge of the above-mentioned responsibilities of the compliance officer, and potential conflicts of interest should be avoided.

3.30 The compliance function should be distinct and autonomous from the internal audit and other assurance functions to enable unbiased judgments and facilitate impartial advice to management and the board.

3.31 Where any conflicts between business lines and the responsibilities of the compliance officer arise, procedures should be in place to ensure that AML/CFT/CPF concerns are objectively considered and addressed at the appropriate level of the reporting institution's management.

3.32 A reporting institution which is part of a financial group shall, in respect of its majority owned subsidiaries and branches, if any, whether local or foreign, implement group-wide programmes for combating money laundering and terrorist financing, as prescribed by the MLPC Act.

Customer Due Diligence

3.33 Customer Due Diligence (CDD) and Know Your Customer (KYC) consists of a number of distinct but connected elements, namely:

a) Identifying and verifying a customer's identity and residency or place of business;
b) Establishing the nature of business and source of funds/wealth of the customer;
c) Undertaking on-going due diligence and monitoring; and
d) Customer screening.

Customer Identification and Identity Verification

3.34 The starting point for customer due diligence is for the reporting institution to identify and verify the identity of a customer. Section 15(1) of the MLPC Act obligates reporting institutions to identify and verify the identity of their customers by means of an official identity document.

3.35 Identification of a customer and verification of the customer's identity are two separate but related requirements under this guideline as indicated below.

a) to identify a customer is to ascertain and record the name of the customer; and
b) to verify the identity is to confirm the customer's identity by obtaining the official identification document of the customer, i.e. national identity document, driver's license or valid passport, in the case of individuals, or certificate of incorporation or other document evidencing the creation and legal status of a legal person.

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

a) where a reporting institution intends to open an account for, or establish a business relationship with a customer; or

b) 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

c) 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

d) regardless of the amount involved, if doubt exists regarding the correctness of previously obtained customer identification information; or

e) regardless of the amount involved, where there is suspicion of money laundering or terrorist financing, in relation to the customer.

Requirement to Identify Ultimate Beneficial Owners of Legal Entities

3.37 Over and above the obligation to identify and verify the identity of a customer who is a legal person, reporting institutions are also required to identify and verify the identity of the ultimate beneficial owner of the entity as set out in section 15(3) of the MLPC Act. 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.

3.38 A beneficial owner is not necessarily the same person/entity listed as legal owner (shareholder) in official company documents. In the context of ML/TF/PF, 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.

3.39 To establish who the beneficial owner(s) is / are, the reporting institution is required to "pierce the veil" of the entity. This may involve "peeling off" various corporate layers in the shareholding structure, until the natural person(s) who controls the entity is/ are identified.

3.40 Where the corporate entity has a number of corporate shareholders, it may not be practical or beneficial to try and 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.

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

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

b) The information can be obtained from 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, founders / settlors and beneficiaries; and

c) Open information sources such as the internet concerning the entity, including the entity's own website, if any.

3.42 Where a reporting institution has failed to obtain sufficient & reliable information for purposes of identifying the beneficial owner(s) of a legal entity and does not have sufficient confidence as to who the customer is, it should not proceed with the business relationship in line with section 22 of the MLPC Act.

Timing of Customer Identification and Verification

3.43 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. 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.

3.44 According to section 16 of the MLPC Act, reporting institutions are 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 reporting institution adequately manages the ML/TF/PF risk through adoption of risk management procedures under which the customer may utilize the business relationship pending identity verification.

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

3.46 Possible risk management measures would be for a reporting 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.

3.47 The appropriate risk management conditions in each case should depend on the nature and level of ML/TF/PF risk.

Particulars of Customer Identification

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

3.49 The following customer identification particulars are required:

a) for a customer who is an individual, his or her full name, identification number 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 reporting institution to fulfil its obligations under the MLPC Act.

3.50 For higher risk customers and situations, in line with the risk-based approach, more information would need to be obtained. Similarly, for low-risk customers and financial products, the FIU is empowered to grant exemptions to dispense with some of the identification requirements.

3.51 Reporting institution should have clear written AML/CFT/CPF procedures, detailing how it implements the different levels of customer due diligence, in respect of the various risk categories.

3.52 The procedures should set out which customers are subject to simplified customer identification requirements and, the procedures should similarly set out enhanced identification requirements for the higher risk customers.

Reliance on Customer Identification by Third Parties/Intermediaries

3.53 The obligation in section 18 of the MLPC Act to comply with customer identification and verification requirements rests entirely with the reporting institution concerned.

3.54 It is permissible for a reporting institution 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/PF;

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 reporting 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.

3.55 The reporting institution that relies on a third party for customer identification is ultimately liable for any non-compliance with the MLPC Act's identity and verification requirements.

3.56 Where a reporting institution relies on agents to recruit / onboard customers, it is the reporting institution's responsibility to ensure that every such agent is adequately trained 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

3.57 Reporting Institutions during the identification and identity verification of non-face-to-face customers shall be guided by the requirements under Section 19 of the MLPC Act.

3.58 A reporting institution 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.

3.59 Such a situation presents a heightened ML/TF/PF risk and as such the reporting institution must take reasonable and adequate measures to satisfy itself that the customer is who they present themselves to be.

Enhanced Identification and Due Diligence Requirements for High-Risk Customers

3.60 Section 20(1)(a) of the MLPC Act requires reporting 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 on-going due diligence procedures with respect to such customers.

3.61 This provision should be read together with section 12B of the MLPC Act which requires reporting institutions to identify, assess and mitigate the ML/TF/PF risks to which their institutions are exposed.

3.62 The obligations in section 12B of the MLPC Act are wider, encompassing assessment of all ML/TF/PF risk factors, including customer, product, delivery channel and geographic risks.

3.63 Section 20 of the MLPC Act, on the other hand, emphasizes customer risk, i.e. the need to identify which customers present the highest ML/TF/PF risk and the need to exercise enhanced customer identification, verification and on-going due diligence and monitoring.

Identification and Due Diligence Requirements for Politically Exposed Persons

3.64 PEPs[2] are a special class of customers, who are deemed, by law, as presenting a high money laundering risk, arising from the power and influence they wield, which can, potentially be abused for personal enrichment through corruption and embezzlement.

3.65 Foreign PEPs are automatically classified as high risk customers and EDD should be conducted prior to on-boarding and on an on-going basis after establishing a relationship with them.

3.66 In relation to domestic PEPs or persons who have been entrusted with a prominent function by an international organisation, the reporting institution should establish whether there are cases of higher risk business relationship and must adopt the measures under foreign PEPs.

3.67 For foreign PEPs identified under 3.65 and higher risk domestic PEPs under 3.66 reporting institutions are required to apply EDD to their family members or close associates.

3.68 Section 20(1)(b) of the MLPC Act requires reporting institutions to put in place risk management systems to determine if a customer or beneficial owner of an account is a politically exposed person (PEP). If a customer or beneficial owner is identified as a PEP, a reporting institution 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 and verify the source of wealth and funds and other assets of the customer or beneficial owner of the customer.

What to do if Customer Identification Obligations Cannot be fulfilled

3.69 Section 22 of the MLPC Act provides that a reporting institution 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

[2] PEPs refer to both foreign and domestic PEPs

make a report on the matter to the FIU. The same should be shared with Banking Supervision, Surveillance & Financial Stability Division.

3.70 In addition to declining or discontinuing the business relationship/transaction, the reporting institution is required to immediately make a report to the FIU and the same should be shared with BSSFS.

Ongoing Due Diligence and Monitoring

3.71 Section 12B (2) of the MLPC Act provides that, reporting institutions should implement enhanced measures for high-risk customers, products, services or situations, as appropriate and may implement simplified or reduced measures for low-risk customers, products, services or situations, as appropriate.

3.72 It should be noted that section 12B (2) of the MLPC Act does not allow a reporting institution to give dispensation on customer due diligence and monitoring requirements for any customer or for any financial product on the grounds that the ML/TF/PF risk is low. ML/TF/PF risk can never be zero, but can only be low, hence the need for reduced level of monitoring for low-risk situations.

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

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

3.75 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.

3.76 A reporting institution should have written AML/CFT/CPF processes and procedures that detail how the business entity implements risk-based customer due diligence. The institution's procedures should set out and describe the different levels of due diligence for each customer risk category.

3.77 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 a reporting institution 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.

3.78 Section 26 of the MLPC Act sets out the obligations of reporting institutions in relation to ongoing due diligence.

Customer Screening

3.79 Transaction screening and monitoring systems should be capable of screening and monitoring all aspects of customer on-boarding as well as payment messages, including all additional information provided by the ordering institution or the customer when conducting wire transfers. To this effect, reporting institutions are required to have an effective screening tool.

3.80 Section 10 of Statutory Instrument 110 of 2021 (Suppression of Foreign and International Terrorism) requires reporting institutions to screen all customers in their books, including beneficial owners, authorized signatories, and customer addresses against the United Nations Security Council Resolution (UNSCR) sanctions lists on terrorism and proliferation of weapons of mass destruction (WMD)

3.81 Reporting institutions should screen their customers:

a) Whenever a new designation is announced by the UNSCR;
b) When a new customer is being on boarded; and
c) When a walk-in customer or a customer who wants to engage in a once off transaction is being attended.

3.82 It is not sufficient for a reporting institution to simply screen its customer lists against the names of sanctioned individuals or entities but should also conduct appropriate due diligence to satisfy themselves that they know who their customers are and, if their customers are controlled by a third party, to identify the third party.

3.83 Further, reporting institutions must maintain real-time sanctions screening systems in place for all cross-border transactions (both incoming and outgoing). These systems must be capable of identifying a match against any internal and vendor supplied UNSCR lists maintained by the institution. Where a reporting institution uses a screening list provided by a third-party vendor, the vendor's Service Level Agreement with the reporting institution should ensure that the list is updated immediately upon any new designation as required.

Training for Officers and Employees

3.84 Pursuant to section 25(1) (c) of the MLPC Act, reporting institutions are required to develop and implement programmes for ongoing training for their 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.

3.85 Ongoing staff training is an essential component of an efficient AML/CFT/CPF programme for preventing and detecting potential illicit transactions related to money laundering, terrorist financing, or proliferation financing. It is therefore, critical for every reporting institution to implement an ongoing training program for its employees in order to discharge part of its statutory duty to take reasonable measures to make staff aware of the MLPC Act and other laws relating to money laundering and the financing of terrorism.

3.86 The main objective of providing on-going training is to ensure that directors, officers and employees of the reporting institution are adequately trained to enable them to perform their obligations in respect of AML/CFT/CPF requirements.

3.87 Reporting institutions should take appropriate measures to make its directors, officers and employees aware of:

i the need for an understanding of ML/TF/PF risk related to customers, products, services, delivery channels and geography, how the monitoring of these risks should occur and what mitigation measures should be applied when these risks are identified;

ii policies and procedures put in place to prevent money laundering and the financing of terrorism;

iii new developments, including information on current money laundering and financing of terrorism techniques, methods and trends; and

iv the reporting of unusual and suspicious transaction reports including the handling of incomplete or declined transactions.

3.88 At a minimum, a reporting institution is required to:

i ensure that directors, officers, and employees understand ML/TF/PF risks, risk monitoring, and risk mitigation techniques;

ii create a training and awareness programme that is appropriate for the reporting institution's size, resources, and type of operation, so that relevant staff are aware of the risks associated with ML/TF/PF risks;

iii sensitise its directors, officers and employees on the importance of adhering to CDD policies, the processes for verifying customer identification and the circumstances for implementing EDD procedures and all AML/ CFT/CPF preventive measures;

iv assess the effectiveness of training; and

v provide all relevant employees with reference manuals/materials that outline their responsibilities and the institution’s policies. These should complement rather than replace formal training programmes.

3.89 While all relevant workers should be trained, the extent and frequency of training should be tailored to the nature of their responsibilities and specific risks faced by the reporting institution.

3.90 Regular refresher trainings will be required to ensure that employees are kept up to date on legal and regulatory developments. In all situations, trainings must be completed whenever a legal or regulatory change occurs, or the reporting institution’s risk assessment is revised.

3.91 As a general guide, the following categories of employees should be trained:

a) Personnel in Charge of Account Opening

Members of staff in charge of opening accounts and accepting new customers must be trained on the requirement to verify a customer's identification as well as the institution's internal account opening and customer verification procedures. They should also be trained on the identification and handling of suspicious transactions, as well as the internal suspicious transaction reporting procedures. Account Opening Personnel should also be trained on how to implement CDD measures informed by the risk profile.

b) Front-line Employees

All front-line employees who interact with the public are the initial point of contact for potential money launderers and terrorist financiers or their agents. They must be trained to recognize the true identity of the customer and to understand the type of business operations anticipated of the customer to recognise what may constitute suspicious activity at a later point. There is need to be on the lookout for any changes in a customer's transaction pattern or situations that could indicate illegal activity. Training should also cover identification and handling of suspicious transactions, as well as the procedures to be followed when a transaction is deemed suspicious. Training should be provided on how to update the customer's risk profile and what mitigation methods to use when higher risk is identified.

c) International Banking/Global Trade Services Staff

Reporting institutions must provide AML/CFT/CPF training to their international banking and global trade services departments and staff, with a focus on trade-based money laundering and wire transfers. Training should also be provided on mitigation methods based on customer's risk profile.

d) New Employees

New employees should be trained on the general background to combating money laundering and terrorist financing, how to implement RBA, and the internal suspicious transactions reporting procedures as soon as reasonably practicable, prior to interacting with consumers. Employees should be made aware of the legal responsibility to report

suspicious transactions and they should also be given a copy of the established policies and procedures for reporting such suspicious transactions. New employees must receive AML/CFT/CPF training in all aspects of the business.

e) Supervisors and Managers

Those in charge of supervising or managing staff should receive a higher degree of training encompassing the entire compliance programme. This will include the MLPC Act's penalties for non-compliance, as well as ensuring that the ML/TF/PF risks are well understood and risk mitigation techniques are appropriately applied.

f) Compliance Officers, Internal Audit and Compliance Employees

The Compliance Officer, as well as the compliance and audit personnel, should get ongoing training because of their vital role in raising the broader employee complement to AML/CFT/CPF concerns and ensuring compliance with established AML/CFT/CPF regulatory framework. Further, the compliance officer and internal auditor will require extensive initial and ongoing training on the validation and reporting of suspicious transactions, understanding of ML/TF/PF risk, risk monitoring, risk mitigation, feedback arrangements, and new trends and patterns of criminal activities among other elements of compliance

3.92 Reporting institutions are required to evaluate the training program's effectiveness. This can be done by:

i testing employees' understanding of the policies and procedures to combat ML/TF/PF, understanding of their statutory and regulatory obligations, as well as their ability to recognise suspicious transactions and understanding of ML/TF/PF risk; and

ii monitoring employees' compliance with the AML/CFT/CPF procedures, the quality and quantity of internal reports so that additional training can be provided.

3.93 Reporting institutions should keep a record of all anti-money laundering and counter-terrorism financing training provided to their employees for at least five (5) years, as provided for by the MLPC Act.

3.94 At a minimum, the records should include:

i details of the content of the training programmes provided;

ii the names of employees who received the training;

iii the date the training was delivered;

iv the results of any testing conducted to measure employees' understanding of the anti-money laundering requirements; and

v an on-going training plan.

Group Arrangements

3.95 Pursuant to section 25(4) of the MLPC Act, reporting institutions operating in a group structure are required to implement group-wide programmes against money laundering and terrorist financing, which shall be applicable, and appropriate to, all branches and subsidiaries of the group[3] and shall include:

a) the internal policies, procedures and controls;

b) policies & procedures for sharing information required for the purposes of CDD and ML/TF/PF risk management;

c) procedures to ensure that group-level compliance shall have the power to request customer, account and transaction information from branches and subsidiaries as necessary to perform their functions in order to combat ML/TF/PF; and

d) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

3.96 The financial group should have a clear understanding of all risks associated with its customers across the group, either individually or as a segment, and should document and update these on a regular basis.

3.97 When a financial group's branch or subsidiary operating outside Zimbabwe is unable to comply with requirements similar to those imposed under this guidance because such compliance is not permitted by local laws, the reporting institution must:

a) notify the Reserve Bank of such failure; and

[3] Section 25(4) of the MLPC Act is applicable to reporting institutions under both local and international groups. Further, reporting institutions under international groups shall apply the concept of, "higher of home or host country" principle i.e strictier requirements between home and host country.

b) take additional measures to effectively mitigate ML/TF/PF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the above requirements.

Independent Audit Arrangements

3.98 Pursuant to section 25(1)(e) of the MLPC Act reporting institutions are obligated to develop and implement independent audit arrangements to review and verify compliance with and effectiveness of the measures taken in accordance with the MLPC Act.

3.99 The Audit function should perform regular reviews to evaluate the adequacy of implementation of the AML/CFT/CPF policies, procedures and systems. The review process should identify weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions, including ensuring that recommendations made by the external auditor, Reserve Bank or the FIU have been satisfactorily addressed.

3.100 All audit documentation, including, amongst others, work plans, audit scope, transaction testing, should be made available to the Reserve Bank or FIU upon request.

3.101 Deficiencies noted during the audit including any breaches of policy or procedure, regulatory or legislative requirements should be clearly documented in an audit report and reported to senior management and the audit committee/ the board. Senior management should advise on corrective actions to address deficiencies and a timeline for implementing such actions.

3.102 The Audit Committee/ Board should follow up consistently to ensure that corrective actions are implemented in a timely manner.

3.103 The frequency and extent of the review should be proportionate to the nature, size and complexity of its businesses and the ML/TF/PF risks arising from those businesses. The basis for the audit frequency must be clearly articulated in the reporting institution's audit policy and scope.

Reporting of Suspicious Transactions

Obligation to report suspicious transactions

3.104 Section 30(1) of the MLPC Act requires reporting institutions, principal officers and their agents to report suspicious activity and transactions where they suspect or have reasonable grounds to suspect that any property or any transaction is involved or linked to crime, terrorism, terrorist acts or those who finance terrorism.

3.105 Such reports should be made promptly to the FIU no later than three (3) working days after forming the suspicion.

3.106 Every suspicious transaction must be reported to the FIU in the prescribed format using the goAML portal by a reporting institution. In this regard, every reporting institution shall be registered with the FIU on the goAML platform.

3.107 In terms of timing, the requirement is to submit the report to the FIU as soon as possible, but no later than three (3) working days after the suspicion is raised.

3.108 A suspicious transaction includes an attempted transaction, i.e. a transaction that was not completed but was suspicious.

3.109 **Annexure "A"** of this guidance contains the basic information needed to complete the suspicious transaction report template on the goAML platform.

3.110 **Annexure "B"** is a non-exhaustive list of indicators or red flags that can assist a reporting institution in detecting and reporting suspicious transactions.

3.111 Some suspicious transaction red flags / indications are industry-specific. As a result, reporting institutions and their staff must be aware of the common ML/TF/PF red flags related to their respective products / services, customer types, geography, and delivery channels.

Reporting Procedures

3.112 A reporting institution should develop, document, maintain, and implement reporting procedures which must:

a) make it clear to all appropriate employees to whom they should report any knowledge or suspicion of ML/TF/PF activity;

b) ensure that there is a clear reporting chain through which that knowledge or suspicion will be passed to the compliance officer;
c) require reports of internal disclosures to the compliance officer of any information or other matters that come to the attention of the person handling that business and which, in that person's opinion, gives rise to suspicion of money laundering or terrorist financing;
d) require the compliance officer to consider any report in light of all other relevant information available to him/her in order to determine whether or not it gives rise to any knowledge or suspicion of ML/TF/PF activity;
e) include the full name and address of the customer as well as a detailed description of the information that gave rise to the suspicion;
f) ensure that the compliance officer has full access to any other information that may be of assistance and is available to the reporting institution; and
g) allow the information or other matters contained in a report to be provided.

Internal Communication of Suspicious Activity

3.113 Where a member of staff notices any suspicious or unusual activity, he or she should immediately notify the compliance officer.

3.114 The escalation procedure should be contained in the internal policy and procedures.

3.115 Reporting institutions should have a secure and anonymous tip-off mechanism which may be internal or external and require training of staff.

Alerts Handling by Compliance Officer

3.116 The compliance officer is required to evaluate every report in light of any other relevant information at his/her disposal in order to determine if it raises any knowledge or suspicion of ML/TF/PF activity.

3.117 In this regard, reporting institutions should ensure that the compliance officer has full access to any other information that may be of assistance and that is available.

3.118 The compliance officer should acknowledge receipt of the alert and ensure that it includes sufficient details of the customer and as full a statement as possible of the information giving rise to the suspicion, in order to allow him/her to further evaluate the disclosure.

3.119 When evaluating an alert, the compliance officer must take reasonable steps to consider all other relevant information available within the reporting institution concerning the person or business to whom the initial report relates. This should include making a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship, and referral to identification records held.

3.120 Reporting institutions are required to maintain separate registers of all internal suspicious alerts. These registers may be contained in a single document if the details maintained in the registers can be presented separately for internal disclosures and external disclosures upon request by a competent authority.

3.121 Such registers must include details of:

a) the date on which the alert is made;
b) the person who makes the alert;
c) the person to whom the alert was made; and
d) any such information sufficient to give pointers on where the information is found.

Suspicious Transaction Report to FIU

3.122 If, after conducting his or her review, the compliance officer determines that there are no facts that would dispel the suspicion, he/she is required to report the suspicious transaction to the FIU.

3.123 Reporting to the FIU should not be limited to internal alerts. The compliance officer should not be a passive recipient of ad hoc reports of suspicious transactions but should take an active role in identifying and reporting suspicious transactions. This may also include a frequent review of exception reports, large or irregular transaction reports, and ad hoc staff reports.

3.124 Reporting institutions are required to maintain separate registers of all suspicious transactions reported to the FIU. These registers may be contained in a single document if the details

maintained in the registers can be presented separately upon request by a competent authority.

3.125 Such registers must include details of:

a) the date on which the report is made;
b) the person who makes the alert;
c) the person to whom the internal disclosure was made; and
d) information sufficient to allow the papers relevant to the report to be located.

Prohibition against Tipping-Off

3.126 With this guidance, all employees of reporting institutions are reminded of the obligation not to tip off the customer or any other third party.

3.127 Except where required by law, a reporting institution shall not disclose to its customer or to a third party that a suspicious transaction report has been submitted, or will be submitted to the FIU.

3.128 Such unlawful 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.

3.129 The provision prohibiting tipping off is contained in Section 31(2) of the MLPC Act.

3.130 In practice, however, preliminary inquiries about a business applicant, whether to collect additional information to verify true identity, or to determine the source of funds or the particular nature of the transaction being done, will not result in a tipping off crime. However, when a suspicious transaction has already been detected and further investigation is required, great care should be taken to ensure that clients are not aware that their names have been brought to the notice of the FIU. In circumstances where the reporting institution suspects ML/TF/PF and reasonably believes that pursuing the CDD procedure will alert the customer, the reporting institution shall not pursue the CDD process and shall instead file an STR with the FIU.

3.131 The compliance officer will be required to act honestly and reasonably, as well as to make decisions in good faith. All internal inquiries undertaken in reference to the report, as well as

the reasoning behind whether or not to submit the report to the authorities, must therefore be documented.

3.132 This documentation may be required to augment the first report or as evidence of good practice and best efforts if, at a later period, an inquiry is conducted in a case on which the compliance officer chose not to report and suspicions are later validated. There shall be no culpability if the compliance officer acts in good faith in determining not to escalate any suspicions.

Submission of Large Cash Transaction and Other Reports (CFTs and EFTs)

3.133 Section 30(6) of the MLPC Act requires reporting institutions to submit threshold-based transaction reports to the FIU.

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

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

a) 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 whereas;
b) CTRs must be submitted in compliance with any applicable directive issued by the FIU, regardless of whether or not the transaction is suspicious; and
c) 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.

Record Keeping

3.136 An essential component in the fight against money laundering and the financing of terrorism is audit trail of customer information and transaction records. Record keeping is pivotal in assisting law enforcement agencies and other stakeholders when conducting money laundering or terrorist financing investigations.

3.137 Reporting institutions are required to provide complete and accurate information of a customer to FIU and law enforcement agencies when carrying out their duties.

3.138 Section 24 of the MLPC Act outlines reporting institutions' record-keeping obligations, including what must be covered by such records and the minimum period such records must be retained.

3.139 A reporting institution must retain all books and records on its customers and transactions that are required and adequate to meet the record-keeping requirements of the MLPC Act, the Banking Act, guidelines and any other regulatory requirements.

3.140 Reporting institutions must ensure that all CDD information and transactions are stored in such a way that they may be quickly made available to the Reserve Bank, FIU and other stakeholders upon request.

3.141 Records of all internal reports made to the compliance officer, as well as reports made by the compliance officer to the FIU, should be kept for at least five (5) years after the date of the report. Any analysis or findings relating to the background and purpose of complex, unusual, or suspicious transactions should also be kept for at least five (5) years after the date of finding.

3.142 If a reporting institution relies on a third party to perform CDD, the reporting institution must get the necessary CDD information and records from the third party on which the reporting institution is depending on to undertake CDD measures as soon as possible. The reporting institution must ensure that the third party provides all necessary CDD data and documentation upon request and without delay, and that the third party has measures in place to comply with all record-keeping requirements under the MLPC Act, including regulations made thereunder. In any case, the reporting institution, not the third party, is responsible for complying with record keeping obligations.

Obligations Relating to Wire Transfers

3.143 Section 27 of the MLPC Act specifies the obligations which reporting institutions must adhere to while conducting or processing wire transfer transactions on behalf of their customers.

3.144 The wire transfer obligations were established in order to prevent criminals from having free access to wire transfers for moving their funds, as well as to detect such misuse when it happens.

3.145 The measures aim to ensure that basic information on the originator and beneficiary of wire transfers is immediately available to:

a. appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;
b. financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and
c. ordering, intermediary and beneficiary reporting institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant UNSCRs.

3.146 The requirements apply to both domestic and cross-border wire transfers, however, more stringent for cross-border transactions than for domestic wire transfers.

3.147 Further, with wire transfers, the requirements will apply when undertaking wire transfers equal to or exceeding one thousand United States dollars (or such lesser or greater amount as may be prescribed).

a) Ordering reporting institution refers to the reporting institution which initiates the wire transfer on behalf of a customer;
b) Intermediary reporting institution refers to a reporting institution that receives and transmits a wire transfer on behalf of the ordering reporting institution (or another intermediary reporting institution) and transmits the wire transfer to the beneficiary reporting institution (or to another intermediary reporting institution);
c) Beneficiary reporting institution refers to the reporting institution at the end of the wire transfer chain, which receives the wire transfer and makes the funds available to the beneficiary customer.

3.148 There are specific obligations for ordering, intermediary and beneficiary reporting institutions. The ordering reporting institution should:–

a) ensure that the wire transfer contains required and accurate originator information;
b) ensure that the wire transfer contains required beneficiary information;
c) maintain the required information in accordance with the record-keeping requirements set out in section 24 of the MLPC Act; and
d) not execute a wire transfer that lacks any of the required information.

3.149 The requirements do not apply to:

a) Credit card or debit card payments for goods and services, provided the credit / debit card number accompanies the payment: However, where a debit / credit card is used to effect a person to person transfer of funds, the requirements apply; and
b) Reporting institution to reporting institution funds transfers and settlements, where the reporting institutions are acting on their own and not for a customer.

3.150 The intermediary reporting institution should:

a) Ensure that, for cross-border wire transfers, all originator and beneficiary information accompanying the wire transfer is retained when the institution transmits the wire transfer to the beneficiary reporting institution (or to another intermediary reporting institution);
b) Take reasonable measures to identify wire transfers that lack required originator or beneficiary information; and
c) Have in place effective risk-based policies and procedures for determining (i) when to execute, reject or suspend a wire transfer that lacks required originator or beneficiary information and (ii) the necessary follow up action;

3.151 The beneficiary reporting institution should:

a) Verify the identity of the beneficiary and maintain the identity verification documents in accordance with the record keeping requirements of section 24 of the MLPC Act;
b) Take reasonable measures to identify wire transfers that lack required originator or beneficiary information;
c) Have in place effective risk-based policies and procedures for determining (i) when to execute, reject or suspend a wire transfer that lacks required originator or beneficiary information and (ii) the necessary follow up action;

3.152 For all qualifying cross-border wire transfers, the following information is required:

a) the name of the originator;

b) the originator account number where such an account is used to process the transaction;

c) the originator's address, or national identity number, or customer identification number or date and place of birth;

d) the name of the beneficiary; and

e) the beneficiary's account number, where such account number is used to process the transaction.

3.153 For domestic wire transfers, the same originator information as above, should accompany the wire transfer, unless the ordering reporting institution maintains such information and is in a position to avail same when required (within 3 days) to the beneficiary reporting institution or to the FIU or law enforcement authorities.

3.154 Reporting institutions should monitor payment messages to and from higher risk countries or jurisdictions, as well as transactions with higher risk countries or jurisdictions and suspend or reject payment messages or transactions with sanctioned parties, countries and jurisdictions.

3.155 A reporting institution which provides money or value transfer services and which controls both the ordering and the beneficiary side of a wire transfer, shall:

a) take into account all the information from both the ordering and beneficiary sides in order to determine whether a suspicious transaction report has to be filed; and

b) file a suspicious transaction report in any country affected by the suspicious wire transfer and make relevant transaction information available to the Financial Intelligence Unit.

3.156 Where name screening checks confirm that the wire transfer originator or beneficiary is a terrorist or terrorist entity, the requirement for the reporting institution is to freeze assets of that entity or individual.

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

4.1 Countries are required to implement targeted financial sanctions imposed from time to time under the authority of the United Nations Security Council (UNSC), for the purpose of combating terrorist financing and financing the proliferation of weapons of mass destruction. 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. The provisions are further discussed in annexures "D" and "F".

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

(i) Statutory Instrument 76 of 2014 (Suppression of Foreign and International Terrorism), requiring financing institutions to identify, freeze and report funds or other assets of individuals and entities identified by or under the authority of the UNSC for financing international terrorism; and

(ii) Statutory Instrument 110 of 2021 (Suppression of Foreign and International Terrorism), requiring reporting institutions to identify, freeze and report funds or other assets of individuals and entities identified by or under the authority of the UNSC for financing proliferation of weapons of mass destruction.

4.3 In addition, the FIU issues directives and guidelines, from time to time, on the implementation of the requirements of the two UN sanctions regimes and as such reporting institutions play a critical role in implementing the requisite measures of the targeted financial sanctions and to identify and freeze assets of designated persons / entities.

4.4 Reporting institutions are required to identify and freeze immediately the funds, other financial assets and economic resources of designated persons or entities and to ensure that no funds or other assets and economic resources are made available to such persons and entities, except in specific situations, and under conditions specified in the UNSC resolutions.

Freezing of Assets

4.5 The requirement to freeze assets of designated individuals is set out in Statutory Instrument 76 of 2014 and Statutory Instrument 110 of 2021 (Suppression of Foreign and International Terrorism), respectively.

4.6 Implementation of targeted financial sanctions requires reporting institutions to freeze, without delay and without prior notice, funds or other assets of designated persons and entities who are tied to a particular act, plot or threat of terrorism and proliferation and to ensure that the accounts, properties or assets are not operated and that no financial services are provided to the designated persons or entities. In this regard, reporting institutions are required to implement the requirement once a positive match has been established.

Funds Frozen in Error

4.7 In cases where funds or other economic resources were frozen, in error, as a result of similarity in names, wrong entries on the Sanctions Lists, wrong entries in the account of a person or entity being investigated, or as a result of any other error; the person affected may apply to the Minister of Foreign Affairs for consideration to de-freeze the funds and the Minister's determination shall be communicated in writing to the reporting institution, after which the reporting institution will act accordingly, as guided by the Minister's written determination.

Internal Controls

4.8 Reporting institutions are required to develop and maintain adequate internal controls (including due diligence procedures and training programs as appropriate) to identify existing accounts, transactions, funds or other assets of designated persons and entities.

4.9 The internal controls should guide reporting institutions in fulfilling the obligations of immediately freezing any identified funds or other assets held or controlled by designated persons and entities.

4.10 Reporting institutions should implement reasonable procedures to prevent designated persons and entities from conducting transactions with, in or through them.

Reporting

4.11 Section 12 of Statutory Instrument 110 (Suppression of Foreign and International Terrorism) stipulates that every reporting institution shall report to the FIU any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions, for review and utilization by the FIU.

4.12 Reporting institutions are required to make a report to the FIU where funds or other assets have been identified that are linked to a designated institution through the goAML platform.

4.13 A nil report will also be made to the FIU when no funds or other assets are identified. A nil report must also be submitted, when a new listing is made by the UNSCR and no match is found in the reporting institution's books.

4.14 Where there is suspicion of TF/PF, a suspicious transaction report (STR) must be filed with the FIU.

4.15 When filing an STR, reporting institutions must consider the provisions of Section 12 of Statutory Instrument 76 (Suppression of Foreign and International Terrorism).

4.16 Annexure "C" gives a non-exhaustive list of indicators or red flags that are useful in helping a reporting institution to identify and report suspicious transactions related to TF/PF.

Record Keeping

4.17 The record keeping obligations set out under Section 24 of the MLPC Act apply to TF/PF.

5. SANCTIONS FOR NON-COMPLIANCE WITH AML/CFT/CPF OBLIGATIONS

5.1 Imposition of sanctions are an essential element of Reserve Bank supervisory actions to promote compliance with AML/CFT/CPF obligations by reporting institutions.

5.2 In this regard, non-compliance by a reporting institution 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).

5.3 Criminal and civil penalties are enforceable against the reporting institution or against any of its employees, directors or agents, as the case may be or against both the institution / business and the responsible individuals.

5.4 Administrative penalties are enforceable by the FIU under section 5 of the MLPC Act as read with Directive No PFIU21,10,2024 (Civil and Administrative Penalties of 2024). Under this provision, the FIU can, among other enforcement measures –

- Impose a financial penalty against the institution / business or any of its employees, directors or agents; and / or
- Order the removal of any employee, director or shareholder; and / or
- Require the reporting institution to take specified remedial action.

Annexure "A": Basic Contents of a Suspicious Transaction Report (STR)

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

iii. Phone number, residence, work

iv. Occupation / type of business

v. Date of birth

vi. Forms of identification - National registration number
- Valid passport number
- Zimbabwean driver's license

vii. Relationship to reporting 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 "B": Indicators/ Red flags of Suspicious Transactions

The following are some examples of red flags for suspicious transactions. The list is not exhaustive and just serves as an example of how money can be laundered.

Unusual Transactions

1. Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.
2. The intensity of transactions for an inactive trading account suddenly increases without plausible reason.
3. Unusually short period of holding securities.
4. Frequent selling of securities at significant losses.
5. Structuring transactions to evade substantial shareholding.
6. Simultaneous transfer of funds to a group of customers' accounts from a third party.
7. Request to exchange large quantities of low denominations for higher denominations.
8. Rapid increase in size and frequency of cash deposits without any corresponding increase in non-cash deposits.
9. Transactions for which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

Large Cash Transactions

1. Larger or unusual settlements of securities transactions in cash form.
2. The crediting of a customer's margin account using cash and by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.
3. Depositing large cash amounts in the reporting institution's multiple bank accounts in the same day.

Transactions Incompatible with Customer's Financial Standing

1. A customer who suddenly starts making investments in large amounts when it is known to the Reporting Institution that the customer does not have the capacity to do so.
2. Transactions that cannot be matched with the investment and income levels of the customer.
3. Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.

Irregular Account Movement

1. Abnormal settlement instructions including payment to apparently unconnected parties.
2. Non-resident account with very large movement with subsequent fund transfers to offshore financial centres.
3. A client who authorizes fund transfer from his account to another client's account.
4. A client whose account indicates large or frequent wire transfer and sums are immediately withdrawn.
5. A client whose account shows active movement of funds with low level of trading transactions.
6. Mixing of cash deposits and monetary instruments in an account which such transactions do not appear to have any relation to the normal use of the account.
7. A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals running down the transferred amount.
8. Building up large balances, not consistent with the known turnover of the customer's business and subsequent transfer of account(s) held overseas.

Suspicious Behaviour/Demeanour

1. A customer for whom verification of identity proves unusually difficult and who is reluctant to provide details.
2. A group of unconnected customers who share a common correspondence address.

3. 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.
4. The excessive or unnecessary use of nominees.
5. The unnecessary granting of wide-ranging Powers of Attorney.
6. The utilization of a client account rather than the payment of things directly.
7. An unwillingness to disclose the sources of funds.

Dealing with High-Risk Jurisdictions

1. Investors based in countries where production of drugs or drug trafficking may be prevalent.
2. Funds credited into customer accounts from and to countries associated with the production, processing or marketing of narcotics or other illegal drugs; or other criminal conduct; or wire transfer to or from a banking secrecy-haven country or country generally known for money laundering and terrorist financing.
3. The sending or receipt of frequent or large volumes of wire transfers to and from offshore institutions.
4. Customers transferring large sums of money to or from overseas with specific requests for payment in cash.
5. International transfers for accounts with no history of such transfers or where the stated business of the customer does not warrant such activity.
6. Significant changes in currency shipment patterns between correspondent banks.
7. Deposits that are followed within a short time by wire transfers of funds to or through a location of specific concern, such as a country with lax controls.

Suspicious Behaviour/Demeanour by Employee(s) of the Reporting Institution

Employees of the Reporting institution may be involved in money laundering in some cases. As a result, if there is a change in the characteristics of the employees, such as lavish lifestyles, unexpected increases in performance, and so on, the reporting institution may want to monitor such situations.

Safe Deposit Boxes

Unusual high frequent access to the safe deposit box by the customer.

Annexure "C": Potential Indicators of Proliferation Financing

Reporting institutions should develop indicators that alert them to customers and transactions (actual or intended) that may be associated with proliferation financing-related activities, such as whether:

1) Transaction involves person or entity in foreign country of proliferation and terrorism concern.
2) The customer or counter-party or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.
3) Customer activity does not match business profile, or end-user information does not match end-user's business profile.
4) A freight forwarding firm is listed as the product's final destination.
5) Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
6) Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
7) Transaction involves possible sister companies (e.g. companies or transactions that demonstrate links between representatives of companies exchanging goods i.e. same owners or management.
8) Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
9) Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
10) Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).
11) Transaction involves reporting institutions with known deficiencies in AML/CFT/CPF controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.

12) Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
13) Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
14) Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.
15) Customer providing vague/incomplete information and is resistant to providing additional information when queried.
16) New customer requesting letter of credit whilst awaiting approval of new account.
17) Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
18) Additional potential indicators of sanctions evasion activity mentioned in third-party reports: involvement of items controlled under WMD export control regimes or national control regimes; involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/or dealing with complex equipment for which he/she lacks technical background; use of cash or precious metals (e.g. gold) in transactions for industrial items; involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.
19) Transactions between companies on the basis of "ledger" arrangements that obviate the need for international financial transactions.
20) Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).
21) Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.
22) Evidence that documents or other representations (e.g. relating to shipping, customs, or payment) are fake or fraudulent.
23) Customer accesses accounts, and/or uses debit or credit cards in high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.

24) Customer identified by media or law enforcement agents as having travelled, attempted/intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
25) Customer conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
26) The customer mentions that they will be travelling to, are currently in, or have returned from, a high-risk jurisdiction (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations
27) Individual/Entity's online presence supports violent extremism or radicalization.
28) Customer indicates planned cease date to account activity.
29) Customer utters threats of violence that could be of concern to National Security/Public Safety.
30) Sudden settlement of debt(s) or payments of debts by unrelated 3rd party(ies).
31) Law enforcement indicates to reporting entity that the individual/entity may be relevant to a law enforcement and/or national security investigation.
32) Customer's transactions involve individual(s)/entity(ies) identified by media or law enforcement as the subject of a terrorist financing or national security investigation.
33) Customer donates to a cause that is subject to derogatory publicly available information (crowdfunding initiative, charity, NPO, NGO, etc.).
34) Customer conducts uncharacteristic purchases (e.g. camping/outdoor equipment, weapons, ammonium nitrate, hydrogen peroxide, acetone, propane, etc).
35) Customer provides multiple variations of name, address, phone number or additional identifiers.
36) The sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity.

- The FATF issues guidelines that are relevant to reporting institutions on combating ML/PF/TF. In that regard, reporting institutions are encouraged to visit the FATF website www.fatf-gafi.org for more details.

Annexure "D": FATF Recommendation 6: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing

1.1 FATF Recommendation 6 provides that: "Countries should implement targeted financial sanctions regimes to comply with UNSCRs relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) 4 designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001)."

1.2 In line with the FATF and UN requirements, Zimbabwe passed the Suppression of Foreign and International Terrorism Act (Application of UNSCR 1267 of 1999, UNSCR 1373 of 2001 and Successor UNSCRs) Regulations, 2014, Statutory Instrument 76 of 2014.

Annexure "E": FATF Recommendation 7: Targeted Financial Sanctions Related to Proliferation Financing

1.3 FATF Recommendation 7 provides that: "Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations."

1.4 Pursuant to these FATF and UN requirements, Zimbabwe passed the Suppression of Foreign and International Terrorism Act (Application of UNSCR 1540 (2004)1673, 1810, 1887, 1977 (On Non-State Actor Proliferation), 1695, 1718, 1874 on Democratic People's Republic of Korea (DPRK) and 1696, 1737, 1747, 1803 and 1929, UNSCR 2094 (2013), 2231 (2015) UNSCR 2270 (2016), UNSCR 2321 (2016), UNSCR 2371 (2017), of 5 UNSCR 2375 (2017) UNSCR 2397 (2017) and Successor UNSCRS) Regulations, 2021, Statutory Instrument 110 of 2021.

1.5 Targeted financial sanctions relating to proliferation financing are applicable to;

(a) persons or entities engaging in or providing support for, including through illicit means, proliferation-sensitive activities and programmes;

(b) persons acting on behalf of, or controlled by, or at the direction of designated persons or entities; and

(c) persons or entities assisting designated persons or entities in evading sanctions or violating resolution provisions.

1.6 In compliance with recommendations 6 and 7, FIs are required to freeze, without delay and without prior notice, funds or other assets of designated persons and entities who are tied to a particular act, plot or threat of terrorism and proliferation, as defined under the various resolutions cited above.

1.7 Reporting institutions are required to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

1.8 Reporting institutions should therefore have sanctions screening systems in place to identify any such sanctioned individuals or entities. There are several reliable IT-based sanctions screening solutions on the market that are accessible on a subscription basis to reporting institutions. Transaction screening and monitoring systems should be capable of screening and monitoring all aspects of customer onboarding as well as payment messages, including all additional information provided by the ordering institution or the customer when conducting wire transfers.

1.9 If there is a positive match, i.e. where the reporting institution has a customer on the UNSCR list in its books, the reporting institution must identify whether the customer owns any funds or other assets within the institution, including the funds or assets identified and immediately verify whether the details of the listed party perfectly match with the particulars of their customer.

1.10 After positively identifying a match and verifying the transactions, the reporting institution is required to freeze the assets, immediately without delay.

EFFECTIVE DATE

The effective date of this Guideline shall be 1 June 2025. Questions relating to the Guideline should be addressed to the Director, Bank Supervision, Surveillance & Financial Stability Division, Reserve Bank of Zimbabwe.

References

- The following informational resources were used in the crafting of this guidance for the purpose of providing direction:

1. FATF Methodology for Assessing Technical Compliance with the FAFT Recommendations and the Effectiveness of AML/CFT Systems (Updated June 2023).
2. Guidance on Ultimate Beneficial Owners of Legal Persons and Legal Arrangements - Bank of Nigeria (January 2023).
3. Guidance To Reporting institutions and Designated Non-Financial Businesses and Professions on The Risk Based Approach to Implementation of Anti-Money Laundering and Combating Financing of Terrorism Obligations - Financial Intelligence Unit of Zimbabwe (January 2021).
4. Guidance to Reporting institutions and Designated Non-Financial Businesses and Professions: Targeted Financial Sanctions Relating to Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction Financial Intelligence Unit of Zimbabwe (July 2021).
5. Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation - Bank of Mauritius (January 2020)
6. Money Laundering and Proceeds of Crime Act [Chapter 9:24].
7. Palermo Convention (2000) against Transnational Organized Crime
8. Statutory Instrument 56 of 2019: 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 and 1696,1737, 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.
9. Statutory Instrument 76 of 2014: Suppression of Foreign and International Terrorism (Application of UNSCR 1267 of 1999 and UNSCR 1373 of 2001) Regulations, 2014.