



Subject: **Money Laundering and Financing of Terrorism & Proliferation
Financing (Prevention) Guideline (AML/CFT/PF/PF) 2024**

Number: **No. 1 of 2024**

Date: **April 2024**

Statutory Reference: **Section 18bis (2) of the Money Laundering and Financing of
Terrorism (Prevention) Act, 2011 [as Amended]**

Scope:

**Central Securities Depositories, Credit Bureaus, Dealers,
Retirement Funds Administrators, Dealer Representatives,
Insurance Agents, Insurance Brokers, Insurers, Investment
Advisor Representatives, Nominees, SACCOS, Retirement
Fund Trustees, Securities Exchanges, and any other Non- Bank
Financial Services Provider as specified in all non-bank
financial services laws as amended from time to time.**

PART 1 – SCOPE, PURPOSE AND APPLICATION.....	6
1. DEFINITIONS	6
2. INTRODUCTION	7
3. APPLICABILITY AND SCOPE	8
4. KEY CONCEPTS OF THE GUIDELINE	8
4.1 Money Laundering.....	9
4.2 Financing of Terrorism	9
4.3 Financing of Proliferation of Weapons of Mass Destruction	9
4.4 Risk Management	10
4.5 Accountable Institution.....	10
4.6 Risk-Based Approach	11
4.7 The effect of a risk-based approach	11
4.8 Risk-Based AML/CFT/PF Compliance Programmes.....	11
4.9 What is risk?	12
4.10 Risk Mitigation	12
4.11 Risk-mitigation measures.....	13
5. RISK MANAGEMENT FRAMEWORK	13
5.1 What is the purpose of a risk assessment?	13
5.2 Whose responsibility is it to undertake a risk assessment?.....	14
5.3 How often should a risk assessment take place?	14
6. RISK INDICATORS	15
7. SOURCES OF INFORMATION FOR THE RISK ASSESSMENT	16
7.1 Sources of Information	16
7.2 ML/TF Risk Assessments	16
8. GOVERNANCE.....	17
8.1. Structure.....	17
8.2. Role of the Board	17
8.3. Key responsibilities of the Board include:	17
8.4. Role of Senior Management.....	18
8.5. Vetting and Recruitment of Compliance Officer	19
8.6. Appointment and Responsibilities of the Compliance Officer	20
9. CONFLICT OF INTEREST.....	20

PART II – CUSTOMER DUE DILIGENCE.....	22
10. CUSTOMER DUE DILIGENCE.....	22
10.1. When CDD is required?	22
10.2. Required CDD measures for all customers	23
10.3. Specific CDD measures required for legal persons and legal arrangements.....	24
10.4. CDD for Beneficiaries of Life Insurance Policies.....	25
10.5. Timing of verification.....	26
10.6. Existing customers.....	26
10.7. Risk-Based Approach	26
10.8. Failure to satisfactorily complete CDD	26
10.9. CDD and tipping-off.....	26
10.10. Anonymous or Fictitious persons	27
10.11. Ongoing Monitoring.....	27
10.12. Non-Face-to-Face Verification.....	28
10.13. Simplified Customer Due Diligence.....	28
11. ENHANCED CUSTOMER DUE DILIGENCE	29
11.1 When EDD is required?	29
11.2 Examples of EDD Measures:	30
11.3 High-Risk Jurisdictions/Countries	31
11.4 Enhanced Monitoring.....	32
11.5 Politically Exposed Persons	32
11.6. PEPs Enhanced Customer Due Diligence	33
11.7. Reliance on Third Parties	34
11.8. Reviewing and Updating the Customer Due Diligence Information	35
11.9. Reliance on Third Parties to Undertake CDD	35
PART III – DUTY TO MAINTAIN PROPER RECORDS	36
12. RECORD KEEPING	36
12.1. Obligation to keep customer due diligence records.....	37
12.2. Obligation to keep transaction records	37
12.3. Manner in which records must be kept.....	37
12.4. Customer Due Diligence Records	38
12.5. Transaction records.....	38

PART IV – KNOW YOUR EMPLOYEE	39
13. KNOW YOUR EMPLOYEE.....	39
14. TRANSACTION MONITORING	40
15. SUSPICIOUS TRANSACTION REPORTING	40
16. TIPPING-OFF AND CONFIDENTIALITY	41
17. TRAINING.....	42
18. AUDIT AND SELF-ASSESSMENT OF CONTROLS	42
19. INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES.....	43
PART V – FINAL PROVISIONS	43
20. UNITED NATIONS SECURITY COUNCIL RESOLUTIONS.....	43
20.1. Effective Client Screening.....	44
20.2. Where to find the updated Sanctions Lists?	45
20.3. Targeted Financial Sanctions (TFS).....	45
20.4. Asset freezing without delay	45
21. SANCTIONS FOR NON-COMPLIANCE WITH THE GUIDELINE	46
22. GUIDANCE AND FEEDBACK	46
Appendix A - Examples of Suspicious Transactions	47

LIST OF ABBREVIATIONS

AML	Anti-Money Laundering
AML/CFT/PF /PF	Anti Money Laundering and Combating the Financing of Terrorism & Proliferation Financing
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CTR	Cash Threshold Reporting
DNFBPs	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
EFIU	Eswatini Financial Intelligence Unit
FATF	Financial Action Task Force
FSRA	Financial Services Regulatory Authority
FSRA Act	Financial Services Regulatory Authority Act, 2010
FSP	Financial Services Provider
FT/TF	Financing of Terrorism/ Terrorism Financing
IAIS	International Association of Insurance Supervisors
IOPS	International Organization of Pension Supervisors
IOSCO	International Organization of Securities Commissions
KYC	Know your customer
KYE	Know your employee
MER	Mutual Evaluation Report
ML	Money Laundering
MLFTP Act	Money Laundering and Financing of Terrorism (Prevention) Act, 2011 (as amended)
NRA	National Risk Assessment
PEP	Politically Exposed Persons
PF	Proliferation Financing
RBA	Risk Based Approach
STR	Suspicious Transaction Report
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UNSCR	United Nations Security Council Resolutions
VAT	Value Added Tax

PART 1 – SCOPE, PURPOSE AND APPLICATION

1. DEFINITIONS

For purposes of this Guideline, unless the context otherwise requires:

“Accountable Institution” means an institution as listed in Schedule 3 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 (as amended), .

“Authority” means the Financial Services Regulatory Authority as established by the Financial Services Regulatory Authority Act, 2010.

“Beneficial owner” means a person or persons who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted and includes those persons who exercise effective control over a legal person or arrangement.

“Business relationship” means any arrangement or proposed arrangement between a person and an Accountable Institution where;

- a. the purpose or effect of the arrangement is to facilitate an occasional frequent, habitual, or regular course of dealing between the person and the institution; and the;
- b. the total amount of payment to be made by any person to any other in the course of that arrangement is not known or capable of being ascertained at the time the arrangement is made.

“Customer” means in relation to a transaction or an account includes;

- a) The person in whose name a transaction or account is arranged, opened, or undertaken;
- b) A signatory to a transaction or account;
- c) Any person to whom a transaction has been assigned or transferred;
- d) Any person who is authorized to conduct a transaction; or
- e) Such other person as the Minister may by Notice published in the gazette prescribe.

“Customer Due Diligence” means a process that involves establishing the identity of a client, the identity of the client's beneficial owners in respect of legal persons and monitoring all transactions of the client against the client's profile.

“Enhance Due Diligence” refers to additional due diligence measures that must be applied where the customer has not been physically present for identification; where the customer is politically exposed or in any situation which by its nature can present a higher risk of money laundering or

terrorism financing. These measures should apply to all higher-risk business relationships, customers, and transactions.

“Financial Crime” includes–

- a) a crime that involves fraud or dishonesty relating to a financial service provider;
- b) financing or facilitating crime relating to a financial service provider;
- c) dealing with the proceeds of crime, whether or not related to a financial service provider;
- d) money laundering or
- e) financing terrorism.

“Non-Bank Financial Services Provider” – means any person mentioned in the second schedule of the FSRA Act, 2010 and/or prescribed in any non-bank financial services law in the first schedule of the FSRA Act, 2010; or its successor.

“Politically Exposed Person” means a person who holds, or has held, a prominent public position, whether in Eswatini or a foreign country, including, but not limited to, a Head of State or Government; a politician at a national level; a senior Government official, judicial, military or party official at the national level; a senior executive of a state-owned enterprise, persons who are or have been entrusted with a prominent function by international organizations; or an individual or entity identified as having close family ties or personal or business connections to any of the aforementioned persons, an international organization; senior official and their close associates; an individual or undertaking identified as having family or personal or business connections close to such International Organisation senior official.

“Proliferation Financing” means 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 goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations

2. INTRODUCTION

2.1. This Guideline is issued in terms of Section 18bis of the MLFTP, 2011 (as amended). It has been amended pursuant to the findings of the Eswatini MER, June 2022, and the FATF Recommendations which requires that an Accountable Institution adopts a Risk-Based Approach (RBA) in its overall management of risks they are exposed to. The RBA starts with conducting risk assessments at institutional level which should be informed by observations at sectoral and national risk assessment levels, trends, and typologies of ML, TF, and PF, amongst others.

2.2.It is common cause that services offered by an Accountable Institution has been abused for ML domestically. Internationally, there are trends and typologies that suggest abuse to advance TF/PF activities. To mitigate ML/TF/PF risks, the Authority issues this Guidance to help Accountable Institutions implement and enhance their internal Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation (AML/CFT/PF/CPF) measures, at institutional level.

2.3.Money laundering, terrorism financing and proliferation financing (ML/TF/PF) risk management continues to be a priority global threat which can adversely affect a country's reputation and lead to multiple negative economic and social consequences, such as de-risking.

The guidance must, therefore, be read together with –

- a) The Money Laundering and Financing of Terrorism (Prevention) Act 2011 (as amended) (MLFTP, Act) (which sets out in detail the AML/CFT/PF statutory obligations of Accountable Institutions and DNFBPs);
- b) All current directives or circulars issued under the MLFTP Act and its regulations. In the event of any conflict between what is set out in this Guideline and what is set out in the MLFTP Act or any applicable law, the relevant legal provision prevails. The Guideline reflects the shift from a previous rule-based, “tick-box” approach, to a risk-based approach (RBA) to combating money laundering and financing of terrorism.

2.4.The rule-based approach, which was enforced before 2012, required Accountable Institutions and DNFBPs to implement AML/CFT/PF obligations uniformly in respect of all customers, to all transactions, and all situations, regardless of the level of money laundering or terrorism financing risk.

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

3. APPLICABILITY AND SCOPE

3.1 This Guideline applies to all Accountable Institutions as defined in the Act that are under the supervision of the Authority.

4. KEY CONCEPTS OF THE GUIDELINE

4.1 Money Laundering

4.1.1 Money laundering is a process in which funds or property believed to be obtained directly or indirectly through illegal or criminal activities are converted into other assets to conceal their true origin or ownership. The main objective is to legitimize income originating from illegitimate sources so that it loses its criminal identity and appears to be legitimately derived. The process of money laundering comprises three stages, during which there may be numerous transactions that could alert a financial services provider to the money laundering activity:

- a) **Placement**—Physical disposal of criminal proceeds or placing dirty money into the financial system via a cash deposit, such as purchasing a policy using cash as opposed to using banking channels or offering top-up premiums, purchasing investments with cash, or repayment of an outstanding loan using dirty money.
- b) **Layering**—The separation of criminal proceeds from their source by the creation of layers of transactions designed to disguise the origin of funds and provide appearance of legitimacy, such as borrowing against an existing policy or an early surrender of an investment policy in circumstances where doing so defies economic logic.
- c) **Integration**—Placing the laundered proceeds back into the economy as apparently legitimate funds. For instance, with the proceeds from a surrendered insurance policy or redeemed shares or reimbursements, a launderer buys a “clean” or legitimate fixed asset or registers a legitimate business into which proceeds are deposited. The funds are then integrated back into criminal activities, such as drug trafficking.

4.2 Financing of Terrorism

4.2.1 The financing of terrorism is an unlawful act of directly or indirectly providing, whether by giving, lending, or otherwise making available or collecting, funds or property with the intention that they should be used, or used or having reasonable grounds to believe that they are to be used, in full or in part, to carry out an act of terrorism. Terrorism seeks to influence or compel governments or others into a particular course of action through the use of violence, damage to property, danger to life, or serious health risks. Terrorists require funds to carry out acts of terrorism, and terrorist financing provides the funds needed. The methods used by terrorists to move, collect, hide, or make available funds for their activities are similar to those used by criminals to launder their funds.

4.3 Financing of Proliferation of Weapons of Mass Destruction

4.3.1 The proliferation of weapons of mass destruction (WMDs) can take many forms but ultimately involves the transfer or export of technology, goods, software, services, or expertise that can be used in programs involving nuclear, biological, or chemical weapons, and their delivery systems (such as long-range missiles).

4.3.2 FATF Recommendation 7 places obligations on countries to comply with all United Nations Security Council Resolutions to apply targeted financial sanctions relating to the financing of the proliferation of weapons of mass destruction. The role of Accountable

Institutions is to implement controls to prevent access to financing by individuals and entities who may be involved in or supporting such proliferation. It is therefore required that financial service providers' AML/CFT/PF compliance programs include PF controls, such as screening against the applicable UNSCR lists of designated persons and countries.

4.4 Risk Management

- 4.4.1 The process of managing ML/TF/PF risks involves identifying, assessing, monitoring, managing, and mitigating the identified risks. Like other risks, ML/TF/PF risks can be controlled and reduced by treating, transferring, tolerating, or eliminating certain risks. Managing and mitigating ML/TF/PF risks will likely involve handling recognized risks inside an Accountable Institution.
- 4.4.2 To address ML/TF/PF risks, the Accountable Institution must create controls and procedures to handle the risks that have been recognized. All available risk mitigation techniques should be included in these systems and controls for the Accountable Institution. An Accountable Institution's risk management systems and controls should incorporate methods that are appropriate for the specific risks involved. These methods include the use of customer due diligence procedures, keeping an eye on client interactions, controlling the channels through which specific goods and services are delivered, organizing the features of specific goods and services, and so forth. The concepts of "ML/TF/PF risk" and "ML/TF/PF risk management" must always be contextualized within the particular business of an Accountable Institution, and as having an impact on the operational, line management, and strategic objectives of that Accountable Institution.

4.5 Accountable Institution

- 4.5.1 The application of risk management systems and controls must be commensurate with the extent of assessed risks. This means that the extent to which particular risk management mechanisms are applied in individual cases must bear relevance to the consequences of ML/TF/PF risk in particular scenarios in relation to the likelihood and impact of the risk.
- 4.5.2 The process of managing ML/TF/PF risk is a continuous cycle. An Accountable Institution should satisfy itself that its ML/TF/PF risk management systems and controls remain adequate in view of changing circumstances relating to emerging threats and vulnerabilities, product innovations, new target markets, changes in circumstances of individual clients or classes of clients, etc.
- 4.5.3 An Accountable Institution should also ensure that their ML/TF/PF risk management systems and controls are adhered to. This means that an Accountable Institution should reassess ML/TF/PF risks, in particular, residual risks after the application of ML/TF/PF risk management systems and controls, at regular intervals. The institutions should then review the continued adequacy of their ML/TF/PF risk management systems and controls based on these regular assessments.

4.6 Risk-Based Approach

- 4.6.1 The risk-based approach (RBA) is central to the effective implementation of the Financial Action Task Force (FATF) Recommendation 1 and the Money Laundering and Financing of Terrorism Prevention Act 2011 as amended. The focus on risk is intended to ensure that a Financial Service Provider (Accountable Institution) can identify, assess, and understand the ML/TF/PF risks to which it is exposed and take the necessary AML/CFT/PF control measures to mitigate those risks. Section 6 of the MLFTP Act requires an Accountable Institution to undertake an ML/TF/PF risk assessment to enable it to identify, assess, monitor, manage, and mitigate the risks associated with ML/TF/PF.
- 4.6.2 To execute an ML/TF/PF risk assessment, an Accountable Institution should take appropriate steps to identify and assess the ML/TF/PF risks related to customers, countries or geographic areas, products, services, transactions, and delivery channels. A risk assessment enables the Accountable Institution to focus its AML/CFT/PF efforts and to adopt appropriate measures to optimally allocate the available resources. The Accountable Institution should document the risk assessment process and keep the risk assessments up to date. The nature and extent of the ML/TF/PF risk assessment should be appropriate to the nature and size of the business undertaken by the Accountable Institution. An Accountable Institution should always understand its ML/TF/PF risks.

4.7 The effect of a risk-based approach

- 4.7.1 An Accountable Institution must make sure that the steps taken to stop or mitigate money laundering and terrorist funding are proportionate to the dangers that have been identified by using a risk-based approach. This will guarantee that resources are allocated according to priorities, giving the biggest dangers the most consideration. The risk-based approach also gives the Accountable Institution the freedom to employ a variety of techniques to confirm and authenticate the identities of their clients. This freedom allows the Accountable Institution to investigate more creative ways to provide financial services to a wider range of customers and reintegrate previously marginalized groups into the formal economy. This promotes financial inclusion and increases the effectiveness of counter-measures against money laundering, terrorist funding, and proliferation of weapons of mass destruction without compromising AML/CFT/PF goals.

4.8 Risk-Based AML/CFT/PF Compliance Programmes

- 4.8.1 Based on the risk assessment, the Accountable Institution should have policies, controls, and procedures that enable it to manage and mitigate effectively the risks that have been identified. An Accountable Institution should monitor the implementation of those controls and enhance them, if necessary. An Accountable Institution may differentiate the extent of mitigation measures, depending on the type and level of risk for the various risk factors. The Accountable Institution's management should decide the appropriate method or format, based on the Accountable Institution's particular risk profile. Whatever format management chooses to use for its risk assessment, it should be relevant and easily understood by all stakeholders.

4.9 What is risk?

4.9.1 Risk can be seen as a function of three factors: threat, vulnerability, and consequence. An ML/TF/PF risk assessment is a product or process based on a methodology, agreed upon by those parties involved, that attempts to identify, assess, and understand ML/TF/PF risks and serves as a first step in addressing them. Ideally, a risk assessment involves making judgments about threats, vulnerabilities, and consequences.

- a) **Threat** – a person or group of people, objects, or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF/PF context, this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present, and future ML/TF/PF activities. Threat is described above as one of the factors related to risk, and typically it serves as an essential starting point in developing an understanding of ML/TF/PF risk.
- b) **Vulnerabilities**- are the intrinsic properties in a system or structure (including weaknesses in systems, controls, or measures) that make it open to abuse or exploitation by criminal elements for ML/TF/PF. The existence of vulnerabilities in a system makes that system attractive for money launderers and terrorist financiers to use.
- c) **Consequence**- refers to the impact or harm that ML/TF/PF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of ML/TF/PF may be short or long-term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector.

4.10 Risk Mitigation

4.10.1 Once the risks have been identified, an Accountable Institution must have policies, procedures, and controls to enable them to manage and mitigate effectively the risks that have been identified. They are required to monitor the implementation of those controls and to enhance them, if necessary. The policies, procedures, and controls must be approved by the Board, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with the MLFTP Act and its Regulations.

4.10.2 The RBA is not a “zero-risk approach” – the Accountable Institution should nevertheless understand that a risk-based approach is not a justification for ignoring certain ML/TF/PF risks, nor does it exempt the Accountable Institution from taking reasonable and proportionate mitigation measures, even for risks that are assessed as low. The statutory obligations require the Accountable Institution to identify, assess, and understand the level of risk and to be in a position to always apply sufficient AML/CFT/PF mitigation measures on a risk-appropriate basis. The risk-based approach is not a “zero failure” approach as there may be occasions where an institution has taken all reasonable measures to identify and mitigate ML/TF/PF risks, but it is still exploited for money laundering or terrorist financing purposes.

4.10.3 An Accountable Institution should use the customer due diligence process as one of the measures to mitigate the ML/TF/PF risk associated with a proposed business relationship or single transaction. The customer due diligence process provides an Accountable Institution with the information required to know who they are doing business with, to know who benefits from the business it does with its clients, to understand the nature of the business it does with its clients and to determine when the business with customers should be considered suspicious or unusual. This is one of the mechanisms the Accountable Institution has to mitigate the risk of exploitation for money laundering or terrorist financing purposes.

4.11 Risk-mitigation measures

4.11.1 Measures that may be applied in cases of higher ML/TF/PF risk:

- a) Increased automated transaction monitoring;
- b) Increased intensity of CDD measures;
- c) Increased review periods of customer information;
- d) Utilizing more or higher quality sources for the vetting of information (impacts both quality and quantity);
- e) Senior management involvement in decisions to on-board customers;
- f) Mandatory site visits;
- g) Dedicated specialist staff managing enhanced due diligence for specific clients;
- h) Limited reliance on another Accountable Institution's controls.

5. RISK MANAGEMENT FRAMEWORK

The risk management framework is a process used to identify the potential threats to an organization and to define the policies and procedures to eliminate or minimize the threats, as well as develop a strategy or guideline to monitor and review those identified risks.

5.1 What is the purpose of a risk assessment?

5.1.1 The key purpose of an ML/TF/PF risk assessment is to drive improvements in ML/TF/PF risk management by identifying the general and specific ML/TF/PF risks an Accountable Institution is facing, determining how these risks are mitigated by the AML/CFT/PF program controls, and establishing the residual risk that remains for the Accountable Institution.

5.1.2 The results of a risk assessment can support the Accountable Institution in many ways, including among others:

- a) identify gaps or opportunities for improvement in AML/CFT/PF policies, procedures, and processes;
- b) contribute to the demonstrable achievement of objectives and improvement of performance, governance, and reputation of the Accountable Institution;
- c) help decision-makers of the Accountable Institution to make informed choices, prioritize actions, and distinguish among alternative courses of action;
- d) help in explicitly taking account of uncertainty, the nature of that uncertainty, and how it can be addressed by the Accountable Institution;
- e) assist the Accountable Institution in making informed decisions about risk appetite and implementation of control efforts, allocation of resources, and technology spending;
- f) support the Accountable Institution in ensuring that regulators are made aware of the key risks, control gaps, and remediation efforts across the Accountable Institution.

5.2 Whose responsibility is it to undertake a risk assessment?

5.2.1 The Board of Directors is ultimately responsible for risk management within the Accountable Institution. The board of directors and senior management of an Accountable Institution are expected to formulate and implement an ML/TF/PF risk assessment framework. The risk assessment must be documented and made available for analysis by the FSRA. The board of directors should have a clear understanding of ML/FT/PF risks. Information about ML/FT/PF risk assessment should be communicated to the board in a timely, complete, understandable, and accurate manner so that it is equipped to make informed decisions.

5.2.2 It should be noted that, while the Board of the Accountable Institution may delegate the risk assessment process, the ownership of the risks remains with the operational business units, who are responsible for carrying out any actions resulting from the gaps or deficiencies identified by the risk assessment exercise. Hence the contribution required from each party should be clearly outlined. The Accountable Institution should also ensure that timely and appropriate training and guidance is provided to staff members involved in the completion of the risk assessment to ensure that a consistent approach is taken.

5.3 How often should a risk assessment take place?

5.3.1 An Accountable Institution is obliged to create, maintain, and update regularly a record of actions taken pursuant to conducting a risk assessment. The frequency of the risk assessment will depend upon many factors including the development of new products, product enhancements, business practices, delivery channels, the use of new or developing technologies, the methodology employed, the validation process, audit reviews, the results of the previous risk assessment, and changes in applicable laws and regulations. A risk assessment should be reviewed at least annually or more frequently due to internal trigger events.

6. RISK INDICATORS

6.1. Factors that may be indicative of ML/TF/PF risks relate to many aspects such as product or service features, new technology, delivery channels, and geographic areas. Each of these may interact differently with the characteristics of different types of clients. The examples of factors that may be indicative of ML/TF/PF risk provided here are not an exhaustive or prescriptive list and Accountable Institutions also have to consider other factors that may be relevant to their organisations or sectors. Furthermore, the examples provided here are phrased in neutral terms, a factor may be indicative of either higher or lower ML/TF/PF risk depending on the context within which it is considered. It is important therefore that Accountable Institutions can demonstrate how they bring different indicators to bear on a given scenario to reach an appropriate risk classification.

6.2. In relation to the products, new technologies, services, transfers, and delivery channels of the Accountable Institution:

- 6.2.1. Nature, scale, diversity, and complexity of the business activities including its geographical diversity of the Accountable Institution, nature of products and services offered by the Accountable Institution;
- 6.2.2. The delivery channel refers to how institutions and clients interact with each other in the offering of products and services, on-boarding of clients, and the usage of products and services. It is trite that not all clients of an Accountable Institution pose the same ML/TF/PF risk. For an Accountable Institution to accurately identify all the factors that may be relevant to a particular client and to include all those factors in an assessment of ML/TF/PF risks, the institution must have a holistic view of the information gathered about the client across all the points of engagement between the institution and the client. This implies that an Accountable Institution that offers a range of products and services should consider the different engagements with a particular client in relation to different products and services as parts of one relationship with that client and assess the ML/TF/PF risks relating to that relationship in a holistic manner
- 6.2.3. the degree to which the operations are outsourced to other entities in the Group or third parties; and
- 6.2.4. the development of new products and new business practices, including new delivery mechanisms and partners; or the use of new or developing technologies for both new and pre-existing products.

6.3. An assessment of ML/TF/PF risks relating to clients could entail an assessment for each client or group of clients fitting the same profile. Where an Accountable Institution evaluates the characteristics of a group of clients as part of a risk assessment, the institution should ensure that any individual client to whom the characteristics of the group are ascribed meets the profile of that group.

6.4. In addition to the characteristics of products and services, new technologies, delivery channels, geographic locations, and clients mentioned above there are also other factors that institutions should take into account when assessing ML/TF/PF risks. These are contextual factors which, on the one hand, relationships or to a more accurate assessment of ML/TF/PF risks in relation to particular business relationships or categories of relationships or assist in determining an institution's risk appetite in relation to particular business relationships or categories of relationships, on the other.

7. SOURCES OF INFORMATION FOR THE RISK ASSESSMENT

7.1 Sources of Information

When conducting or updating risk assessments, Accountable Institutions should consider information obtained from relevant internal and external sources, such as:

- a) The Accountable Institution's heads of business lines and relationship managers;
- b) Internal/external audit and regulatory findings;
- c) Sectoral emerging risks and typologies;
- d) Corruption indices and country risk reports;
- e) Guidance issued by regulators;
- f) Threat reports and typologies issued by the FIU and law enforcement agencies;
- g) National risk assessment reports;
- h) Independent and public assessment of a country's or jurisdiction's overall AML/CFT/PF regime such as Mutual Evaluation Reports, IMF Financial Sector Assessment Program Reports, or Reports on the Observance of Standards and Codes; and
- i) Public sources of adverse news or relevant public criticism of a country or jurisdiction, including FATF, ESAAMLG, and FATF Style Regional Bodies public statements.

7.2 ML/TF Risk Assessments

There is no single prescribed or universally accepted methodology for conducting an AML/CFT/PF risk assessment. A risk assessment should consist of two distinct but related steps:

- a) Identification of ML/TF/PF risk,
- b) Assessment of the ML/TF/PF risk and the likelihood that the Accountable Institution will be used for ML/TF/PF;
- c) Mitigation measures;
- d) Monitoring; and
- e) Manage

8. GOVERNANCE

8.1. Structure

8.1.1. For the AML/CFT/PF framework of any Accountable Institution to be effective, it must be based on the foundation of a sound governance structure and held together by a strong compliance culture. This includes appropriate management structures that are accountable for clear ML/TF/PF risk management and mitigation measures, as well as appropriate independent control functions. It is therefore imperative that the board and senior management of an Accountable Institution ensure that the policies, procedures, systems, and processes put in place to prevent ML/FT are appropriate. The AML/CFT/PF program of an Accountable Institution should be risk-based and commensurate with the nature, size, complexity, and inherent risks of the Accountable Institution.

8.2. Role of the Board

8.2.1. The Board of Directors of an Accountable Institution has oversight and accountability for the AML/CFT/PF compliance program and monitoring the effectiveness of the AML/CFT/PF Risk Management and Compliance Program regularly. It is the responsibility of the Board to ensure compliance by an Accountable Institution and its employees with the provisions of the MLTFP Act and the AML/CFT/PF Risk Management and Compliance Program.

8.2.2. The Board should further align its governance and oversight practices with the FSRA Act, 2010, and sector-specific legislation under the regulatory ambit of the FSRA.

8.3. Key responsibilities of the Board include:

- a) Approving the AML/CFT/PF compliance program including all AML/CFT/PF policies;
- b) Ensuring the establishment of appropriate mechanisms to periodically review key AML/CFT/PF policies to ensure their continued relevance in line with changes in the products and services and to address new and emerging ML/TF/PF risks of the Accountable Institution;
- c) Ensuring the establishment of an appropriate AML/CFT/PF risk management framework with clearly defined lines of authority and responsibility for AML/CFT/PF and effective separation of duties between those implementing the policies and procedures and those enforcing the controls;
- d) Ensuring that the Board receives the requisite training on AML/CFT/PF generally as well as on the Accountable Institution's specific AML/CFT/PF risks and controls;

- e) Ensuring receipt of regular and comprehensive management information and reports on the AML/CFT/PF risks from the Compliance Officer and or senior management or board committees of the Accountable Institution.

8.4. Role of Senior Management

8.4.1. Senior Management is responsible and accountable for the day-to-day implementation and management of the AML/CFT/PF Compliance Program. Senior Management has to ensure that it is adequate to mitigate ML/TF/PF risks and that it is implemented effectively in all relevant business areas, including ensuring adherence to established AML/CFT/PF policies and procedures.

8.4.2. Senior Management should ensure that:

- a) policies and procedures are risk-based, proportional, and adequate to mitigate ML and TF risks of the Accountable Institution;
- b) The Accountable Institution complies with all relevant AML/CFT/PF laws, regulations and guidelines;
- c) are implemented effectively across relevant business areas or throughout the financial group as applicable;
- d) review policies and procedures periodically for consistency with the business model, product and service offerings, and risk appetite of the Accountable Institution;
- e) Senior Management must review policies and procedures periodically for consistency with the business model, product and service offerings, and risk appetite of the Accountable Institution. Attention should be paid to new and developing technologies and Accountable Institutions should identify and assess the ML/FT/PF risks arising from new products, services and delivery channels; new business practices and new or developing technologies for new and existing products; and put measures in place to manage and mitigate such risks;
- f) Risk assessments take place before the launch or use of such products, services, channels, business practices, and technologies;
- g) All significant recommendations made by internal and external auditors and regulators in respect of the AML/CFT/PF program are acted upon in a timely manner;
- h) Relevant, adequate, and timely information regarding AML/CFT/PF matters is provided to the Board;
- i) There is an ongoing employee training program that enables employees to have sufficient knowledge to understand and discharge their AML/CFT/PF responsibilities.

8.5. Vetting and Recruitment of Compliance Officer

- 8.5.1. Senior Management and/or the Board should ensure that an appropriately qualified person of sufficient competence and seniority is appointed as a Compliance Officer;
- a) Accountable institutions are to apply for approval prior to the appointment of the Compliance Officer; provided that such application is accompanied by a detailed curriculum vitae of the Compliance Officer and a full description of the duties of the Compliance Officer;
 - b) the Compliance Officer must be a resident of Eswatini;
 - c) the Authority is informed in writing of the termination of services of a Compliance Officer and provided with an explanation of the reasons for the termination, within 15 days of such termination;
 - d) the Compliance Officer is a member of Senior Management or reports directly to Senior Management or the Board of Directors and does not report to the internal auditor to avoid potential conflicts of responsibilities;
 - e) the Compliance Officer has clear and documented responsibility and accountability for designing the AML/CFT/PF Risk Management and Compliance Program ensuring that the Accountable Institution assesses the risk of ML/TF/PF it may expect to face in the course of its business and uses the results of the risk assessment in designing the AML/CTF Risk Management and Compliance Program.
 - f) the Compliance Officer and the internal auditor have adequate resources in terms of people, data management systems, and budget to implement and administer the AML/CFT/PF Risk Management and Compliance Program effectively and to offer objective advice to the Board and Senior Management; and;
 - g) any recommendations made by the Compliance Officer, the internal auditor, and Senior Management in respect of the AML/CFT/PF Risk Management and Compliance Program are acted upon in a timely manner.
 - h) ensure that there is a robust and effective independent audit function in place to ensure the adequacy and effectiveness of the AML/CFT/PF compliance program.
 - i) Senior Management should further ensure that they receive sufficient pertinent information from the Compliance Officer, the internal auditor, and other sources, as appropriate, to enable them to ensure the overall adequacy and effectiveness of the AML/CFT/PF Risk Management and Compliance Program.

8.6. Appointment and Responsibilities of the Compliance Officer

- 8.6.1. For purposes of ensuring compliance with Section 18 of the MLFTP Act, an Accountable Institution must appoint a Compliance Officer with the appropriate seniority status, relevant qualifications, and experience to perform the statutory duties and responsibilities associated with this role, including keeping abreast of the latest developments in ML/FT/PF techniques and the AML/CFT/PF best practices within the industry. The Compliance Officer must have sufficient authority, independence, and seniority to be able to effectively carry out his duties in accordance with the MLFTP Act. The Compliance Officer must be approved by the FSRA before assuming his or her responsibilities.
- 8.6.2. This individual is responsible for creating, deploying, and organizing AML systems and controls. In addition, they report to state and federal authorities in the event of suspicious activity or financial crimes. Where an Accountable Institution does not employ more than five (5) employees, the most senior employee shall be the Compliance Officer. The Compliance Officer has the overall responsibility for the implementation of the enterprise-wide AML/CFT/PF compliance program.
- 8.6.3. The nature of the reporting line of the Compliance Officer – the Compliance Officer should have a direct reporting line to the Board of Directors (or relevant Committee of the Board) of the Accountable Institution. For smaller Accountable Institutions where independence may not be practical, that Accountable Institution must consider the administrative reporting lines of the Compliance Officer. Ultimately, the Accountable Institution must be able to demonstrate the independence of the Compliance Officer in instances where practically, independence cannot be achieved functionally.

9. CONFLICT OF INTEREST

- 9.1. Potential conflicts of interest between the Compliance Officer's responsibilities and any other responsibilities that the Compliance Officer may have – Ideally, the Compliance Officer should not have any other responsibilities than that of AML/CFT/PF compliance. However, where this is not feasible, the Accountable Institution should make appointments that as far as possible, avoid conflicts of interest.
- 91.1. The responsibilities of the Compliance Officer should, among others, include the following:
 - a) have oversight of the AML/CFT/PF control activity in all relevant business areas to establish a reasonable level of consistent control throughout the Accountable Institution.

- b) conducting, on an on-going basis, the AML/CFT/PF 's risk assessment on the Accountable Institution in a timely manner; including timely assessments of new products, services, and new technologies and developing appropriate control mechanisms. The risk assessment should be documented and approved by the Board and reviewed on an on-going basis.
- c) developing a risk-based AML/CFT/PF Risk Management and Compliance Program that is current and relative to the identified inherent risks of the Accountable Institution; and, considering Eswatini and international developments in ML/TF;
- d) the Compliance Officer is the suspicious transaction reporting officer of the Accountable Institution. The Compliance Officer must ensure that systems resources, including those required to identify and report suspicious transactions and suspicious attempted transactions, are appropriate and adequate for the Accountable Institution. The Compliance Officer is further responsible for keeping a register of all reports received from staff and a separate register of all reports made to the EFIU;
- e) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorism financing is suspected;
- f) develop written AML/CFT/PF policies and procedures that are kept up to date and approved by the Board;
- g) responsible for establishing and maintaining a strong and effective AML/CFT/PF training program that is current, relevant, and undertaken by all employees, senior management, and the Board to ensure that staff members are well-qualified, well-trained, well-equipped, and well-aware of their responsibility to combat the threat posed by ML/TF/PF.
- h) ensuring that the Accountable Institution conducts on-going monitoring of transactions and high-risk customers in compliance with this Guideline and the MLFTP Act;
- i) ensuring that systems resources, including those required to identify and report suspicious transactions and attempted suspicious transactions are appropriate in all relevant areas of the Accountable Institution;
- j) promoting compliance with this Guideline, including observation of the underlying principles of AML/CFT/PF and taking overall charge of all AML/CFT/PF matters within the Accountable Institution;
- k) formulate and implement appropriate policies, procedures, and controls with regard to staff screening.
- l) acting as a liaison officer between the Accountable Institution, the Authority, and the EFIU in matters relating to compliance with the provisions of the MLFTP Act and any other law or directive with respect to ML/TF;
- m) conducting periodic assessments of AML/CFT/PF control mechanisms to ensure their continued relevance and effectiveness in addressing changing ML/TF risks,

assessing operational changes, including the introduction of new technology and processes to ensure that ML/TF risks are addressed;

- n) Ensuring that management information is received by the relevant governance forums of the Accountable Institution, ensuring that systems and other processes that generate information used in reports to senior management and the Board are adequate, appropriate and that they generate accurate information; and
- o) Report pertinent information to the Board and senior management in a timely manner regarding the adequacy of the AML/CFT/PF framework or any associated ML/TF issues.
- p) The reports from the Compliance Officer should include information on significant patterns or trends, self-assessment of controls and material changes thereto, as well as remedial action plans or recommendations, if any, with milestones and target dates for completion.
- q) Where appropriate, the Compliance Officer should draw conclusions, offer advice, and make recommendations about the overall structure and scope of the AML/CFT/PF Risk Management and Compliance Program.

PART II – CUSTOMER DUE DILIGENCE

10. CUSTOMER DUE DILIGENCE

10.1. When CDD is required?

10.1.1. Accountable Institutions shall undertake CDD measures when:

- a) establishing business relations;
- b) carrying out occasional transactions above the applicable designated threshold (E 25 000), (Twenty Five Thousand Emalangen) including situations where the transaction is carried out in a single operation or in several operations that appear to be linked;
- c) carrying out occasional transactions that are wire transfers in the following circumstances:
 - i. cross-border wire transfers: Information accompanying all qualifying wire transfers should always contain: the name of the originator; the originator account number where such an account is used to process the transaction; the originator's address, or national identity number, or customer identification number, or date and place of birth; the name of the beneficiary; and the beneficiary account number where such an account is used to process the transaction.
 - ii. domestic wire transfers: Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means.

- d) there is a suspicion of ML/TF/PF,
- e) the Accountable Institution has doubts about the veracity or adequacy of previously obtained customer identification data.

10.2.Required CDD measures for all customers

10.2.1. An Accountable Institution shall be required to identify the customer (whether permanent or occasional, and whether a natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data, or information (identification data). Provided that, in verifying a natural person's identity, an Accountable Institution shall require, among others, the following documents:

- 10.2.1.1. Full legal names used, including aliases;
- 10.2.1.2. Occupation;
- 10.2.1.3. Public position held and name of employer (if self-employed, the nature of self-employment);
- 10.2.1.4. Specimen signature;
- 10.2.1.5. Residential Address;
- 10.2.1.6. Contact number;
- 10.2.1.7. Nationality;
- 10.2.1.8. Date and place of birth;
- 10.2.1.9. Copy of National Identity Card.

10.2.2. An Accountable Institution shall be required to verify that any person purporting to act on behalf of the customer is so authorized and identify and verify the identity of that person.

10.2.3. An Accountable Institution is required to inquire if any beneficial owner exists in relation to a customer. Where there is one or more beneficial owners in relation to a customer, the Accountable Institution should take reasonable measures to obtain information sufficient to identify and verify the identity of the beneficial owner(s).

10.2.4. When an Accountable Institution establishes and verifies the identity of the beneficial owner of a legal person the institution must –

- a) identify and verify each natural person who, independently or together with a connected person, has a controlling ownership interest or ultimately owns the legal person; and
- b) if there is doubt as to whether a natural person contemplated in paragraph (a) is a beneficial owner of the legal person in question or where no natural persons ultimately owns the legal person, identify each natural person who ultimately controls the legal

person or who otherwise exercises executive control or management or similar position in the legal person.

10.2.5. An Accountable Institution shall be required to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the Accountable Institution is satisfied that it knows who the beneficial owner is.

10.2.6. An Accountable Institution shall understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship.

10.2.7. An Accountable Institution should be required to conduct ongoing due diligence on the business relationship, including:

- a) scrutinizing transactions undertaken throughout that relationship to ensure that the transactions being conducted are consistent with the Accountable Institution's knowledge of the customer, their business, and risk profile, including where necessary, the source of funds; and;
- b) ensuring that documents, data, or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.

10.3. Specific CDD measures required for legal persons and legal arrangements

10.3.1. For customers that are legal persons or legal arrangements, the Accountable Institution shall understand the nature of the customer's business and its ownership and control structure;

10.3.2. For customers that are legal persons or legal arrangements, the Accountable Institution shall identify the customer and verify its identity through the following information:

- a) name, legal form, and proof of existence;
- b) the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement; and
- c) the address of the registered office and, if different, a principal place of business.

10.3.3. For customers that are legal persons, the Accountable Institution shall identify and take reasonable measures to verify the identity of beneficial owners through the following information:

- a) the identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person; and

- b) to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and
- c) where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

10.3.4. For customers that are legal arrangements, the Accountable Institution shall identify and take reasonable measures to verify the identity of beneficial owners through the following information:

- a) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);
- b) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

10.4.CDD for Beneficiaries of Life Insurance Policies

10.4.1. In addition to the CDD measures required for the customer and the beneficial owner, an Accountable Institution shall conduct the following CDD measures on the beneficiary of life insurance and other investment-related insurance policies, as soon as the beneficiary is identified or designated:

- a) for a beneficiary that is identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;
- b) for a beneficiary that is designated by characteristics or by class or by other means – obtaining sufficient information concerning the beneficiary to satisfy the Accountable Institution that it will be able to establish the identity of the beneficiary at the time of the payout;
- c) for both the above cases – the verification of the identity of the beneficiary should occur at the time of the payout.

10.4.2. An Accountable Institution shall include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. Where the Accountable Institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it shall take enhanced measures which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

10.5. Timing of verification

An Accountable Institution shall verify the identity of the customer and beneficial owner before or during establishing a business relationship or conducting transactions for customers. Additionally, an Accountable Institution shall adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship before verification.

10.6. Existing customers

An Accountable Institution shall apply CDD requirements to existing customers based on materiality and risk and conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

10.7. Risk-Based Approach

An Accountable Institution shall perform enhanced due diligence where the ML/TF/PF risks are higher. Accountable Institutions may only apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the country or the Accountable Institution. The simplified measures should be commensurate with the lower risk factors but are not acceptable whenever there is suspicion of ML/TF/PF, or specific higher risk scenarios apply.

10.8. Failure to satisfactorily complete CDD

Where an Accountable Institution is unable to comply with relevant CDD measures:

- a) it shall not open the account, commence business relations or perform the transaction, or should be required to terminate the business relationship; and
- b) it shall be required to consider making a suspicious transaction report (STR) in relation to the customer.

10.9. CDD and tipping-off

In cases where an Accountable Institution forms a suspicion of money laundering or terrorist financing or proliferation financing, and reasonably believes that performing the CDD process will tip-off the customer, the Accountable Institution should be permitted not to pursue the CDD process, and instead should be required to file an STR.

10.10. Anonymous or Fictitious persons

An Accountable Institution should know its customers and shall not deal with any person on an anonymous basis, or any person using a fictitious name and should give special attention to the risks arising from new or developing technologies that may favour the anonymity of customers.

10.11. Ongoing Monitoring

- 10.11.1. An Accountable Institution should pay attention to all requested changes that occur after the business relationship has been established. The Accountable Institution should monitor on an ongoing basis their business relations with customers and should observe and assess the activity in respect of the customer and scrutinize transactions undertaken to ensure that they are consistent with the knowledge of the consumer, its business and risk profile and where appropriate and the sources of funds.
- 10.11.2. An Accountable Institution should pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent economic or lawful purpose. To the extent possible, the Accountable Institution should inquire into the background and purpose of all such transactions and document their findings to make this information available to the EFIU should the need arise.
- 10.11.3. Periodic reviews of customer identification information obtained should be done to ensure that the information is kept up to date, particularly for higher-risk categories of customers.
- 10.11.4. For ongoing monitoring, an Accountable Institution should put in place and implement adequate systems and processes, commensurate with the size, nature and complexity of the Accountable Institution, to;
 - a) monitor its business relations with customers; and
 - b) detect and report suspicious, complex, unusually large, or unusual patterns of transactions.
- 10.11.5. Where there are any reasonable grounds for suspecting that existing business relations with a customer are connected to money laundering or the financing of terrorism, and where the Accountable Institution considers it appropriate to retain the customer it should –
 - a) substantiate and document the reasons for retaining the customer; and
 - b) subject the Accountable Institution's business relations with the customer to enhanced risk mitigation measures, including enhanced on-going monitoring.

10.12. Non-Face-to-Face Verification

10.12.1. An Accountable Institution should put in place policies and procedures to address specific risks associated with non-face-to-face business relationships or transactions, which should be implemented when establishing business relations and transacting through instructions conveyed by customers over the post, telephone, or Internet.

10.12.2. Where there is no face-to-face contact, the Accountable Institution should use equally effective identification and verification procedures as those available for face-to-face customer acceptance, supplemented with specific and adequate measures to mitigate the higher risk. It is important to note that not all non-face-to-face business relationships will present higher risk.

10.12.3. As a guide, the following measures should be considered to mitigate the heightened risk associated with not being able to have face-to-face contact when establishing business relations:

- a) telephone contact with the customer at a residential or business number that can be verified independently;
- b) confirmation of the customer's address through an exchange of correspondence or another appropriate method;
- c) subject to the customer's consent, telephone confirmation of the customer's employment status with the customer's employer at a listed business number of the employer;
- d) confirmation of the customer's salary details by requiring the presentation of recent bank statements; and
- e) other reliable verification checks adopted by the Accountable Institution for non-face-to-face business.

10.13. Simplified Customer Due Diligence

10.13.1. Where the risks of money laundering and terrorism financing are lower, an Accountable Institution may apply simplified CDD measures. The simplified measures must have been identified through a risk assessment and should be commensurate with the lower risk factors having regard to the circumstances of each case. This means that the Accountable Institution must have a basis for applying simplified CDD measures.

10.13.2. Some examples of possible simplified measures are:

- a) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g., if account transactions rise

- above a defined monetary threshold);
- b) reducing the frequency of customer identification updates;
- c) reducing the degree of on-going monitoring and scrutinizing transactions based on a reasonable money threshold; and
- d) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.

10.13.3. Some examples of when an Accountable Institution might apply reduced CDD measures are where:

- a) reliable information on the customer and beneficial owner is publicly available or where adequate checks and controls exist elsewhere in the national system;
- b) the Accountable Institution is dealing with another Accountable Institution whose AML/CFT/PF controls it is familiar with by virtue of previous dealings; or
- c) the customer is an Accountable Institution that is subject to and supervised for compliance with AML/CFT/PF requirements consistent with standards set by the FATF;
- d) the customer poses a lower risk of ML/TF/PF because of the nature of the product that the customer has bought or intends to buy such as a micro insurance product or a micro-credit loan.

10.13.4. Where simplified CDD measures have been performed in relation to a customer, the Accountable Institution should document:

- a) the findings of its risk assessment; and
- b) the nature of the simplified CDD measures.

10.13.5. Simplified CDD measures are not allowed where there is a suspicion of money laundering and terrorist financing or where specific higher-risk scenarios apply.

11. ENHANCED CUSTOMER DUE DILIGENCE

11.1 When EDD is required?

11.1.1 An Accountable Institution is required to apply EDD for such categories of customers, business relationships, or transactions that are determined to present higher ML/TF risk due to business activity, ownership structure, nationality, residence status, politically exposed status, or other higher-risk indicators.

11.1.2 The policy framework of the Accountable Institution should therefore include a description of the type of customers that are likely to pose higher than average risk and the EDD

procedures to be applied in such instances. The commencement of a business relationship with a high-risk customer must be approved by senior management. Senior management should receive sufficient information to make an informed decision on the level of ML/TF/PF risk the institution would be exposed to if it enters into or continues that business relationship and how well-equipped it is to manage that risk effectively.

11.1.3 An Accountable Institution should also ensure that monitoring systems are appropriately tailored and provide timely and comprehensive reports to facilitate effective monitoring of such relationships and periodic reporting on such relationships to senior management and the Board.

11.1.4 EDD must be applied in the following circumstances:

- a) Business transactions with persons and financial institutions in or from other countries that do not or insufficiently comply with the FATF Standards;
- b) Complex, unusual, or large transactions, whether completed or not, to all unusual patterns of transaction and to insignificant but periodic transactions which have no apparent economic or visible lawful purpose;
- c) Where money laundering risks are higher;
- d) When establishing correspondent banking relationships;
- e) Where the customer is a foreign politically exposed person (PEP);
- f) Where higher risks have been identified with a customer who is a domestic PEP or a PEP associated with an international organization; and;
- g) Non-face-to-face business relationships or transactions.

11.2 Examples of EDD Measures:

11.2.1 When a person becomes a new customer or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, examples of EDD measures include (but are not limited to) taking more intrusive and exhaustive steps to:

- a) Increase the quantity of information obtained for CDD purposes (e.g., request additional information as to the customer's residential status, employment, salary details, and other sources of income) and requesting additional documentary evidence or utilizing publicly available sources (e.g., scrutiny of negative media news, internet searches, use of social media).
- b) Understand the customer's ownership and control structure to ensure that the risk associated with the relationship is well-known. This may include obtaining and assessing information regarding the customer's reputation including any negative media allegations against the customer.

- c) Understand the intended nature of the business relationship and the reasons for intended or performed transactions. This may include obtaining information on the number, size, and frequency of transactions that are likely to be conducted. It may be appropriate to request a customer's, business plans, cash flow projections, and copies of contracts with vendors. The financial institution should understand why the customer is requesting a certain service or product particularly when it is unclear why the customer is seeking to establish business relationships in another jurisdiction from where he is domiciled. The account may have to be monitored for some time to establish a full view of the nature of the activity and whether it fits with the initial risk profile of the customer.
- d) Establish the source of funds or source of wealth of the customer. Where the risk associated with the customer is particularly elevated, intrusive measures to verify the source of funds and wealth may be the only adequate risk mitigation measure. Possible sources may be a reference to VAT and income tax returns, pay-slips, title deeds, or, if from an inheritance, request a copy of the will or documentation to evidence divorce settlement or sale of property or other assets.
- e) Evaluate the principals and conduct reference checks and checks of electronic databases;
- f) Review current financial statements; and
- g) Conduct enhanced, ongoing monitoring of the business relationship, by increasing the number and timing of controls applied, and through more frequent formal review.

11.3 High-Risk Jurisdictions/Countries

- a) An Accountable Institution must implement EDD measures commensurate with the ML/TF/PF risks associated with business relationships and transactions with customers (and, in the case of legal persons and arrangements, their Beneficial Owners, beneficiaries, and other controlling persons) from high-risk countries;
- b) An Accountable Institution is required to consider establishing adequate internal policies, procedures, and controls in relation to the application of EDD measures and risk-proportionate effective countermeasures to customers and business relationships associated with high-risk countries commensurate with the nature, size of the business and the risks involved.

For updates on high-risk and non-co-operative jurisdictions, an Accountable Institution is advised to view the following websites:

<http://www.fatf-gafi.org/countries/#high-risk>

<https://www.fsra.co.sz/legal/aml/links/>

11.4 Enhanced Monitoring

11.4.1. The following are examples of measures a financial institution may employ to monitor high-risk customers:

- a) Conducting more frequent reviews of the business relationship and establishing more stringent thresholds for updating CDD information;
- b) Setting specific business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
- c) Requiring senior management approval at the transaction level for products and services that are new for the customer;
- d) Reviewing transactions more frequently against red flag indicators relevant to the relationship. This may include establishing the purpose and destination of funds and obtaining more information on the beneficiary before conducting the transaction;
- e) Flagging unusual activities and escalating concerns and transactions for senior management's attention.
- f) Ascertain source of funds and source of wealth of the customer and of the customer's beneficial owner

11.5 Politically Exposed Persons

11.5.1 This Guideline defines a PEP means a person who holds, or has held, a prominent public position, whether in Eswatini or a foreign country, including, but not limited to, a Head of State or Government; a politician at a national level; a senior Government official, judicial, military or party official at the national level; a senior executive of a state-owned enterprise, persons who are or have been entrusted with a prominent function by international organizations; or an individual or entity identified as having close family ties or personal or business connections to any of the aforementioned persons, an international organization; senior official and their close associates; an individual or undertaking identified as having family or personal or business connections close to such International Organisation senior official. The definition of a PEP is not intended to cover middle-ranking or more junior individuals.

11.5.2 Factors to consider in determining PEPs:

11.5.2.1. Immediate family members such as parents, siblings, spouses, children, and close associates of the PEP may also benefit from or be used to facilitate the abuse of public funds by the PEP and are also considered to be PEPs.

11.5.2.2. It is not contemplated that every person associated with a PEP will be considered a close associate. An Accountable Institution may consider factors such as the level of influence the PEP has on such a person or the extent of the close

associate's exposure to and influence on the PEP. The Accountable Institution may rely on information available from public sources to identify an individual who is widely and publicly known to maintain a close relationship with PEP, either socially or professionally.

11.5.2.3. An Accountable Institution must take reasonable measures to determine whether a person is associated with a PEP. Reasonable measures include, but are not limited to, one or more of the following actions:

- a) Asking the customer at the inception of the relationship. The customer's occupation or employment obtained at the time of account opening or during the ongoing due diligence process is a key factor in PEP determination or self-disclosure of PEP status by the customer;
- b) Conducting an open-source search. Use the internet and media as sources of information for the determination, monitoring, and verification of information in relation to PEPs, noting that information retrieved may not in all cases be comprehensive or reliable;
- c) Consulting a source of commercially available information. An Accounting Institutions must consider the limitations of such databases noting that the use of these databases should never replace risk-based CDD processes.

11.6. PEPs Enhanced Customer Due Diligence

11.6.1. In addition to performing the CDD measures required above in this Guideline, an Accountable Institutions must undertake the following due diligence measures when determining whether a customer is a domestic or foreign PEP:

- a) put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
- b) obtain senior management approval before establishing (or continuing, for existing customers) such business relationships;
- c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
- d) conduct enhanced ongoing monitoring of that relationship.
- e) conduct enhanced ongoing monitoring of the business relations with the customer.
- f) review the PEP relationship annually.

11.6.2. A combination of activities may be used to make the PEP determination. For example, the Accountable Institution should:

- a) during account opening procedures, include a specific question on PEP status and/or capture occupation to identify holders of public office.
- b) periodically monitor their existing client base against changes in the PEP universe and not just at the time of client on-boarding.
- c) Outside of periodic screening, the Accountable Institution may also rely on media monitoring to identify PEPs. For example, newspaper announcements regarding changes to board members of state-owned corporations. Additional sources of information include the Government website (foreign or domestic), and Parliament website (foreign or domestic), the EFIU website (foreign or domestic); and the website of the FATF.
- d) Understanding and documenting the length of time, the title or position, and the country in which the PEP holds, or held, political exposure;
- e) If the individual customer is a close family member or close associate, the relationship of the person to the PEP must be documented;
- f) Understanding and documenting the nature and intended purpose of the relationship/account, the source of the initial funds (where appropriate), and the anticipated levels of account activity;
- g) Understanding and documenting the customer's source of funds and source of wealth (e.g. salary and compensation from official duties and wealth derived from other sources). Where the risks are high or there are doubts as to the veracity of the information provided by the customer, financial institutions should validate this information using independent and reliable sources;
- h) Conduct Negative News or Adverse Media screening on the customer and evaluate any positive hits.

11.7.Reliance on Third Parties

11.7.1. An Accountable Institution may rely on intermediaries or other third parties to perform some elements of the CDD process, provided that the following requirements are met:

- a) the Accountable Institution must be satisfied that the third party it intends to rely upon is subject to and is supervised for compliance with AML/CFT/PF requirements consistent with the standards set by the FATF, and has adequate AML/CFT/PF systems in place to comply with those requirements;
- b) the third party is able and willing to provide to the Accountable Institution without delay, any identification data, documents, or information obtained by the third party relating to CDD measures applied to customers and beneficial owners;
- c) the third party commits in writing that it shall perform CDD measures, grant the Accountable Institution access to CDD documentation in its custody, and report to the

EFIU and the Accountable Institution in the case of a suspicious or unusual transaction; and

- d) the Accountable Institution undertakes and completes its verification of the customer and beneficial owner if it has doubts that appropriate due diligence was performed by the third party.

11.7.2. For the avoidance of doubt, notwithstanding the reliance on a third party, the ultimate responsibility for the customer and beneficial owner identification and verification remains with the Accountable Institution relying on a third party. However, third parties are responsible for the validity of all information obtained.

11.7.3. For an Accountable Institution to rely on a third party that is part of the same financial group, relevant competent authorities may also consider that the requirements of the criteria above are met in the following circumstances:

- a) the group applies CDD and record-keeping requirements, in line with Recommendations 10 to 12, and programs against money laundering and terrorist financing, in accordance with Recommendation 18;
- b) the implementation of those CDD and record-keeping requirements and AML/CFT/PF programs is supervised at a group level by a competent authority; and
- c) any higher country risk is adequately mitigated by the group's AML/CFT/PF policies.

11.8.Reviewing and Updating the Customer Due Diligence Information

11.8.1. An Accountable Institution must ensure timely review and update of customer due-diligence information as this is a fundamental component of an effective ML/TF/PF risk management and mitigation program. Accountable Institutions are required to maintain up to date records of the due-diligence documents, data, and information obtained on customers, and on their beneficial owners or beneficiaries in the case of legal persons or arrangements.

11.8.2. An Accountable Institution should consider establishing clear rules with respect to the maximum period that should be allowed to elapse between regular due-diligence reviews/updates of customer records for business relationships in different risk categories.

11.9.Reliance on Third Parties to Undertake CDD

11.9.1. An Accountable Institution may use the services of a third party for collecting and the performance of CDD measures, keeping and maintaining of records as long as the records can be obtained upon request and without delay by internal, and external auditors, law

enforcement agencies, the FSRA and the EFIU and that the third party adheres to the record-keeping provisions of the MLFTP legislation.

11.9.2. Where an Accountable Institution relies on a third party to keep and maintain records on its behalf, the Accountable Institution must provide the EFIU and the FSRA with the following particulars of the third party:

- a) registered name;
- b) name under which the third-party conducts business;
- c) name and contact particulars of individual who exercises control over access to the records;
- d) address where records are kept;
- e) address from where the third-party exercises control over the records; and
- f) name and particulars of the individual(s) or the third party who liaises with the Accountable Institution concerning the records and their retention.

11.9.3. For the avoidance of doubt, the ultimate responsibility for ensuring that records are kept and maintained in the manner set out in this paragraph lies with the Accountable Institution which shall also be liable for failure to meet the requirements.

11.9.4. Records may be kept in electronic form, provided that they are capable of being reproduced in a legible format which will be admissible in a court of law in Eswatini.

PART III – DUTY TO MAINTAIN PROPER RECORDS

12. RECORD KEEPING

- a) Maintaining accurate records is crucial to the effectiveness of any system designed to stop the funding of terrorism and money laundering. When it comes to the identification, investigation, prosecution, and confiscation of criminal funds when there are illicit financial flows involved, the records of clients' names and transaction activities frequently serve as a single piece of evidence. Thus, recordkeeping is the other half of the CDD measures, and when combined, these two components increase the financial system's openness. The MLFTP Act mandates that responsible institutions keep records pertaining to client identity and transaction activity because of this.
- b) An Accountable Institution should put in place a document record-keeping and retention policy that provides for the maintenance of a variety of records, including those related to ML/TF/PF risk assessment, customer identification, business transactions, internal and external reporting, and training. The statutory requirement is that records must be kept for five years from the date on which the business relationship is terminated. An Accountable

Institution may maintain particular records beyond the minimum requirement of five years, where required by the EFIU or the FSRA.

- c) Adhering to record-keeping obligations will guarantee that sufficient data is recorded in the records of a responsible organization to allow for the reconstruction of a transaction trail, which will help investigators identify financial flows while carrying out their investigations. In light of this, it is beneficial for the Accountable Institution to consider their MLFTP Act reporting responsibilities when developing internal procedures and systems for record-keeping. This will help to guarantee that all pertinent data is easily accessible and that reporting requirements under the MLFTP Act are not unnecessarily delayed or hampered by a lack of information.

12.1. Obligation to keep customer due diligence records

Section 8 of the MLFTP Act provides for an obligation on an Accountable Institution to keep customer due diligence records. This means that for the Accountable Institution to meet their MLFTP Act duties, the Accountable Institution must maintain a record of all client information acquired throughout their operations. An Accountable Institution should be required to keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction. Copies of or references to information that was given to or acquired by the Accountable Institution to confirm the customer's identity must be included in these documents.

12.2. Obligation to keep transaction records

According to the MLFTP Act, An Accountable Institution must maintain transaction records of both individual transactions and transactions completed during their business relationship with a client. This implies that the responsible institution is required to maintain documentation of every interaction it has with a client. Transaction records must contain enough information to allow the transaction to be recreated. An Accountable Institution must establish and maintain records in a manner and form that will enable the Accountable Institution to comply immediately with requests for information from law enforcement EFIU, and other competent authorities. This information must include the transaction's amount, currency, date, parties involved, nature, and any pertinent or relevant business correspondence. If the responsible institution offers account facilities, it must also include the specifics of each account and file linked to the transaction.

12.3. Manner in which records must be kept

The MLFTP Act is not prescriptive as to how records must be kept. This implies that records may be stored in accordance with standard procedures of an Accountable Institution for the capture of information and the retention of records.

Regardless of how records are kept, the Accountable Institution must ensure that the following principles are met:

- a) The Accountable Institution must have free and easy (in other words unencumbered) access to the relevant records;
- b) The records must be readily available to the EFIU and the FSRA when required;
- c) The records must be capable of being reproduced in a legible format and
- d) If the records are stored off-site the EFIU and the FSRA must be provided with the details of the third party storing the records.

12.4.Customer Due Diligence Records

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

12.5.Transaction records

12.5.1. An Accountable Institution must keep a record of every domestic or international transaction, whether the transaction is a single transaction or concluded in the course of an ongoing business relationship with the customer. The transaction records must be sufficient to enable the transaction to be readily reconstructed at any time, to provide evidence for the prosecution of any offence, and to assess the level of compliance with this Guideline. The records must include at least the following information:

- a) the amount involved and the currency in which it was denominated;
- b) the date on which the transaction was concluded;
- c) the parties to the transaction;
- d) the nature of the transaction; and
- e) if the Accountable Institution provides account facilities to its customers, the identifying particulars of all accounts that are involved in the transaction.

12.5.2. Records that relate to a transaction that is concluded must be kept for at least five years from the date on which the transaction was concluded. On the other hand, records that relate to a transaction that gave rise to a suspicious or unusual transaction report must be kept for at least five years from the date on which the report was submitted to the EFIU.

12.5.3. Accountable Institutions shall further maintain specific records beyond the minimum period of five years when requested to do so by the EFIU, a law enforcement agency, or the FSRA.

PART IV – KNOW YOUR EMPLOYEE

13. KNOW YOUR EMPLOYEE

13.1. An Accountable Institution shall implement programs against ML/TF/PF, which have regard to the ML/TF/PF risks and the size of the business, and which include the following internal policies, procedures, and controls: screening procedures to ensure high standards when hiring employees.

13.2. In addition to knowing the customer, an Accountable Institution must have robust procedures in place for knowing its employees. In this regard, every Accountable Institution should have a know-your-employee or recruitment policy to attract and retain employees of the highest levels of integrity and competence. The ability to implement an effective AML/CFT/PF program depends in part on the quality and integrity of employees.

13.3. An Accountable Institution should undertake due diligence on prospective employees and throughout employment. The Accountable Institution shall, amongst others:

- a) Verify the applicant's identity and personal information including employment history and background.
- b) Develop a risk-based approach to determining when pre-employment background screening is considered appropriate or when the level of screening should be increased, based on the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, educational, professional qualifications, and financial crime background;
- c) Maintain an ongoing approach to screening for specific positions, as circumstances change, or for a comprehensive review of employees over a period of time. Internal policies and procedures should be in place (e.g., codes for conduct, ethics, conflicts of interest) for assessing employees;

- d) Have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided;
- e) Have a robust recruitment policy: an Accountable Institution should implement ongoing monitoring of employees to ensure that they continue to meet the standards of integrity and competence of the Accountable Institution.

14. TRANSACTION MONITORING

14.1. An Accountable Institution must have appropriate processes in place that allow for the identification of unusual transactions and patterns. Since these will not all be suspicious, the Accountable Institution should also have processes to analyse transactions and patterns to determine if they are suspicious and meet the reporting requirements. Transaction monitoring processes or systems may vary in scope or sophistication (e.g., using manual spreadsheets and exception reports to automated and complex systems or a combination of both) depending on the size, volumes, and complexity of the business operations. Regardless, the key elements of any system are having up-to-date customer information, based on which it will be possible to identify the unusual activity and asking pertinent questions to elicit the reasons for unusual transactions or activities to make a reasonable determination whether they may represent something suspicious.

14.2. The parameters and thresholds used to generate alerts of unusual transactions should be customized to be commensurate with the ML/TF/PF risk profile and the complexity and extent of its business activities of the Accountable Institution. Standard parameters provided by the vendor may be used but the Accountable Institution must be able to validate and demonstrate to the FSRA that these reflect and are appropriate for the institution's risk position. The monitoring system should be tested periodically to ensure that the parameters are performing as expected and remain relevant. Modifications may be required as a result of such testing.

15. SUSPICIOUS TRANSACTION REPORTING

15.1. An Accountable Institution must report suspicious transactions, attempted suspicious transactions, and where there are reasonable grounds to suspect that a transaction may be related to the commission of a criminal activity or related to ML/TF/PF. An Accountable Institution must provide any additional information required by the EFIU in relation to the filed suspicious transaction reports.

15.2. All suspicious or unusual transactions must be reported to the EFIU within two days of forming the suspicion regardless of the amount of the transaction or funds involved.

15.3.To fulfil the reporting obligations, an Accountable Institution should implement adequate internal policies, procedures, and controls in relation to the identification and reporting of suspicious transactions to the EFIU.

15.4.An important pre-condition for the recognition of a suspicious transaction is for the Accountable Institution to know enough about the customer and business relationship to recognize that a transaction is, or a series of transactions are, unusual or suspicious.

15.5.To meet its obligations, an Accountable Institution is required to:

- a) establish a single reference point within the organization to whom all staff and representatives are instructed to promptly refer all transactions suspected of being connected with money laundering or terrorist financing. This involves putting in place a clear process and procedure for ensuring that all suspicious and unusual transactions are reported through the Compliance Officer to the EFIU.
- b) document the policy and procedures for reporting to the Compliance Officer so that employees know what should be reported and the process to follow when reporting; and
- c) keep records of all transactions referred to the EFIU together with all internal findings and analyses done in relation to any suspicious transactions, including transactions that are not reported to the EFIU.

15.6.To fulfill this obligation, an Accountable Institution must also put in place and update indicators that can be used to identify the suspicion of criminal activity and involvement in ML/FT/PF activities.

15.7.Examples of suspicious transactions are set out in Appendix A to this Guideline. These examples are not exhaustive and are only examples of the most basic ways money may be laundered. If any transactions similar to those in Appendix A, or any other suspicious transactions, are identified, this should prompt further inquiries and, where necessary, investigations into the source of funds.

16. TIPPING-OFF AND CONFIDENTIALITY

16.1.An Accountable Institution and directors, officers, employees, and auditors of the Accountable Institution are:

- a) prohibited from disclosing (“tipping-off”) the fact that a suspicious transaction report (STR) or related information is being filed with the EFIU; and

- b) protected from civil, criminal, or disciplinary proceedings if they report their suspicions in good faith to the EFIU, even if they did not know precisely what the suspected criminal activity was, and regardless of whether the illegal activity occurred.

16.2.A risk exists that customers could be unintentionally tipped off when an Accountable Institution performs its CDD obligations. A customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing activity. Therefore, where the Accountable Institution forms a suspicion that a transaction or transactions relate to money laundering or terrorist financing, the Accounting Institution should take into account the risk of tipping off when performing the CDD process.

17. TRAINING

17.1.Officers, employees, and representatives of an Accountable Institution should receive initial and ongoing training on;

- a) AML/CFT/PF legislation, regulations, and in particular, CDD measures and detecting and reporting suspicious and unusual transactions;
- b) the policies, procedures, and controls on AML/CFT/PF;
- c) the roles and responsibilities of officers, employees, and representatives in combating money laundering and terrorism financing in terms of the AML/CFT/PF legislation; and
- d) prevailing trends, developments techniques, and trends on money laundering and terrorism financing.

17.2.To ensure the effectiveness of training, entities should train relevant staff ensuring that training is tailor-made for the AML/CFT/PF responsibilities of those particular staff members, monitor attendance at such training, and take appropriate follow-up action in relation to staff.

17.3.Records of all training undertaken, the content of the training program, names and qualifications of the facilitators, and the lists of attendees should be kept for a minimum period of five years from the date of the training.

18. AUDIT AND SELF-ASSESSMENT OF CONTROLS

18.1.An Accountable Institution should conduct independent testing of the AML/CFT/PF compliance program. An Accountable Institution should maintain an adequately resourced and independent audit function to test compliance with policies, procedures, and controls. The assessment of AML/CFT/PF controls is an important component of the AML/CFT/PF Risk Management Program because of its quality assurance outcome. The Accountable

Institution should perform a self-assessment of control measures annually, which at a minimum covers the adequacy of risk assessment, AML/CFT/PF policies and procedures, training, and other controls implemented to mitigate money laundering and terrorism financing risks.

18.2. Like the assessment of other risk management controls, effectiveness testing of the AML/CFT/PF Risk Management Program is important and it should be planned and performed by an auditor(s) who has appropriate training and experience in respect of money laundering and terrorism financing risk and an appropriate level of knowledge of the regulatory requirements and guidelines.

19. INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES

19.1. An Accountable Institution that is part of a group must implement group-wide programs against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT/PF purposes. An Accounting Institution should ensure that foreign branches and subsidiaries apply AML/CFT/PF measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programs against ML/TF/PF. An Accountable Institution should not merely comply with group policies and regulatory requirements but should appropriately identify the applicable Eswatini legislation and ensure that the local policies reflect the Eswatini legislation.

19.2. Where the minimum AML/CFT/PF requirements of the host country are less strict than those of the home country, an Accountable Institution should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks and inform their home supervisors.

PART V – FINAL PROVISIONS

20. UNITED NATIONS SECURITY COUNCIL RESOLUTIONS

The sanctions review aims to apply Targeted Financial Sanctions (TFS) against all individuals listed by the UN Security Council. An Accountable Institution must screen customers or potential customers involved in transactions against United Nations Security Council Resolution (UNSCR) sanctions lists. Such screening must be performed before opening accounts or before giving a

customer access to the services, regardless of whether the customer is dealing below or above the CDD threshold. Where a credit institution uses brokers or agents in any way to facilitate or access its services, the credit institution must ensure that such third parties comply with their AML/CFT/PF/CPF obligations when they are trusted. This is necessary to combat TF and PF activities by ensuring that selected individuals, organizations, or countries are identified and do not benefit from improperly exploited services and that their funds and assets are frozen accordingly. The term "targeted economic sanctions" primarily refers to the immediate freezing of assets and the prohibition of making funds or other property or services directly or indirectly available to sanctioned individuals, entities, or groups.

20.1.Effective Client Screening

20.1.1. To effectively implement TFS, a credit institution must ensure:

- a) all customers undergo a sanction control before using the services; and
- b) Services will not be available to customers until the sanctions review is completed and documented. Screening should not be done after using services or facilitating transactions. Preliminary inspection enables the proactive detection of persons subject to punishment. All persons found with such penalties should not be allowed access to the Services at all and their business activities should be reported to the EFIU immediately, while the related funds (or assets) are frozen or other transactions prohibited. In practice, policies and procedures must therefore ensure that customers can at least attempt transactions to ensure proper identification, enabling effective verification and, if the customer is listed, the possible freezing of the funds with which the customer attempted to make transactions, followed by a full record of further transactions and reporting.

20.1.2. The following databases of the Lending Institution must be included in the screening process:

- a) Existing customer databases. All systems (if any) containing customer data and transactions need to be mapped to the screening system to ensure full compliance;
- b) Loan applicants/Potential customers before conducting any transactions or entering a business relationship with any person;
- c) Ultimate beneficial owners of clients who are legal persons and trusts;
- d) Names of individuals, entities, or groups with direct or indirect relationships with them; and
- e) Directors and/or agents acting on behalf of customers (including individuals with power of attorney).

20.2. Where to find the updated Sanctions Lists?

All Accountable Institutions are required to access lists of sanctioned persons and screen their clients against such lists before establishing a business relationship and whenever the sanctions lists are updated. The most recently updated sanctions list of the UNSCR18 can be found on the UNSC website or via the following link: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

20.3. Targeted Financial Sanctions (TFS)

As mentioned above, TFS includes asset freezing without delay and prohibition from making funds or other assets or services, directly or indirectly, available for the benefit of sanctioned individuals, entities, or groups.

20.4. Asset freezing without delay

20.4.1. Freezing is the prohibition to transfer, convert, dispose, or move any funds or other assets that are owned or controlled by designated individuals, entities, or groups in the Local Terrorist List or UN Consolidated List. In terms of international standards, without delay means within a matter of hours. Asset freezing includes:

- a) The freezing of funds and other financial assets and economic resources, including preventing their use, alteration, movement, transfer, or access; and
- b) The freezing of economic resources also includes preventing their use to obtain funds or other assets or services in any way, including, but not limited to, selling or mortgaging them.
- c) Reporting transaction under this part to the EFIU.

20.4.2. An Accountable Institution must be able to identify and enforce funds UNSCR freeze without delay or not deal with any designated entities or individuals in terms of the relevant Eswatini legislations.

20.4.3. An Accountable Institution must ensure to screen customers before establishing business relations and/or carrying out of an occasional transaction with new customers.

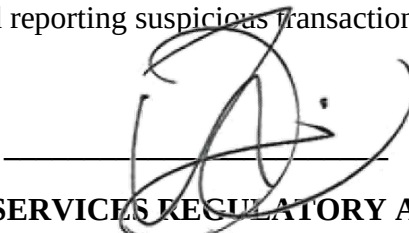
20.4.4. Accountable institutions are also required to ensure that they monitor and update the sanction list issued by the Security Council and evidence of such monitoring shall be documented. The sanctions list and updates thereto shall flow through all the Accountable Institution's branches with clear instructions on the use of the list.

21. SANCTIONS FOR NON-COMPLIANCE WITH THE GUIDELINE

Non-compliance with the Guideline will expose Accountable Institutions to disciplinary action in terms of section 35 of the Money Laundering and Terrorism Financing (Prevention) Act 2011. Accountable Institutions should further note that compliance with the Guideline does not constitute a defence for prosecution for an offence under the MLTFP Act and/or under the FSRA Act. Therefore, entities are encouraged to take steps to ensure that they comply with the Guideline, the MLTFP Act, and the FSRA Act.

22. GUIDANCE AND FEEDBACK

The Authority, in assisting accountable institutions to comply with this guideline will provide feedback, which will assist Accountable Institutions in applying national AML/CFT/PF measures, and in particular, in detecting and reporting suspicious transactions.



**FINANCIAL SERVICES REGULATORY AUTHORITY
CHIEF EXECUTIVE OFFICER
NCAMISO T. NTSHALINTSHALI**

Appendix A - Examples of Suspicious Transactions

Non-Bank Financial Service Providers

An Accountable Institution that provides life insurance or annuities should consider the following indicators of potentially suspicious transactions:

- a) Customer wants to use cash for a large transaction;
- b) The customer requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment;
- c) A customer who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump sum payment;
- d) The customer conducts a transaction that results in a conspicuous increase in investment contributions;
- e) The scale of investment in insurance products is inconsistent with the client's economic profile;
- f) Unanticipated and inconsistent modification of customer's contractual conditions, including significant or regular premium top-ups;
- g) Unforeseen deposit of funds or abrupt withdrawal of funds;
- h) Involvement of one or more third parties in paying the premiums or in any other matters involving the policy;
- i) Overpayment of a policy premium with a subsequent request to refund the surplus to a third party;
- j) Funds used to pay policy premiums or deposits originate from different sources;
- k) Use of life insurance products in a way that resembles the use of a bank account, namely making additional premium payments and frequent partial redemptions.
- l) Customer cancels investment or insurance soon after purchase;
- m) Early redemption takes place in the absence of a reasonable explanation or a significantly uneconomic manner;
- n) Customer shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with the termination of the contract;
- o) The customer makes payments with small denomination notes, uncommonly wrapped, with postal money orders or with similar means of payment;
- p) The first (or single) premium is paid from a bank account outside the country;
- q) Repeated and unexplained changes in beneficiary;
- r) The relationship between the policyholder and the beneficiary is not established.

Securities Dealers

An Accountable Institution that is involved in the business of dealing in securities, segregated fund products, or any other financial instruments, including portfolio management and investment counselling, should consider the following indicators of potentially suspicious transactions;

- a) Inactive accounts suddenly experience large investments that are inconsistent with the normal investment practice of the customer or the customer's financial ability;
- b) Any dealing with a third party when the identity of the beneficiary or counterparty is undisclosed;
- c) The customer attempts to purchase investments with cash;
- d) The customer uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period and such activity is inconsistent with the normal investment practice of the customer or the customer's financial ability;
- e) The customer wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the customer;
- f) The customer frequently makes large investments in stocks, bonds, investment trusts, or other securities in cash or by cheque within a short period, inconsistent with the normal practice of the customer;
- g) The customer makes large or unusual settlements of securities in cash;
- h) The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading;
- i) Transfers of funds or securities between accounts not known to be related to the customer;
- j) Several customers open accounts within a short period to trade the same stock;
- k) The customer is an institutional trader who trades large blocks of junior or penny stock on behalf of an unidentified party;
- l) Unrelated customers redirect funds toward the same account;
- m) Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity;
- n) Transaction of very large monetary size;
- o) Customer is willing to deposit or invest at rates that are not advantageous or competitive.

Credit Providers and SACCOs

In terms of a pawn broking transaction; the title of property pledged by the customer appears not to be authentic.

- a) The value of the property pledged by the customer appears to be significantly less than what it appears to be.
- b) The customer pledges property with no intention to settle and buyback.
- c) The customer borrows funds on behalf of a third party.
- d) The customer suddenly settles a loan in full.

- e) Repayment by a guarantor or third party under abnormal circumstances.
- f) Third parties settle higher purchase contracts on behalf of account holders.
- g) Frequent multiple deposits to member savings accounts.
- h) Borrowing large amounts of funds against member non-withdrawable savings and pledging to repay using unexplained funds (outside normal salary sources).
- i) Lump sum deposits to member savings accounts.