CENTRAL BANK OF LIBERIA

AML/CFT RISK MANAGEMENT GUIDELINE FOR FINANCIAL INSTITUTIONS

REGULATION AND SUPERVISION DEPARTMENT

MONROVIA, LIBERIA

Guideline on Money Laundering and Terrorism Financing (ML/TF) Risk Assessment and Management for Financial Institutions

PART I: INTRODUCTION

1. Risk assessment is the systematic process of identifying and measuring hazards and risk factors that have the potential to cause harm and determining appropriate ways to eliminate the hazard or control the risk when the hazard cannot be eliminated (risk control). Financial Action Task Force (FATF) requires countries to identify, assess and understand their ML/TF risks. Based on the assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. In addition, countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their ML/TF risks.

2. The draft Anti-Money Laundering, Preventive Measures and Proceeds of Crime Act (AML Act), requires reporting entities (financial institutions and DNFBPs) to identify, assess, monitor, manage and mitigate the risks associated with money laundering and financing of terrorism. The CBL Regulation on AML/CFT requires financial institutions to conduct risk assessment on new products, services and technology and identify all ML/TF risks and set out procedures on how these risks will be effectively mitigated.

3. This Guideline shall apply to all institutions licensed under the Financial Institutions Act and Insurance Act. This Guideline is issued under Section 39 and Sections 7.2 and 8.7 of the Financial Institutions Act and Insurance Act, respectively, which empowers the Central Bank of Liberia (CBL) to issue Guidelines to be adhered to by institutions to maintain a stable and efficient financial system.

4. ***Definition:*** The terms and acronyms used in this Guideline are defined below:

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.

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

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

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

Money Laundering Reporting Officer means an officer appointed under Anti-Money Laundering Regulations.

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

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 Liberia's financial system and the safety and security of Liberians.
- At the reporting entity level: threats and vulnerabilities that put the reporting entity at risk of being used to facilitate ML/TF.

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.

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: OBJECTIVE AND SCOPE OF THE GUIDELINES

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

- Is compliant with the Central Bank of Liberia (CBL) Regulations on Anti- Money Laundering and Combating the Financing of Terrorism.
- Meets international standards i.e. FATF Recommendations.

- Is robust enough to support risk-based approach to managing money 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.

7. This Guideline sets the minimum standards that financial 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 directives that financial institutions must comply with as part of their regulatory obligations.

8. The board of directors and senior management of a financial 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 CBL**.**

9. FATF standards require financial institutions and DNFBPs to take appropriate steps to identify, assess, and understand their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). This includes being required to:

(a) document their risk assessments;

(b) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) take into account the ML/FT risks identified at the country level (NRA);

(d) keep these assessments up to date; and

(e) have appropriate mechanisms to provide risk assessment to their supervisory authorities.

PART III: CBL RISK MANAGEMENT FRAMEWORK

The Risk Management Guidelines issued by CBL to the banking sector in 2009 listed the following risk management framework, which is also applicable to AML/CFT environment.

Corporate Governance

10. Financial institutions should establish a robust and effective corporate governance

framework that ensures transparency, accountability, and high ethical conduct in all aspects of their operations. Financial Institutions should adopt a Code of Ethics that promotes consistently high standards of ethical conduct by all employees. A sound corporate governance framework includes the use of effective policies and procedures, monitoring and reporting mechanisms and internal controls. Measures that ensure appropriate separation of functions and the avoidance of conflicts of interests are essential hallmarks of an effective corporate governance regime. The Board of Directors (BoD) is ultimately responsible for establishing a corporate vision, strategy and business model and for overseeing an institution's corporate governance culture and is expected to develop mechanisms including board committees to achieve this objective. Senior management is responsible for ensuring the effective functioning of the corporate governance framework on a day-to day basis.

Board of Directors (BoD)

11. Members of the BoD should have a good understanding of the institution's business model and operations and the general business climate in which it operates. They should have the qualifications and experience necessary to understand the institution's business model and operations and how these relate to Liberia's general economic and social environment. The BoD should ideally be comprised of both executive, non-executive and independent directors to ensure a desirable level of independence from the institution's management function.

12. The BoD should establish the institution's overall risk appetite and should ensure that mechanisms are in place to effectively mitigate risk. The BoD must ensure that appropriate policies, procedures and controls are in place to manage such risks and should also ensure that arrangements are in place for the effective reporting on all issues related to the functioning of the risk management framework. The BoD is ultimately responsible for the institution's operations, its management of the risk to which it is exposed and its compliance with all laws, regulations and guidelines to which it is subject.

Senior Management

13. An institution's senior management is responsible for implementing the corporate vision, strategy and business model approved by the BoD. Senior management should demonstrate a firm understanding of all aspects of the institution's business model and is responsible for developing

the components of the risk management framework. Senior management is responsible for ensuring that the institution has all the resources necessary to effectively manage risk. They are also responsible for ensuring that effective communication and reporting arrangements are in place to support good risk management practices. This includes ensuring that all staff members are aware of the requirements of the risk management framework and their specific roles and responsibilities. Senior management is responsible for ensuring that internal reporting mechanisms, including reports to be sent to the BoD, are developed to provide accurate and timely information relevant to the effective management of risks.

14. *The Risk Management Function*

a) To carry out the day-to-day risk management function, a dedicated risk management function should be established by financial institution.

b) An effective risk management function should:

i. have clearly defined responsibilities;

ii. have a direct reporting line to the relevant risk management committee or senior management;

iii. be independent from the business units that generate risks; and

iv. be supported by an effective management information system; and be given adequate resources to perform its duties and staffed by persons with the relevant expertise and knowledge.

c). The responsibilities of the risk management unit include:

i. to ensure that the risks are well understood and adequately assessed before a transaction is entered into;

ii. to ensure that the established policies and control procedures in respect of risk management are implemented and complied with;

iii. to monitor the use of risk limits and ensure that quantifiable risks are within the approved limits structure. This will include ensuring that the risk exposures of individual business units in respect of various risks are properly aggregated and monitored against the aggregate limits for the institution as a whole; and

iv. to ensure that the risks are properly measured and promptly reported to the relevant risk

management committee or senior management.

15. ***Risk management information system***

a) Financial institutions should establish and maintain a management information system which can effectively measure and report on the risks of major functions, products or business activities.

b) An effective risk management information system should produce timely, accurate and reliable reports to the board, senior management and line managers to support decision making at the different levels.

c) The level of sophistication of the system depends on the nature, scale and complexity of a financial institution's business and the products involved. Generally, it should be capable of measuring the risk of a product or an activity in accordance with the measurement methods or models adopted;

i. aggregating data on a product, functional, geographical and group basis;
ii. conducting variance analysis against annual budget or targets;
iii. alerting the management, e.g. when a risk exposure approaches a pre- set limit;
iv. reporting excesses and exceptions;
v. facilitating the allocation of capital charges to the business products and activities according to the level of risk-taking; and
vi. calculating risk-adjusted performance

To remain effective, the system should be subject to regular upgrades and modification.

New products and services

16 Services and activities that are new to a financial institution should be subject to a careful evaluation or pre-implementation review to ensure that the board or its designated committee and management fully understand the risk characteristics and that there are adequate staffing, technology and financial resources to launch the product or service.

17. Proposals to introduce new products or services should generally include:

a) a description of the product or service;

b) a detailed risk assessment;

c) a cost and benefit analysis;

d) consideration of the related risk management implications and identification of the resources required to ensure effective risk management of the new product or service (e.g. system enhancement);

e) an analysis of the proposed scale of new activities in relation to the financial institution's overall financial condition and capital strength; and

f) the procedures to be used for measuring, monitoring and controlling the risks.

18. All the relevant departments e.g. risk control, accounting, operations, legal and compliance should be consulted as appropriate, before a new product or service is launched. New products or services which could have a significant impact on an institution's risk profile should be brought to the attention of the board or its designated committee.

19. Financial institutions should perform a post launch evaluation of new products, the results of which should be taken into account for the development of any similar products or services in the future.

Policies and Procedures

20. Senior management should develop policies and procedures to effectively manage the ML/TF risks that arise from an institution's operations. Policies and procedures developed by senior management should be approved by the BoD. Policies and procedures should set out the day-to-day measures that should be employed to ensure that the institution effectively identifies, measures, monitors and controls ML/TF risks. The policies and procedures should therefore be developed to reflect the risks implicit in an institution's customers, products and services, delivery channels and geographic regions. Policies and procedures should be comprehensively documented and communicated to all staff. They should also be subject to periodic review to ensure they are appropriate in regard to changes to the institution's ML/TF risk profile.

21. Policies and procedures should clearly set out lines of responsibility and

accountability for the execution of the risk management function and should also establish effective reporting lines for all persons and business units involved in the management of ML/TF risks.

22. An effective risk management framework should establish limits in the context of the institution's stated appetite for ML/TF risk and the overall effective implementation of the risk management system. Policies and procedures should limit, for example, an institution's exposure to the ML/TF risks arising from exposure to specific types of customers, products and services, delivery channels and geographic regions. An effective ML/TF risk management framework should include a mechanism to report incidents where established limits have been breached and the frequency of such events.

Enhanced and Simplified Due Diligence Measures

23. The level of identified risk will determine the level of due diligence that is required. Any due diligence that is completed should be in line with institution's documentation policies and procedures and should be documented for future reference. Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is appropriate where there is little opportunity or risk of your services or customer becoming involved in money laundering or terrorist financing. Enhance Due Diligence is required where the customer and product/service combination is considered to be a greater risk. This higher level of due diligence is required to mitigate the increased risk. A high-risk situation generally occurs where there is an increased opportunity from money laundering or terrorist financing through the service and product you are providing or your customer. According to FATF standards, where the risk of ML/TF is higher, an enhanced CDD measures must be taken and, where the risks of ML/TF are lower, simplified CDD measures may be taken. These enhanced and simplified measures are outlined below:

Enhanced due diligence measures for high risk customers/transactions

24. Every financial institution should examine and document, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of ML/TF are higher, financial institutions should be required to conduct enhanced due diligence (EDD) measures for higher-risk business relationships which may include:

i. Obtaining and verifying additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet search, etc.);
ii. Updating more regularly the identification data of customer and beneficial owner;
iii. Obtaining and verifying additional information on the intended nature of the business relationship;
iv. Obtaining and verifying information on the source of funds or source of wealth of the customer;
v. Obtaining and verifying information on the reasons for intended or performed transactions;
vi. Obtaining and verifying the approval of senior management to commence or continue the business relationship;
vii. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and
viii. Requiring the first payment to be carried out through an account in the customer's name with a financial institution subject to similar CDD standards.

Simplified CDD measures for low risk customers/transactions

25. Where the risks of ML/TF are lower, the financial institutions are subject to Liberia's AML/CFT laws and regulations, allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring).

Examples of possible measures are:

i. Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (delayed verification);
ii. Reducing the frequency of customer identification updates;
iii. Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold;
iv. 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; and

26. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF, or where specific higher-risk scenarios apply.

Internal Controls

27. An on-going system of internal controls is an essential component of a risk management framework. Financial institutions should employ measures on an on-going basis to ensure adherence to establish policies and procedures as well as relevant laws, regulations, and guidelines.

28. Arrangements should be in place to reinforce the "four eyes"[i] principle and avoid conflicts of interest. Measures should be employed, for example, to ensure adequate separation between operational and control functions such as front office and back office activities.

29. Financial institutions should develop effective internal audit arrangements. The internal audit function should be an independent function with a direct reporting line to the Board Audit Committee. The internal audit function should periodically assess the effectiveness of the institution's ML/FT risk management framework and practices paying specific attention to the institution's adherence to established policies procedures and limits and applicable laws, regulations and guidelines.

30 Financial institutions should ensure that their ML/TF risk management framework and practices are subject to external audit review.

The Compliance Function

31. Financial institutions should develop an effective compliance function as a component of its ML/TF risk management framework. The compliance function should be commensurate with the, size, nature and complexity of the institution's business model and operations. The compliance function is separate from the internal audit function as it is a component of an institutions day-to-day operational activity. The compliance function should on an-ongoing basis assess the extent to which the institution is complying with established policies, procedures and limits and obligations arising from applicable laws, regulations and

guidelines. The effectiveness of the compliance function rests heavily on the effectiveness with which the Management Information System (MIS) generates accurate and timely reports related to the management of ML/TF risks. Compliance officer should possess sufficient seniority and knowledge and be up to date with recent laws and regulations.

Training

32. Financial institutions should have effective arrangements in place to train their staff and BoD on all issues related to their AML/CFT regime. It is important that staff understand the institution's inherent ML/TF risks and the nature of the measures that have been developed to mitigate these risks. Training must be provided for all staff upon joining the institution and should be an-ongoing activity. Apart from general training provided to all staff, targeted training programs should be developed for specific categories of staff in light of the nature of their work in the context of ML/FT risks. AML/CFT awareness programs should be conducted for members of the BoD.

PART IV: THE RISK ASSESSMENT PROCESS

General Principles

33. The Guideline provides high- level minimum requirements rather than prescriptive criteria for undertaking ML/TF risk assessments. CBL will review an institution's ML/TF risks assessment as part of its risk-based supervisory process.

34. In determining the methods or models to be adopted for risk measurement, a financial institution should consider the following factors:

- nature, scale and complexity of its business activities;
- the business need (e.g. for pricing);
- assumptions of the methods or models;
- data availability;
- the sophistication of its management information system; and
- staff expertise.

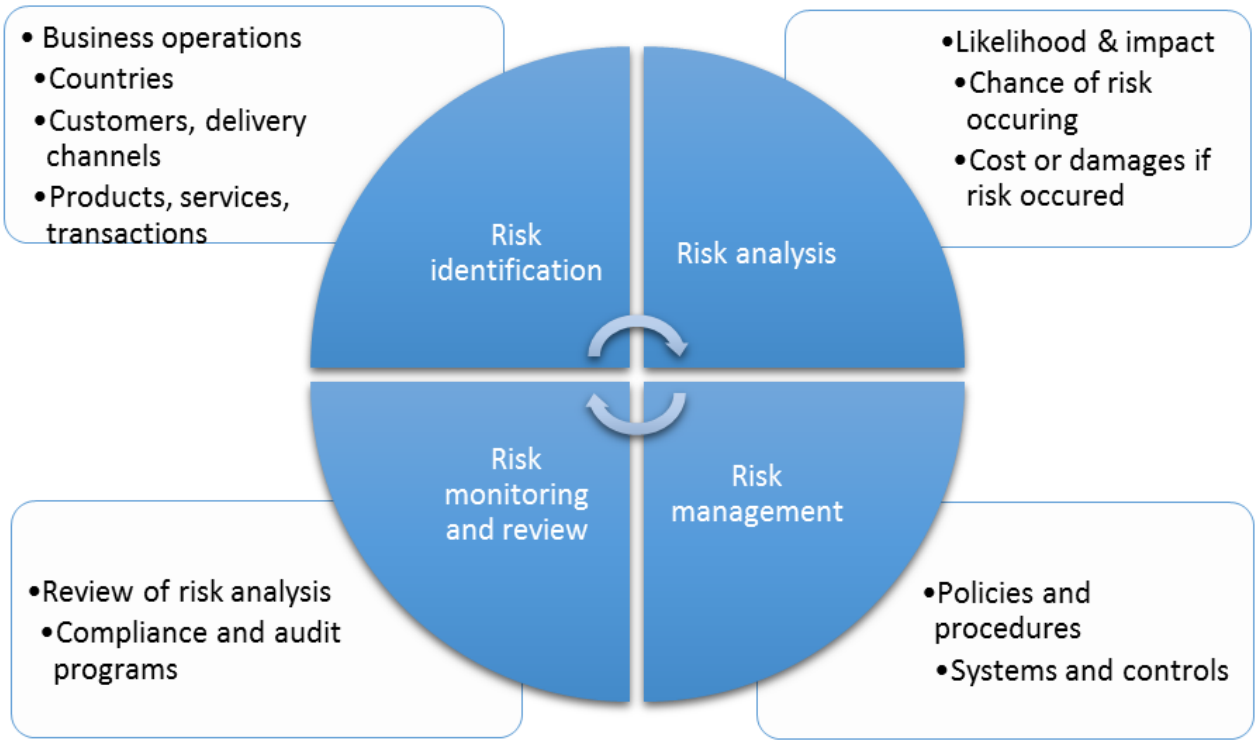
- The board or its designated committee and senior management should understand the underlying assumptions used and constraints of the methods or models chosen. They should also satisfy themselves as to the adequacy and appropriateness of the key assumptions, data sources and procedures used to measure the risks.
- The accuracy and reliability of a risk measurement method or model should be verified against the actual results through regular back-testing. The measurement method or model should also be subject to periodic updates to reflect changing market conditions.
- Whatever format management chooses to use for its risk assessment, it should be relevant and easily understood by all appropriate parties.
- The risk assessment should provide a comprehensive analysis of the ML/TF risks in a concise and organized presentation, and also be shared and communicated with all business lines across the financial institution, board of directors and management.

35. The ML/TF risk assessment undertaken should at a minimum:

a) 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;
b) Involve analysis of all available data to assess risks identified;
c) Evaluate the institution's AML/CFT compliance program;
d) Establish the residual risk for the risk categories identified;
e) Use appropriate weights and scoring;
f) Be specific to the institution and commensurate with the nature and size of the financial institution's business;
g) Document risk assessment conducted;.
h) Be subjected to internal review and approval by the board and management;
i) Methodology followed to undertake the assessment should be enumerated in a policy document; and
j) Kept up to date i.e. CBL Prudential Risk Management 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.

k) Risk Assessment Process



Identification of Specific Risk Categories

36. Attempts to launder money, finance terrorism, or conduct other illegal activities through a financial institution 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.

37. Customer Risk

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, insurance companies 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.

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

38. Products and Services Risk

Financial 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.

39. Delivery Channels Risks

Financial 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.

40. Geography/Country

This involves identifying geographic locations that may pose a higher risk to a financial institution'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 analyzed 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.

Financial 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; and
iii. Countries identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations 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.

41. Other Qualitative Risk Factors

The financial institution 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; and
- National Risk Assessments.

Detailed Analysis

42. Once the financial 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.

43. This step involves evaluating data pertaining to the financial institution's activities (e.g., number of domestic and international funds transfers, types of customers, geographic locations of the financial institution'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 financial institution'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.

44. Financial 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 high, 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.

Evaluation of the AML/CFT Program

45. 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.

46. 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.

Weights and Scoring

47. 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.

48. 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.

Residual Risk

49. 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.

50. 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 Very low (1), Low (2), Moderate (3), High (4) and Very High (5).

Residual Risk Computation (3 level rating scale)

RESIDUAL RISK	MITIGANTS		
INHERENT RISKS	Strong	Satisfactory	Weak
Low	Low	Moderate	Moderate
Moderate	Moderate	Moderate	High
High	Moderate	High	High

PART V: REPORTING TO THE BOARD OF DIRECTORS AND CBL

Reports to Board of Directors

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

52. 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.

Report to CBL

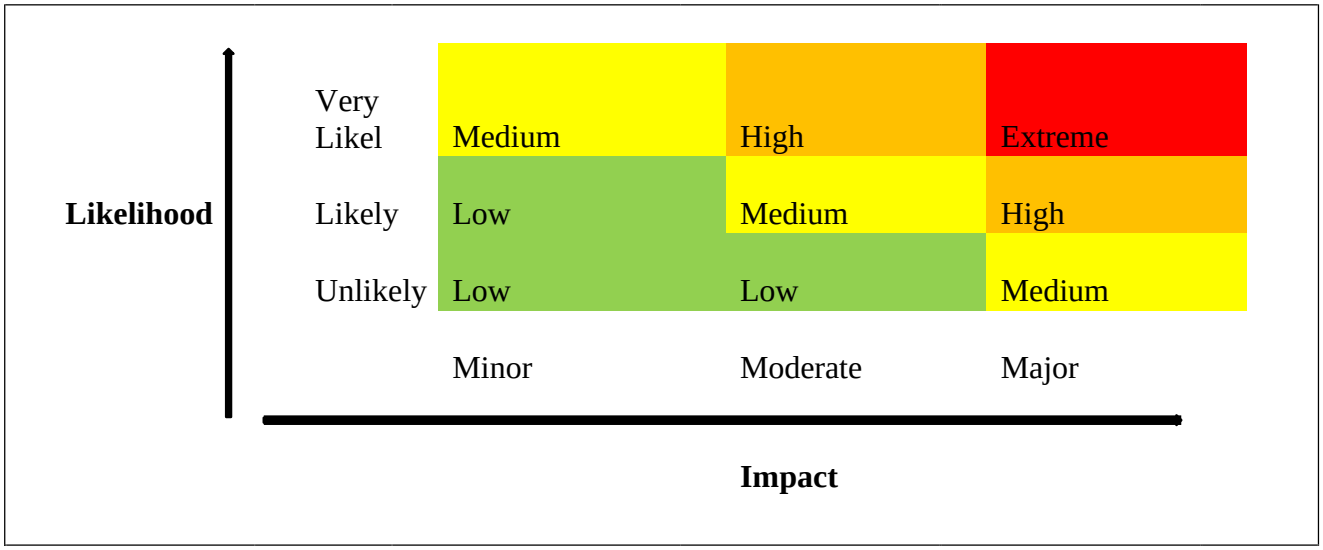
53. On an annual basis, institutions shall provide Central Bank of Liberia with a report on the latest results of its MT/TF risk assessment. The report should be submitted by 15th January of the following year.

In the event of any query or clarification, please contact:

The Director,
Regulation and Supervision Department
Central Bank of Liberia

Annex 1

Overall ML/FT Risk



[i] The Four eyes principle is a requirement that two individuals approve some action before it can be taken. The Four eyes principle is sometimes called the two-man rule or the two-person rule.