Bank Use Promotion & Suppression of Money Laundering Unit

GUIDELINES ON ANTI-MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM FOR INSURERS, 2012

Issued in terms of the Bank Use Promotion & Suppression of Money Laundering Act [Chapter 24:24]

These guidelines amplify and explain obligations that insurers are required to comply with under the Bank Use Promotion and Suppression of Money Laundering Act [Chapter 24.24] (hereinafter referred to as "the Act").

The guidelines are issued in terms of the Act and are legally binding, laying down minimum standards on Anti Money Laundering and Combating Financing of Terrorism (AML/CFT) measures for every insurer as defined in the Insurance Act [Chapter 24:07].

TABLE OF CONTENTS

Terms and Acronyms Used

Terms	Definition
AML / CFT	Anti Money Laundering and Combating Financing of Terrorism
Beneficial owner	Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
BUPSML UNIT / FIU or Unit	Refers to the Bank Use Promotion and Financial Intelligence Unit established in terms of the Bank Use Promotion and Suppression of Money Laundering Act
BUPSML Act	Bank Use Promotion and Suppression of Money Laundering Act [Chapter 24:24]
BUPSML UNIT	Bank Use Promotion and Financial Intelligence Unit
BUPSML Unit	Bank Use Promotion and Suppression of Money Laundering Unit established in terms of the Bank Use Promotion and Suppression of Money Laundering Act (otherwise known as "the Financial Intelligence Unit or "FIU")
Business Relationship	'Business relationship' is any arrangement between the financial institution and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a 'frequent, habitual or regular' basis and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset.
CDD	Customer Due Diligence
Customer	In relation to insurers, 'Customer' includes: • An insurance policyholder or an applicant for such policy; • An individual, a legal person, a legal arrangement, beneficial owners or controller who exercises influence over an insurance policy. The beneficiary of the policy may be the customer or it may be a third party to the relationship between the insurer and the customer.
Designated Institution	Means any institution designated in terms of the Bank Use Promotion and Suppression of Money Laundering Act [Chapter 24:24] for

	purposes of implementing statutory AML / CFT obligations prescribed therein. The term covers Financial Institutions (which includes insurers) as well as Designated Non-Financial Businesses and Professions.
DNFBPs	Designated Non Financial Businesses and Professions e.g. legal practitioners, public accountants, real estate agents and casinos.
FIU	Financial Intelligence Unit (referred to in the Act as the Bank Use Promotion and Suppression of Money Laundering Unit.
KYC	Know Your Customer principle
Money Laundering	A transaction (or series of connected transactions) which is intended to conceal or disguise the illicit nature, source, location, disposition or movement of the proceeds of crime.
Insurer	Refers to every entity (or individual) that is registered or is required to be registered as an insurer in terms of the Insurance Act [Chapter 24:07] and which offers insurance products as contemplated in that Act.
PEP	Politically Exposed Person. This refers to a person holding high public office. A PEP may be domestic/local or foreign. Financial institutions are required to implement enhanced CDD measures in respect of a PEP customer or prospective customer. The enhanced measures should also be applied to spouses, close relatives or associate of a PEP.
STR	Suspicious Transaction Report
Suspicious Transaction	Includes a transaction which is inconsistent with a customer's known, normal business or lacks an obvious economic rationale. It includes a transaction which is unusual because of its size, volume, type or usual pattern of transacting or otherwise suggestive of known money laundering methods or financing of terrorism.

1. INTRODUCTION

1.1 General Overview

1.1.1 Zimbabwe is a member of the Eastern and Southern Africa Anti Money Laundering Group (ESAAMLG). ESAAMLG, along with other similar regional groups, is an associate member of the Financial Action Task Force (FATF). The FATF is an intergovernmental body tasked with setting standards and measures relating to Anti Money Laundering and Combating Financing of Terrorism (AML/CFT) and overseeing their implementation by countries.

1.1.2 FATF and ESAAMLG member countries, including Zimbabwe, have undertaken to implement AML / CFT measures in their jurisdictions, guided by the FATF Recommendations, as amended from time to time.

1.1.3 In line with Zimbabwe's international obligations and the country's commitment to play its part in the national, regional and global fight against money laundering and terrorist financing, the country has put in place a legal and institutional framework designed to make it more difficult for criminals to use the country's financial system to launder proceeds of their criminal activities or to channel funds for the financing of terrorist activities.

1.1.4 The government has enacted various pieces of legislation, among which is the Bank Use Promotion & Suppression of Money Laundering Act [Chapter 24:24] (hereinafter the "BUPSML Act" or simply "the Act"); The Serious Offences (Confiscation of Profits) Act [Chapter 9:07]; and the Suppression of Foreign and International Terrorism Act [Chapter 11:17].

1.1.5 The BUPSML Act imposes certain obligations on designated institutions and establishes a financial intelligence unit named the Bank Use Promotion and Financial Intelligence Unit (hereinafter referred to as the "BUPSML Unit" or simply "the Unit") whose main responsibility is to oversee compliance with the Act.

1.1.6 The BUPSML Unit is empowered to issue guidelines to amplify and give effect to the provisions of the BUPSML Act.

1.1.7 It is against this background that the Unit has issued these Guidelines, known as the Anti Money Laundering / Combating the Financing of Terrorism Guidelines for Insurers, 2012 (hereinafter simply referred to as "the Guidelines").

1.2 *What is Money Laundering and Terrorist Financing?*

1.2.1 Money Laundering is any transaction that is designed to disguise the illegal source of proceeds of crime to make it look as though the funds came from a legitimate source.

1.2.2 There are various methods of laundering proceeds of crime, including transmitting such funds through the formal financial systems and purchasing high value assets such as real estate.

1.2.3 For money laundering to take place, an offence or offences would have been committed from which the criminals derived a financial benefit. The offence from which the funds have been derived is referred to as the "predicate offence". Predicate offences to money laundering include all offences defined as "serious offence" in terms of the Serious Offences (Confiscation of Profits) Act. They include theft, fraud, drug trafficking, human trafficking, corruption and tax-related offences, among many others.

1.2.4 The objective behind money laundering is that the criminals or their accomplices want to "clean up" proceeds of crime so that the funds don't appear to be connected with the predicate offence.

1.2.5 The person laundering funds may or may not have been directly involved in the predicate offence.

1.2.6 The offence of financing of terrorism is different from the offence of money laundering in that, with financing of terrorism, the funds are not necessarily linked to a predicate offence. Funds used to finance terrorism may come either from a legitimate or illegitimate source.

1.2.7 Financing of terrorism or terrorist financing (FT) includes the channeling of funds or other material resources for terrorist acts, to terrorists or terrorist organizations.

1.2.8 Criminals favour using financial systems of countries to clean up and disguise the illicit origins of proceeds of crime. Similarly individuals and entities who finance terrorism around the world also find it convenient to use the financial systems of countries to move funds that are used to finance terrorism.

1.2.9 Zimbabwe, like the majority of countries the world over, has put in place a framework designed to make it more difficult for criminals to use the country's financial system to either launder proceeds of crime or to finance terrorism.

1.2.10 It is in this context that the law requires financial and other designated institutions that are seen as vulnerable to money-laundering and terrorist financing, to implement AML/CFT measures, including conducting prescribed Customer Due Diligence (CDD) measures and submitting Suspicious Transaction Reports (STRs) to the financial intelligence unit.

1.2.11 The offence of money laundering is criminalized in terms of the Serious Offences (Confiscation of Profits) Act while the offence of financing of terrorism is criminalised under the Suppression of Foreign and International Terrorism Act.

1.2.12 The Bank Use Promotion and Suppression of Money Laundering Act sets out the measures that designated institutions are required to implement to combat money laundering and financing of terrorism. The Act also establishes the Bank Use Promotion and Financial Intelligence Unit which is a unit within the Reserve Bank of Zimbabwe tasked with overseeing compliance with the Act.

1.3 ***The Role of the BUPSML Unit***

1.3.1 The BUPSML Unit is the financial intelligence unit of the country whose main responsibility is to ensure compliance with AML/CFT statutory and regulatory requirements by designated reporting institutions.

1.3.2 More particularly, the Unit is responsible for –

- Receiving STRs from designated institutions;
- Analyzing the received STRs;
- Disseminating STRs of interest to law enforcement agencies;
- Supervising and monitoring designated institutions to ensure compliance with the Act and Guidelines.

1.4 **What are Designated Institutions?**

1.4.1 Designated institutions are persons and entities designated in terms of the BUPSML Act for purposes of implementing AML/CFT requirements. Designated Institutions consist of Financial Institutions and Designated Non-Financial Businesses and Professions (DNFBPs).

1.4.2 Financial institutions include banks, insurers, moneylenders, pension funds; asset managers; bureau de change and money transfer agencies, while DNFBPs include legal practitioners; public accountants; estate agents and casinos.

1.4.3 Some AML/CFT requirements apply to Financial Institutions but not to DNFBPs.

1.4.4 Insurance agents and insurance brokers are an integral part of the insurance industry due to their direct contact with customers and are, typically, involved in the sales operations of the insurers.

1.4.5 Given their direct contact with customers, insurance agents and brokers must be integrated into an insurance company's anti-money laundering programme and monitored for compliance with all AML/CFT requirements.

1.4.6 An insurer's AML/CFT programme must include procedures for obtaining relevant customer-related information from its agents and/or brokers, or any other introducers.

1.4.7 In this regard, the Unit requires each insurance company to integrate its agents and brokers into its own AML/CFT programme, providing all necessary AML/CFT training and monitoring.

1.5 Insurance Products

1.5.1 Insurance companies offer a variety of products that include:

- life insurance policies
- annuity policies,
- property insurance policies,
- casualty insurance policies; and
- health insurance policies.

1.5.2 These products are offered through a number of different distribution channels. Some insurers sell their products directly to the public while others employ agents or brokers who may either be captive or independent.

1.5.3 Insurance policies that have a cash, investment or surrender value are potential money laundering and terrorist financing vehicles.

1.5.4 Cash value can be redeemed by a money launderer, or can be used as a source of terrorist funding, or even for further investment of tainted proceeds.

1.5.5 Similarly, investment or annuity contracts also pose a money laundering risk because they allow money launderers to exchange illicit funds for an immediate or deferred income stream or to purchase a deferred annuity and obtain clean funds upon redemption.

1.5.6 The extent of money laundering or terrorist financing risks may differ with different types of policies or products.

1.5.7 AML/CFT measures apply special focus on combating money laundering and terrorist financing risks in life insurance policies and those insurance products with investment and /or cash features as these can be liquidated easily to provide funds for criminals.

1.5.8 Insurers are required to implement prescribed AML/CFT measures when offering the following types of insurance products:

(i) a permanent life insurance policy, other than a group life insurance policy;
(ii) any annuity contract, other than a group annuity contract;
(iii) any insurance product with features of cash value or investment; and
(iv) any other insurance product that the insurer considers, on the basis of the risk-based approach, as posing money laundering or terrorist financing risk.

2 CUSTOMER DUE DILIGENCE AND KYC REQUIREMENTS

2.1 General

2.1.1 Customer Due Diligence (CDD) and the Know Your Customer (KYC) principle are key elements in the fight against money laundering and terrorist financing.

2.1.2 Financial Institutions are required to have a thorough understanding of their customers by gathering as much information as possible concerning-

- The identity of the customer;
- In the case of legal persons and arrangements, sufficient information must be obtained concerning the identity of the natural persons who ultimately control and/or are the ultimate owners or beneficiaries of the legal person or legal arrangement. This may involve unmasking several levels of corporate veils to gut to the ultimate owners, beneficiaries and controllers.;
- The nature of business and source of funds of the customer: it is very important for the financial institution that receives/ handles or expects to receive/ handle funds from a customer to know the source of funds or expected source of funds of the customer. In this regard, the financial institution should not just accept information provided by the customer at face value. It should take reasonable steps to independently verify the information supplied by the customer.

2.1.3 A thorough knowledge of the customer, its nature of business and source or expected source of funds will make it easier for the financial institution to detect and report suspicious transactions that are inconsistent with the institution's knowledge of the customer, his source of funds or normal transacting patterns.

2.1.4 The insurer should comply with all AML/CFT statutory and regulatory measures that are required for all financial institutions as well as additional measures that are necessary, taking into account the peculiarities of the insurance sector, including its peculiar AML/CFT vulnerabilities.

2.1.5 Customers of financial institutions may be either occasional / once off relationships or may involve an ongoing business relationship. CDD procedures are required in both cases. With ongoing business relationships, CDD requirements should be carried out both at the inception of the business relationship and on an ongoing basis to ensure the insurer is up to date in its knowledge of the customer.

2.1.6 CDD should be undertaken whenever it appears to the insurer that there has been a material change in the ownership and/or control structure of the customer or in the customer's nature of business or source of income.

2.1.7 An insurer shall therefore carry out CDD measures when:

- establishing a business relationship with a customer; or
- undertaking any occasional transaction above US$5 000 (five thousand United States dollars), whether in the form of a single transaction or a series of transactions that are or appear to be linked and whose aggregate value exceeds the prescribed threshold; or
- there is a suspicion of money laundering or terrorist financing, regardless of the above threshold (i.e. even when the value of the transaction or series of transactions is below the US$5 000); or
- there are doubts about the veracity or adequacy of previously obtained customers identification data.

2.1.8 Normally, an insurer shall not conclude the establishment of a business relationship before the completion of CDD requirements.

2.1.9 In cases where it is not reasonably feasible to wait for the completion of the due diligence process, however, the business relationship may be established immediately provided that simultaneous steps are immediately taken to verify the identity of all relevant parties and to complete the due diligence process:

2.1.10 In such a case that the insurer shall terminate the relationship immediately if for any reason the insurer is unable to complete the due diligence process within 14 days from the date of establishment of the business relationship.

2.1.11 If the failure to complete the CDD process is on account of lack of cooperation by the customer, e.g. failure to furnish requested documents or other relevant information, the insurer shall, in addition to terminating the business relationship, file an STR with the Unit.

2.1.12 Where an applicant is permitted to utilize the business relationship prior to the customer due diligence process being satisfactorily completed e.g. in selecting or changing the assets to be linked to the policy, the insurer must consider adopting risk management procedures, e.g. a limitation of the number, types and/or amount of activity that may be permitted before the insurer is satisfied as to the customer due diligence of the applicant, and any other relevant parties.

2.1.13 In any event, an insurer would not be expected to settle a claim made under the policy unless it is satisfied as to the identity of the applicant or policyholder, the source of wealth of the original applicant and, if different, the identity of any beneficiary of the policy.

2.1.14 CDD measures that insurers are required to undertake consist of:

- Identifying and verifying the identity of every customer and beneficial owner;
- Identifying and verifying the identity of every natural person who is a member of the board of directors of the customer or a member of a similar controlling organ of the customer;
- Obtaining information on the purpose and intended nature of the business relationship;
- Obtaining information on the source of funds of the transaction or expected transactions;
- Conducting ongoing due diligence in respect of customers with whom the insurer has an account with or has established an ongoing business relationship.

2.1.15 The insurer shall obtain and maintain accurate information (name, address and policy/account number) of an applicant or policyholder / customer.

2.1.16 An insurer may apply reduced or simplified identification measures where the risk of money laundering or terrorist financing is lower. Simplified identification/ verification measures may only be implemented following a proper and documented risk analysis. The simplified measures must be approved by the board of directors of the insurer.

2.1.17 In addition, information beyond customer identity, such as customer address and location, and purpose of the transaction, is required to adequately assess risk.

2.1.18 Where a policy is assigned to a third party, verification of identity must be obtained either before assignment takes place, or as soon as reasonably practicable thereafter and, in any event, no later than 7 business days.

2.1.19 An insurer shall put in place KYC policies and procedures which incorporate the following four key elements:

a. Customer Acceptance Policy;
b. Customer Identification Procedures;
c. Monitoring of Transactions; and
d. Risk Management.

2.2 Customer Acceptance Policy

2.2.1 Every insurer shall develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship with the insurer:

2.2.2 No transaction shall be conducted in anonymous or fictitious name(s). The insurer shall not allow any transaction in any anonymous or fictitious name (s) or on behalf of a person whose identity has not been disclosed or cannot be verified.

2.2.3 The insurer shall not conduct any transaction where it is unable to apply appropriate customer due diligence measures i.e. the insurer is unable to verify the identity and /or obtain documents required due to non-cooperation of the customer or non reliability of the data/information furnished to the designated institution. Where a business relationship had already been established before completion of applicable CDD measures, the insurer shall terminate such relationship forthwith and, where appropriate, submit an STR.

2.2.4 Circumstances in which a customer is permitted to act on behalf of another person/entity shall be clearly spelt out in the customer acceptance policy. In such cases, the beneficial owner(s) should be identified and all reasonable steps shall be taken to verify their identities.

2.2.5 Where a beneficiary is nominated to receive any benefit arising under a policy, the verification of the identity of that beneficiary may take place after the business relationship has been established, provided that it takes place at or before the time of payout or at or before the time the beneficiary exercises a right under the policy.

2.2.6 For the purposes of this waiver, a beneficiary cannot be the policyholder or any person who should normally be identified at the outset of a business relationship. This waiver does not apply to any beneficiary who is able to exercise control over the assets of the policy prior to their being transferred into the beneficiary's ownership.

2.2.7 The insurer shall prepare a profile for each new customer, where regular transactions or a continuing business relationship is expected, based on risk categorization. The nature and extent of due diligence shall depend on the risk perceived by the designated institution.

2.2.8 The insurer shall apply enhanced due diligence measures based on risk assessment, especially on higher risk customers or those for whom the source of funds are not clear. Examples of customers requiring enhanced due diligence include:

(a) non-resident customers;

(b) customers from jurisdictions designated by the FATF as non-cooperating jurisdictions or as jurisdictions that do not sufficiently apply the FATF standards;

(c) high net worth individuals;

(d) Politically Exposed Persons (PEPs);

(e) non-face to face customers; and

(f) those with dubious reputations as per public information available, etc.

2.3 Customer Identification and Verification Procedures

2.3.1 Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. The insurer shall obtain sufficient information necessary to establish, to its reasonable satisfaction, the identity of each new customer, whether a once off or ongoing relationship is contemplated.

2.3.2 For customers that are natural persons, the insurer shall obtain sufficient identification document/s to verify the identity of the customer such as;

- National identity document,
- Valid Passport,
- Driving licence and
- Letter from a recognized public authority or public servant verifying the identity of the customer to the satisfaction of the insurer.

2.3.3 For customers that are legal persons, the insurer shall;

(i) verify the legal status of the legal person through proper and relevant documents;

(ii) verify that any person purporting to act on behalf of the legal person is so authorized and his identity verified;

(iii) Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person (beneficial owner(s));

(iv) For non-individual customers such as corporate customers, clubs, societies and charities trusts and similar legal persons and legal arrangements, the insurer shall obtain a letter of authorization from the entity, authorizing a named person to conduct transactions on behalf of the entity. The letter shall have a letterhead specifying the name of the entity, its address and business registration number. Where possible, the insurer shall verify the identification data of the entity as stated on the authorization letter.

(v) Where the applicant is a trustee the insurer shall satisfy itself that the settler, all trustees and all beneficiaries have been identified in accordance with the appropriate verification requirements for individuals.

(vi) The insurer shall introduce a system of periodical updating of customer identification data.

2.3.4 When there is suspicion of money laundering or financing of terrorism, or where there are doubts regarding the adequacy or veracity of previously obtained customer identification data, the insurer is required to review the due diligence measures including verifying again the identity of the customer and obtaining information on the purpose and intended nature of the business relationship, as the case may be.

Verification by Outside Agency, Internet or Other Methods

2.3.5 When an external agency or other external source of information is used for the verification of customer identity, the insurer should be able to demonstrate that an assessment of reliability of the source has been made, usually by an investigation into the agency providing the data.

2.3.6 Where the verification of identity or source of wealth is done using an agency, internet or other sources, the following must be recorded and retained in the insurer's records:

(a) the name of the agency or database which has provided the information;

(b) the information upon which the insurer is basing its verification;

(c) the name of the person who has reviewed the information, and, if necessary, sign-off by a senior member of staff; and

(d) the date of verification.

Additional Identification Requirements for Politically Exposed Persons

2.3.7 Politically exposed persons are individuals who are or have been entrusted with prominent public functions in the local or a foreign jurisdiction, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, political party officials, etc. Persons holding high office in international organizations shall also be treated as PEPs. Close relatives and associates of PEPs shall also be similarly treated.

2.3.8 The insurer shall gather sufficient information on any person/customer of this category intending to undertake a transaction and check all the information available on the person in the public domain.

2.3.9 The insurer shall verify the identity of the person and seek information about the source/s of wealth and source/s of funds before accepting a PEP as a customer.

2.3.10 The decision to undertake a transaction with a PEP shall be taken at board or similar level, and be documented. This requirement shall be clearly spelt out in the Customer Acceptance Policy.

2.3.11 Insurers shall subject all ongoing business relationships with PEPs to enhanced monitoring on an ongoing basis.

2.3.12 These requirements may also be applied to customers who become PEPs subsequent to establishment of the business relationship.

2.3.13 These requirements are also applicable to transactions where a PEP is or appears to be the ultimate beneficial owner of a policy or other transaction.

Powers of Attorney and Third Party Mandates

2.3.14 When an application for a business relationship is received from an applicant acting under a power of attorney or similar authority, evidence of identification must be obtained for the holder(s) of the power of attorney and/or third party mandates, in addition to the evidence of identification for the person granting the power.

2.3.15 The insurer must be satisfied that the power or mandate exists. The reason for granting the power of attorney must also be recorded.

Other Parties to an Application

2.3.16 Where an application for a business relationship has persons other than the applicant and beneficiaries who are able to exercise significant control over the assets, for example an investment advisor on a personalized bond, the insurer shall establish procedures for verifying the identity of the controlling person(s) as appropriate.

2.3.17 Where the controlling person or entity is a regulated investment advisor they may be accepted without detailed identification and verification checks being made, provided that the insurer is satisfied on reasonable grounds, that the insurer is a regulated investment advisor.

2.3.18 A designated institution shall ensure that the persons within the controller from whom the designated institution is to take instructions have been identified (although their identity need not be verified) and specimen signatures have been obtained.

2.4 Monitoring of Transactions

2.4.1 Where the insurer has repeat customers or ongoing business relationships, ongoing monitoring is essential. Insurers are required to have an understanding of the normal transacting patterns and source of funds of the customer. This will give the designated institution the means to identify transactions that fall outside the regular pattern of activity.

2.4.2 The extent of monitoring will depend on the risk sensitivity of the customer or of the transaction. Special attention should be paid to all complex or unusually high-value transactions and all unusual patterns or transactions which have no apparent economic or visible lawful purpose.

2.4.3 The following features may tend to increase the risk profile of a product:

- Acceptance of payments or receipts from third parties.
- Acceptance of very high value or unlimited value payments or large volumes of lower value payments.
- Acceptance of payments made in cash or endorsed money orders or cashier cheques.
- Acceptance of frequent payments outside of a normal premium policy or payment schedule.
- Allowance of withdrawals at any time with limited charges or fees.
- Acceptance to be used as collateral for a loan and/or written in a discretionary or other increased risk trust.
- Products that allow for high cash values.
- Products that accept high amount lump sum payments, coupled with liquidity features.
- Products that allow for assignment without the insurer being aware that the beneficiary of the contract has been changed until such time as a claim is made.

2.4.4 The insurer shall set key indicators for such policies, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

2.4.5 The insurer shall put in place a system of periodic review of risk categorization of customers and the need for applying enhanced due diligence measures.

2.4.6 The insurer shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in the FATF Statements on uncooperative jurisdictions or jurisdictions that do not or insufficiently apply the FATF Recommendations.

2.4.7 Further, if the policy has no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined and written findings together with all the documents should be retained and made available to the Unit and other relevant authorities, on request.

2.4.8 Where the insurer is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the insurer shall not enter into the business relationship or where it had already established a business relationship, the insurer shall terminate the relationship forthwith and submit a suspicious transactions report to the Unit.

2.5 Risk Management and Risk Assessment

2.5.1 The insurer shall adopt a risk based approach when undertaking CDD measures.

2.5.2 The insurer shall identify the main AML/CFT vulnerabilities it is exposed to and address them accordingly.

2.5.3 Higher risk customers, products and services should be identified.

2.5.4 **Risk assessment** must include a variety of factors, depending upon particular circumstances, including but not limited to:

- the size/value of the transaction;
- the applicant and any other parties involved, and their status, including considerations in respect of PEPs;

- time scale, especially in relation to early encashment;
- the complexity of the structure(s) involved;
- the involvement of additional parties to the application;
- the nature, scale and complexity of the insurer's operations, including geographical diversity;
- The initial and ongoing due diligence or monitoring conducted on the insurer's agent locations;
- The insurer's customer, product, and activity profile;
- The nature of the business relationship;
- The volume and size/value of transactions;
- The extent to which the designated institution is dealing directly with customers or is dealing through intermediaries, third parties or in a non-face-to-face setting.

2.5.5 The effectiveness of the risk-based approach is enhanced where insurers are able to share information with other insurers and financial institutions, including foreign counterparts.

Controls for Higher Risk Situations

2.5.6 The insurer shall implement appropriate measures and controls to mitigate the potential ML/TF risks for situations that are considered to be of higher risk as a result of the insurer's risk assessment.

2.5.7 The enhanced measures and controls may include:

- Increased levels of know your customer (KYC) or enhanced due diligence, such as proactive contact with the customer to determine the reason for the transactions.
- Increased levels of controls and frequency of reviews of customer relationships.
- Increased transaction monitoring of higher-risk products, services and channels.
- Enhanced systematic controls and data integrity at the points of payment, particularly at higher risk agent/broker location.

2.5.8 Insurers should pay special attention to any money laundering or terrorist financing threats that may arise from new or developing technologies, including transactions through internet, which might promote anonymity, and take appropriate measures to address such threats.

Risk Based Approach to Risk Management

2.5.9 Insurers shall formulate and implement a risk-based approach in their AML/CFT programmes.

2.5.10 This approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme.

2.5.11 This should be evidenced by categorization of the customer base, products and services by risk rating (e.g. low, medium, high) and identification of assigned actions by risk types.

2.5.12 While each insurer will determine the number and name of risk categories, the fundamental issue is for the adoption of reasonable criteria for assessing risks.

2.5.13 A insurer shall conduct periodic reviews (not more than two years apart) to determine whether any adjustment should be made to the risk rating.

2.5.14 Review of the risk rating for high risk customers may be undertaken more frequently than for other customers and a determination should be made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions shall be documented.

2.5.15 The risk rating framework should take into account customer acceptance and on-going monitoring policies and procedures that assist the insurer in identifying the types of customers that are likely to pose higher than average money laundering and terrorist financing risk.

2.5.16 A more extensive customer due diligence process should be adopted for higher risk customers. There should also be clear internal guidelines on

which level of management is able to approve business relationships with such customers.

2.5.17 The risk rating framework should provide for documentation of any changes in a customer's risk rating and the reason for such change.

2.5.18 The insurer shall therefore design an AML/CFT framework that addresses the needs of the institution and should include at a minimum:

- Differentiation of customer relationships by risk categories (such as high, moderate or low);
- Differentiation of customer relationships by risk factors (such as products, customer type/profession, country of domicile, complexity of ownership and legal structure, source of business, type of assets, size, volume and type of transactions, cash transactions, adherence to customer activity profile);
- KYC documentation and due diligence information requirements, appropriate for each risk category and risk factor; and
- Requirements for the approval of upgrading and downgrading of customer risk ratings.

2.5.19 The insurer shall establish a customer's profile taking into account, at a minimum:

- The nature of the customer's business (whether cash intensive e.g. casinos and restaurants);
- The complexity of the product;
- Type of customer, based on specific risk factors (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports transaction patterns, whether the customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place);

- Delivery channels to meet premium requirements(e.g. whether mobile/internet banking, wire transfers to third parties, remote cash payments);
- Geographical origin of the customer;
- Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking, corruption or lacking proper standards in the prevention of money laundering/financing of terrorism, whether the customer is subject to regulatory or public disclosure requirements);
- Whether the origin of wealth and/or source of funds can be easily verified and whether the audit trail has been deliberately broken and/or unnecessarily layered;
- Unwillingness of the customer to cooperate with the insurance company's customer due diligence process for no apparent reason;
- Any other information that raises suspicion of the customer's connection to money laundering or terrorist financing.

2.5.20 In addition to examples of suspicious transactions given in this Guideline, insurers should regularly consult literature on typologies on money laundering and terrorist financing available on FATF and ESAAMLG websites.

Cancellation Periods /Cooling Off

2.5.21 Where an applicant takes up the right to decline to proceed with a contract during a cooling off or cancellation period (where this is permitted by the prevailing regulations and rules under which the contract was sold), the circumstances surrounding the request to cancel must be considered, and if they are viewed as suspicious, then an SRT shall be submitted to the Unit.

2.5.22 Any payout to a policyholder as a result of such a right being exercised should normally be made to the account from which the funds were originally

received. If the payout is to be by cheque, the cheque must be payable to the policyholder and marked ‘account payee only’.

2.5.23 Under certain circumstances payment may be made to a third party account, for example a customer money account, or payment to the original account may be impossible, for example if the account has subsequently been closed. In these circumstances the insurer must be satisfied with the connection between the payee and the policyholder, and must also consider whether the payment request is suspicious, in which case, suspicion reporting procedures must be followed.

2.5.24 Since cancellation/cooling-off rights could offer a readily available route for laundering money and terrorist financing, insurers need to be alert to any suspicious exercise of these rights by a customer, or in respect of business introduced through an intermediary.

3 INTERNAL CONTROLS, POLICIES & PROCEDURES

3.1 General

3.1.1 The Board of directors or equivalent decision-making body of the insurer shall ensure that effective internal controls are in place by establishing appropriate procedures and ensuring their effective implementation.

3.1.2 The procedures shall cover proper management oversight systems and controls, segregation of duties, training and other related matters. Responsibility shall be explicitly allocated within the designated institution so as to ensure that the AML/CFT policies and procedures are implemented effectively.

3.1.3 An insurer's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the AML/CFT policies and procedures.

3.1.4 As a general rule, the compliance function should provide an independent evaluation of the insurer's compliance with legal and regulatory requirements.

3.1.5 The insurer shall ensure that its audit department or unit is staffed adequately with qualified and competent individuals.

3.2 Appointment of a Money Laundering Reporting Officer (MLRO)

3.2.1 Every insurer shall appoint a senior managerial employee as a Money Laundering Reporting Officer (MLRO) who shall be located at the head/corporate office of the insurer.

3.2.2 The MLRO shall, among other things, be responsible for;

- Reporting of all suspicious transactions to the Unit;
- Submission of any returns or other information as may be required in terms of the law, Guidelines or directive issued by the Unit;

- Overseeing and ensuring overall compliance with statutory and regulatory AML/CFT requirements;
- Developing and implementation of appropriate compliance procedures across the full range of AML/CFT areas (e.g. CDD, record keeping, etc.)

3.2.3 To enable the MLRO to discharge his responsibilities, the insurer shall ensure that the MLRO and other appropriate staff members have access to customer identification data and other CDD information, transaction records and other information relevant to AML/CFT.

3.2.4 The insurer shall:

(a) have in place procedures for the prompt reporting of suspicious transactions by the internal employees to the MLRO and

(b) provide the MLRO with the necessary access to systems and records to enable him/her to investigate and validate internal suspicious reports which would have been reported to him/her and

(c) ensure that all employees are informed of the identity of the MLRO and in his absence, the alternative MLRO.

3.2.5 The insurer shall ensure its employees are trained, on an ongoing basis to ensure adequate awareness and understanding of the insurer's AML/CFT statutory and regulatory requirements as well as its internal AML/CFT procedures and programmes.

4 REPORTING OF SUSPICIOUS TRANSACTIONS

4.1 Section 26 of the Bank Use Promotion and Suppression of Money Laundering Act imposes obligations on designated institutions, including insurers, to report suspicious transactions to the Unit.

4.2 A designated institution shall draft and submit an STR to the Unit, if it has reasonable grounds for believing that the transaction, including an attempted transaction or activity, involves proceeds of crime;

4.3 The STR shall be submitted to the Unit promptly and in any case within 3 working days of identification of the suspicious transaction.

4.4 STRs, shall be reported to the Unit using the STR Template provided as **Annexure 1.**

4.5 Information in the STR shall include -

(a) the nature and amount involved in the transaction; and
(b) the name of the customer and any other relevant parties to the transaction; and
(c) reasons for regarding the transaction as suspicious;
(d) the name of the MLRO or other officer who prepared the report;

4.6 The insurer shall retain a copy of every STR submitted to the Unit;

4.7 Where a transaction is uncompleted or abandoned/ aborted by the customer or prospective customer on being asked to furnish further documents or information shall be reported to the Unit as suspicious irrespective of the amount involved.

4.8 In determining whether a transaction is suspicious, the insurer and its employees are expected to exercise reasonable judgment. The following are examples / indicators of suspicious transactions. The list is by no means exhaustive;

- the purchase of an insurance product inconsistent with the customer's needs;

- unusual payment methods, such as cash, cash equivalents (when such a usage of cash or cash equivalents is unusual), or structured monetary instruments;
- early termination of a product for no obvious reason, especially at a cost to the customer;
- where payment is made by, or any refund cheque is requested to be directed to an apparently unrelated third party;
- the transfer of the benefit of a product to an apparently unrelated third party;
- a customer who shows little concern for the investment performance of a product, but a great deal of concern about the early termination features of the product;
- a customer who is reluctant to provide identifying information when purchasing a product, or who provides minimal or seemingly fictitious information;
- a customer who borrows the maximum amount available soon after purchasing the product.

NB: The above list is only an indicative, and not exhaustive.

4.9 Where an STR is filed or contemplated, the insurer or any of its employees or agents shall not disclose this fact to the customer or any third party other than to the Unit or to any other competent authority entitled at law to such information.

4.10 In terms of section 28 (2), no employee shall be liable to any legal, administrative or employment related sanction, regardless of any breach of a legal or employment obligation, for reporting any information concerning a suspicious transaction to the Unit in good faith.

4.11 The insurer shall make it a requirement for its employees to report to the MLRO any violations of the insurer's AML/CFT compliance program.

4.12 Where the violations involve the MLRO, the insurer shall ensure there is a mechanism to allow employees, regardless of their rank, to report the violation to an authority above the MLRO.

5 MAINTENANCE OF RECORDS OF TRANSACTIONS

5.1 Sections 25 of the Bank Use Promotion and Suppression of Money Laundering Act imposes obligations on designated institutions to record and maintain customer information and transactions details.

5.2 The insurer shall take all steps and shall introduce a record keeping system to record transactions and maintain records as prescribed under this requirement.

5.3 Information maintained in respect of transactions shall permit reconstruction of individual transactions.

5.4 Some of the customer and transaction information to be recorded and maintained include the following:

(a). identity of the customer and beneficiaries, i.e. parties to the transaction;
(b). the nature of the transaction;
(c). the amount in and the currency involved in the transaction;
(d). source of funds;
(e). the type and identifying number of account involved in the transaction;
(f). the date on which the transaction was conducted;

5.5 The insurer shall take appropriate steps to employ a system that allows data to be retrieved easily and quickly whenever required or when requested by competent authorities.

5.6 The records shall be kept for at least **five years** from the date of termination of a business relationship or, in the case of an occasional transaction, within five years from the date of completion of the transaction.