GUIDANCE NOTE: CONDUCTING MONEY LAUNDERING/ TERRORISM FINANCING RISK ASSESSMENT

CENTRAL BANK OF KENYA

MARCH 2018

PART I Preliminary

1.1 Title

1.2 Authorization

1.3 Application

1.4 Definitions

PART II Statement of Policy

2.1 Purpose

2.2 Scope

2.3 Responsibility

2.4 Introduction

PART III Specific Requirements

3.1 Governance & Controls

3.1.1 Governance

3.1.2 Control Functions

3.2 General principles

3.3 Steps in Risk Assessment

3.3.1 Prudential Requirement

3.3.2 Identification of Specific Risk Categories

3.3.3 Detailed Analysis

3.3.4 Evaluation of AML/CFT program

3.4 Weights and Scoring

3.5 Residual Risk

PART IV Reporting

4.1 Reports to Management

4.2 Reports to CBK

PART I: PRELIMINARY

1.1 **Title**- Guidance Note on Conducting Money Laundering/ Terrorism Financing (ML/TF) Risk Assessment.

1.2 **Authorization**-This Guidance Note is issued under Section 33(4) of the Banking Act, which empowers the Central Bank of Kenya (CBK) to issue Guidance Notes to be adhered to by institutions in order to maintain a stable and efficient banking system.

1.3 **Application -** All institutions licensed under the Banking Act (Cap.488) and their foreign branches and subsidiaries.

1.4 **Definition:** The terms and acronyms used in this Guidance Note are defined below:

1.4.1 Financial Action Task Force (FATF) is an inter-governmental body which sets standards and develops and promotes policies to combat money laundering and terrorist financing and proliferation.

1.4.2 Inherent risk refers to risk that exists before the application of controls or mitigation measures.

1.4.3 Impact: this refers to the seriousness of the damage that would occur if the ML/TF risk materializes (i.e. threats and vulnerabilities).

1.4.4 Mitigation measures: Controls put in place to limit the potential money laundering and terrorist financing risks identified while conducting a risk assessment.

1.4.5 Money Laundering Reporting Officer means an officer appointed under Regulation 10 of Proceeds of Crime and Anti-Money Laundering (POCAML) Regulations.

1.4.6 Residual risk is the level of risk that remains after the implementation of mitigation measures and controls.

1.4.7 Risk can be defined as the likelihood of an event and its consequences. In the context of money laundering/terrorist financing (ML/TF), risk means:

- At the national level: threats and vulnerabilities presented by ML/TF that put at risk the integrity of Kenya's financial system and the safety and security of Kenyans.

- At the reporting entity level: threats and vulnerabilities that put the reporting entity at risk of being used to facilitate ML/TF.

1.4.8 Threats: this could be a person (or group), object that could cause harm. In the ML/TF context, a threat could be criminals, facilitators, their funds or even terrorist groups.

1.4.9 Vulnerabilities: elements of a business that could be exploited by the identified threat. In the ML/TF context, vulnerabilities could be weak controls within a reporting entity, offering high risk products or services, etc.

PART II: STATEMENT OF POLICY

2.1 Purpose

This Guidance note is designed to assist financial institutions conduct a money laundering/ terrorism finance risk assessment. Therefore, the purpose of this Guidance Note is to ensure an institution's ML/TF risk assessment:

- Is compliant with the Central Bank of Kenya (CBK) Prudential Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism (CBK/PG/08 clause 5.5) and Regulation 6 of the Proceeds of Crime and Anti-Money Laundering (POCAML) Regulations.
- Meets international standards i.e. FATF Recommendations.
- Is robust enough to support risk based approach to managing money laundering laundering/ terrorism finance risks.
- Takes inventory of risks relating to products, services and delivery channels, clients and business relationships, geography and other relevant factors.
- Assists in implementing effective mitigation measures and in monitoring the money laundering and terrorist financing risks reporting entities may have or encounter as part of their activities and business relationships.

2.2 Scope

This Guidance Note sets the minimum standards that institutions should adopt to develop an effective ML/TF risk assessment framework. It is not a replacement for and does not supersede the legislation, regulations and guidelines that institutions must comply with as part of their regulatory obligations.

2.3 Responsibility

The board of directors and senior management of an institution are expected to formulate and implement ML/TF risk assessment framework. The framework must be documented and made available for review by external auditors and CBK.

2.4 Introduction

Clause 5.5 of the Central Bank of Kenya (CBK) Prudential Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism (CBK/PG/08) requires a reporting institution to undertake a Money Laundering (ML) and Terrorism Finance (TF) risk assessment to enable it identify, assess, monitor, manage and mitigate the risks associated with money laundering and financing of terrorism.

CBK recognizes that there are many effective methods and formats used in completing a ML/TF risk assessment. A bank's management should decide the appropriate method or format, based on the bank's particular risk profile. Whatever format management chooses to use for its risk assessment, it should be relevant and easily understood by all appropriate parties.

A well-developed risk assessment assists in identifying the bank's ML and TF risk profile. Understanding the risk profile enables the bank to apply appropriate risk management processes to the Anti-Money Laundering /Combating the Financing of Terrorism (AML/CFT) compliance program to mitigate the risks.

The risk assessment should provide a comprehensive analysis of the ML/TF risks in a concise and organized presentation, and should be shared and communicated with all business lines across the bank, board of directors and management.

The focus of this Guidance Note is to provide high level minimum requirements rather than prescriptive criteria for undertaking ML/TF risk assessments. CBK will review an institution's ML/TF risks assessment as part of its risk-based supervisory process.

PART III: SPECIFIC REQUIREMENTS

3.1 Governance & Control

3.1.1 Governance

a) Board of Directors

All board members should understand the nature of money laundering threats and vulnerabilities the institution faces. Further, the board should ensure that the bank adopts a risk based approach to managing ML/TF risks. The responsibilities of the board in relation to ML/TF risk assessment include:

i. Ensure development of a documented framework to conduct ML/TF risk assessment.
ii. Review outcome of the risk assessment process.
iii. Understand the ML/TF risk profile of the institution.
iv. Allocation of adequate resources to undertake the process.
v. Approve any strategic decisions proposed by management after the assessment of the process.
vi. Ensure all relevant departments/functions are involved in the process.

b) Senior Management

Senior management are required to ensure that the bank's activities are consistent with the business strategy, risk tolerance/appetite and policies approved by the board.

As such, the Senior Management should: -

i. Implement the board approved ML/TF risk assessment framework.
ii. Identify the risks relating to products, services and delivery channels, clients and business relationships, geography and other relevant factors.
iii. Continuously improve collection and analysis data used in the assessment.
iv. Provide periodic reports of the institution's ML/TF risk assessment.
v. Be responsible for carrying out any actions resulting from the gaps or deficiencies identified by the risk assessment exercise.
vi. Clearly identify and allocate duties and responsibilities as regards undertaking of the exercise.
vii. Ensure results as disseminated to all relevant parties.
viii. Ensure a copy of risk assessment is forwarded to CBK.

c) Money Laundering Reporting Officer

A financial institution is required to appoint a Money Laundering Reporting Officer (MLRO). The officer will be the central point of contact with the CBK for anti-money laundering/ combating the financing of terrorism purposes.

With regards to ML/TF risk assessment, the MLRO responsibilities include:

i. Coordinating the ML/TF risk assessment process.
ii. Collation and verification of input, data and comments from other departments.
iii. Analysis of data for the purpose of understanding the risks identified.
iv. Determining the residual risk for the different categories.
v. Determining the overall ML/TF risk profile of the bank.
vi. Preparing reports to senior management and the board on the ML/TF risk assessment process.

3.1.2 Control functions

Conducting an ML/TF risk assessment requires a collaborative approach that encompasses both business functions as well as control functions such as Internal Audit, Risk Management and External Audit. The management should ensure that an independent review of the ML/TF risk assessment process and results is undertaken. Where a control function is

required to undertake certain aspects of the exercise, this fact should be clearly enumerated in the ML/TF risk assessment framework.

Reports of any independent review of the ML/TF risk assessment exercise should be shared with the board and management.

3.2 General Principles

The ML/TF risk assessment undertaken should meet the following minimum requirements:

3.2.1 Identify and assess the money laundering and terrorism financing risks that may be associated with the institution's unique combination of products and services, customers, geographic locations, delivery channels and other factors.

3.2.2 Involve analysis of all available data to assess risks identified.

3.2.3 Evaluates the institution's AML/CFT compliance program.

3.2.4 Establishes the residual risk for the risk categories identified.

3.2.5 Use appropriate weights and scoring.

3.2.6 Should be specific to the institution and commensurate with the nature and size of the bank's business.

3.2.7 The risk assessment must be documented.

3.2.8 Be subjected to internal review and approval by the board and management.

3.2.9 The methodology followed to undertake the assessment be enumerated in a policy document.

3.2.10 Kept up -to -date i.e. CBK Prudential Guidelines requires institutions to update their risk assessment policies/programs at least every two years or after the occurrence of a significant event whichever comes earlier.

3.3 Steps in the Risk Assessment Process

3.3.1. Prudential Requirement

CBK/PG/08 Clause 5.15 stipulates that the development of an AML risk assessment framework involves the following steps:

a) Identifying and assessing the money laundering and terrorism financing risks that may be associated with the institution's unique combination of products and services, customers, geographic locations and delivery channels;
b) Conducting a detailed analysis of all available data to assess the level of risk within each high risk category; and
c) Determining whether the institution's AML compliance program is adequate and provides the necessary controls to mitigate the risks identified.

3.3.2. Identification of Specific Risk Categories

Attempts to launder money, finance terrorism, or conduct other illegal activities through a bank can emanate from many different sources. However, certain products, services, customers, entities, and geographic locations may be more vulnerable or have been historically abused by money launderers and criminals. This step involves identifying and assessing the money laundering and terrorism financing risks that may be associated with the institution's unique combination of:

- Customers.
- Products and services.
- Geographic locations.
- Delivery channels and
- Other qualitative factors.

3.3.2.1 Customers Risk

This should be assessed for the purposes of identifying the inherent money laundering risk of an institution's client base and business relationship. An institution shall determine, based on its own criteria, what risks a particular customer poses.

Certain customers and entities may pose specific risks depending on the nature of the business, the occupation of the customer, the nature of anticipated transaction activity and as prescribed under FATF standards.

Some factors to consider are:

a) Customers conducting their business relationship or transactions in unusual circumstances, such as:
   i. Significant and unexplained geographic distance between the institution and the location of the customer;
   ii. Frequent and unexplained movement of accounts to different institutions; and;
   iii. Frequent and unexplained movement of funds between institutions in various geographic locations.
b) Customers whose structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests.
c) Foreign financial institutions, including banks and foreign money service providers such as forex bureaus, and money transmitters.
d) Non-bank financial institutions such as money services businesses, casinos and brokers/dealers in securities, and dealers in precious metals, stones, real estate dealers.
e) Politically exposed persons (PEPs). Individuals who are or have been entrusted with prominent public functions (both foreign and local), for example, senior politicians, senior government officials, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs may involve reputational risks similar to those with PEPs.
f) Resident and Non- resident aliens (NRAs) and accounts held by foreign individuals.
g) Foreign corporations and domestic business entities, particularly offshore corporations such as domestic shell companies, private investment companies and international business corporations located in high-risk geographic locations.

h) Cash-intensive businesses, including, for example, supermarkets, convenience stores, restaurants, retail stores, liquor stores, wholesale distributors, car dealers among others.
i) Foreign and domestic non-governmental organizations and charities.
j) Professional service providers.

Institutions should develop a worksheet to capture the customer risk assessment based on the inherent characteristics of its clients. The worksheet should as a minimum have columns on; the Customer Type, Risk Rating, Rationale, Mitigation/ Controls, Scores, Weights used and the Residual Risk.

3.3.2.2 Products and Services Risk

Institutions should consider the potential money laundering and terrorism financing risks associated with each of its specific product or service. An institution will seek to identify its portfolio of products/account types and assign an inherent score to each, based on its general inherent characteristics and the degree of money laundering and terrorism financing risk present.

In undertaking this assessment, the institution is required to list all its products, identify Inherent Risks, Rationale, Mitigation/ Controls, Scores, Weights used and the Residual Risk.

3.3.2.3 Delivery Channels Risks

Institutions have various modes of transaction and distribution (delivery channels) of its products and services.

Some delivery channels may be more susceptible to ML/TF risk. Consequently it should be assessed whether, and to what extent, the method of delivery, such as non-face-to-face or the

involvement of third parties, including intermediaries and agents, could increase the inherent money laundering risk.

In undertaking this assessment, the institution is required to list all delivery channels, identify Inherent Risks, Rationale, Mitigation/ Controls, Scores, Weights used and the Residual Risk.

3.3.2.4 Geography/Country

This involves identifying geographic locations that may pose a higher risk to a bank's business. An institution will seek to understand and evaluate the specific risks associated with doing business in, opening and servicing accounts, offering products and services and/or facilitating transactions involving certain geographic locations. The Geography/Country risk may also be analysed with respect to the location of the business division, unit or business line, and may also include its subsidiaries, affiliates and offices, both internationally and domestically.

Institutions should identify domestic and international geographic locations that may pose a higher risk to its AML/CFT compliance program. Each case should be evaluated individually when assessing the risks associated with doing business, such as opening accounts or facilitating transactions, in certain geographic locations.

Factors that may result in a country or region posing a higher risk include:

i. Countries that are subject to sanctions, embargoes or similar measures issued by credible organizations such as the United Nations and the Financial Action Task Force.
ii. Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
iii. Countries identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

In undertaking this assessment, the institution is required to identify risks and explain the risk scoring allotted to each geographical area highlighted. The assessment should also indicate: Rationale for Rating, Mitigation/ Controls, Scores, Weights used and the Residual Risk.

3.3.2.5 Other Qualitative Risk Factors

The bank should also assess additional risk factors that can have an impact on operational risks and contribute to an increasing or decreasing likelihood of breakdowns in key AML/CFT controls. Qualitative risk factors that directly or indirectly affect inherent risk factors may include:

- Significant strategy and operational changes.
- Structure of ownership/ business e.g. presence of subsidiaries.
- National Risk Assessments.

3.3.3. Detailed Analysis

Once the institution has identified the risk, the second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess ML/TF risk.

This step involves evaluating data pertaining to the bank's activities (e.g., number of domestic and international funds transfers, types of customers, geographic locations of the bank's business area and customer transactions).

This detailed analysis is ultimately important because within any type of product or category of customer there will be account holders that pose varying levels of risk. This step in the risk assessment process gives management a better understanding of the bank's risk profile in order to develop the appropriate policies, procedures, and processes to mitigate the overall risk.

Additionally, institutions should undertake an impact analysis and develop a likelihood versus impact matrix to help determine the level of effort or monitoring required for the identified inherent risks.

Institutions can also use a risk matrix as a method of assessing risk in order to identify the risk categories that are in the low-risk zone, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing. In classifying the risk, an entity, taking into account its specificities, may also define additional levels of ML and TF risk. A risk matrix is not static; it changes as the circumstances of the entity change.

3.3.4. Evaluation of the AML/CFT Program

In this step, internal controls must be evaluated to determine how effectively they offset the identified risks. Controls are programmes, policies or activities put in place by the institution to protect against the materialization of a ML /TF risk, or to ensure that potential risks are promptly identified.

Each control is assessed for overall design and operating effectiveness. One way in which control effectiveness may be assessed is by undertaking a focused self-assessment by business unit/business line. A self-assessment of this kind can be challenged independently using subject matter expertise as well as existing internal information, such as business risk reviews, audit testing and assurance testing. A specific control may be rated according to a pre-defined rating scale or based on qualitative factors, e.g. ‘satisfactory’, ‘needs improvement’ or ‘deficient’ for each of the above control factors. After evaluating all controls, institutions are required to give an overall rating.

3.4 Weights and Scoring

Due to the nature of each institution’s unique business activities, products and services (including transactions), client base and geographic footprint, a risk based approach is used to calculate inherent risk. Each risk factor is usually assigned a score which reflects the

associated level of risk. Each risk area may then be assigned a weight which reflects the level of importance in the overall risk calculation relative to other risk areas. Similarly, each control may be assigned a weight which reflects the relative strength of that control.

The weight assigned to each of these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary from one institution to another, depending on their respective circumstances. Consequently, an institution will have to make its own determination as to the risk weights and scores to assign to the different risk.

3.5 Residual Risk

Once both the inherent risk and the effectiveness of the internal control environment have been considered, the residual risk should be determined.

Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management activities/controls. The residual risk rating is used to indicate whether the ML/TF risks within the institution are being adequately managed.

It is possible to apply a 3 tier rating scale, to evaluate the residual risk on a scale of High, Moderate and Low. Alternatively another rating scale could also be used, for example a 5 point scale of Low, Low to Moderate, Moderate, Moderate to High, and High.

PART IV: REPORTING

4.1 Reports to Management

The results of the ML/TF risk assessment should be presented to senior management and the board and communicated by the MLRO to all business units and the controls functions of the institution.

As a result of the volume of data that will underpin any ML/TF risk assessment, results can be presented in a number of different ways, highlighting risks by any factor recorded, for example by business division, product type, geography or client types, amongst others. This is more than just an averaging of results, but should be able to highlight inherent and residual risk, as well as control effectiveness, for any part of an institution's business.

The report should clearly indicate proposed action points to be adopted by the institution.

4.2 Report to CBK

On an annual basis, institutions shall provide Central Bank of Kenya with a report on the latest results of its MT/TF risk assessment. The report should be submitted by 31st December of the year.

In the event of any query or clarification, please contact:
The Director,
Bank Supervision Department
Central Bank of Kenya P. O. Box 60000 - 00200,
Nairobi Tel: 2860000
Email: fin@centralbank.go.ke