



Jamhuuriyadda Federaalka Soomaaliya  
Wasaaradda Maaliyadda  
Xafiiska Wasiirka

MOF/OM/1581/19

October 28<sup>th</sup> 2019

To:

Central Bank of Somalia  
Financial Reporting Centre

By the authority vested in me as the Minister of Finance by the Constitution under Article 99(b) and Article 52 of the Anti-Money Laundering and Countering financing of Terrorism act of 2016 ('AML/CFT').

**Having considered** the call of the National Anti-Money Laundering and Financing of Terrorism Committee (NAMLAC) dated June 29, 2019 where the committee resolved that the Ministry of Finance shall issue Anti-Money Laundering and Countering financing of Terrorism Regulation pursuant to its authority under the Constitution and the Laws of the Federal Republic of Somalia.

**Having taken into consideration** the comments received from the representatives of the Somali private Financial Institutions, Central Bank of Somalia, Financial Reporting Center and other stakeholders.

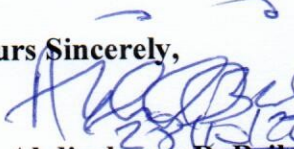
**Given** the need to address gaps that exist in the implementation and enforcement of AML/CFT regimes consistent with the best practices.

**Reaffirming** the commitment of the Federal Government of Somalia to restore and strengthen the nascent financial sector.

**Cognizant** that well-regulated and properly functioning financial sector is critical to revitalization the economy of the country, support financial intermediation and increase financial inclusion.

I Hereby issue AML/CFT regulation for the financial institutions (MoF/AML-CFT/REG/01) effective as of October 31, 2019. This regulation repeals, and replaces all existing AML/CFT regulations.

Yours Sincerely,

  
Dr. Abdirahman D. Beileh  
The Minister



**Federal Government of Somalia  
(Ministry of Finance)**

**ANTI-MONEY LAUNDERING &  
COUNTERING THE FINANCING OF  
TERRORISM (AML/CFT) REGULATION 2019**

**FOR**

**Financial Institutions**

**MoF/AML-CFT/REG/01**

**2019**

## ACRONYM AND ABBREVIATION

AML	-	Anti-Money Laundering
CBS	-	Central Bank of Somalia
CDD	-	Customer Due Diligence
CFT	-	Combating of the Financing of Terrorism
CTR	-	Cash Transaction Report
FATF	-	Financial Action Task Force
FRC	-	Financial Reporting Center
KYC	-	Know Your Customer
LCT/LCTR	-	Large Cash Transaction Report
LEA	-	Law Enforcement Agency
ML	-	Money Laundering
MTBs	-	Monet Transfer Businesses
NGO	-	Non-Governmental organization
NIC	-	National Identity Card
NPOs	-	Non-profit Organizations
PEP	-	Politically Exposed Person
STR	-	Suspicious Transaction Report
TF	-	Terrorist Financing
EFT	-	Electronic Fund Transfer

A7



1.	Article 1: PRELIMINARY	1
1.1	Authority	1
1.2	Citation	1
1.3	Application	1
1.4	Purpose:	1
1.5	Interpretation	2
2.	Article 2: AML/CTF Compliance Policies and Procedures	8
2.1	Designation of Compliance officer	9
2.2	Financial Institutions Risk Based Approach and Risk Assessment Requirement	10
2.3	Risk assessment	10
2.3.1	Retaining document for risk assessment	11
2.4	Staff Training and Awareness	13
2.4.1	Ongoing Training Requirement	14
2.5	Review the effectiveness of the AML/CFT compliance and procedures.	15
3.	Article 3: Customer Identification and Due Diligence Requirements	18
3.1	CDD measures used when Establishing Business Relationship	19
3.2	On-going Monitoring	19
4.	Article 4: Customer identification for Personal Accounts or Transactions	20
5.	Article 5: Identification of Natural Persons Acting on behalf of a customer	21
5.1	Obtaining and recording information regarding Beneficial Owners	21
6.	Article 6: Enhanced Due Diligence	22
7.	Article 7: Suspicious Transactions Reporting (STRs) Requirements.	23
8.	Article 8: Large Cash Transactions (LCTs) Threshold Reporting Requirements	24
9.	Article 9: Wire Transfers (Fund Transfers, incoming/outgoing) reporting requirements	24
10.	Article 10: Politically Exposed Persons (PEPs)	26
11.	Article 11: Shell Banks	26
12.	Article 12: NGOs, NPOs and Charities' Accounts	27
13.	Article 13: Prohibited relationships	27
14.	Article 14: Prohibition of anonymous accounts	28
15.	Article 15 : Reliance on Third Parties Intermediaries	28
16.	Article 16: Correspondent Banking Relationships	28



17.	Article 17: Record Keeping Requirements	29
18.	Article 18: Tipping-off Offences	30
19.	Article 19: AML/CFT Regulation on Asset Seizure and Confiscation	31
20.	Article 20: Cooperation with Law Enforcement	31
21.	Article 21: Sanctions;	32
22.	Article 22: Penalties for AML/CFT Non-Compliance	33
23.	Article 23: Supervision	34
24.	Article 24: Issuance of Circulars and Guidelines	34

A7

## **1. Article 1: PRELIMINARY**

### **1.1 Authority**

This Regulation is made by the Ministry of Finance pursuant to its authority set forth in Article 52 of the Anti-Money Laundering and Countering Financing Terrorism (AML/CFT) Law, 2016.

### **1.2 Citation**

This Regulation may be cited as the AML/CFT Regulation for Financial Institution, 2019.

### **1.3 Application**

This regulation applies to Financial Institutions such as Banks, Money Transfer Businesses, Mobile Money and other financial Institutions operating in the Federal Republic of Somalia as defined in the AML/CFT Act, 2016. This regulation will repeal all existing AML/CFT regulations for financial institutions.

### **1.4 Purpose:**

The objective of the AML/CFT regulation is to detect, deter and disrupt the money laundering and terrorists financing protecting Financial Institutions from being abused by financial crime practices, and thus, protecting their reputations and mitigating operational risk. Financial Institutions are required to fully cooperate with the requirement of this regulation and perform their duties in the fight against financial crimes, particularly in the provisions of information that may lead to investigations and prosecutions of money launderers and terrorist financiers.

These regulations aim among others the Financial Institutions requirements:

- a) To put in place policies, procedures, and controls and identify their customers to deter from financial crimes taking place.
- b) To develop policies on customer acceptance that clearly identify customers information and conduct CDD
- c) To keep records of their transactions.
- d) To designate an anti-money laundering compliance officer responsible for enforcing the policies, procedures, and controls.
- e) To submit reports on large cash transactions (LCT) and suspicious transactions reports (STR) to the FRC.





## 1.5 Interpretation

In this Regulation, unless the context otherwise requires, the terms below shall have the following meanings: -

“Agent” means any person who acts under the direction of or by contract with a registered or licensed Financial Institutions and thereafter may subcontract other agents in a network while retaining overall responsibility for the agency relationship with subagents;

“AML/CFT” means Anti-Money Laundering and Countering the Financing of Terrorism;

“Beneficial owner” means the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes persons who exercise ultimate and effective control over a legal person, business entity or a non-profit organization;

“Beneficiary/Recipient” means a customer record holder who receives money or assets transfer from another person;

“Branch” means any premises, other than its head office, at which the financial institution conduct businesses activities on its behalf in Somalia;

“Business entity” means any firm, whether or not a legal person, which is not an individual and includes a corporate body or other, unincorporated association;

“Business Relationship” means a business, professional or commercial relationship between a Financial Institutions and a customer, which is expected by the Financial Institutions, at the time when contact is established, to have an element of duration;

“Central bank” means the Central Bank of Somalia;

"Central Bank of Somalia Act" means the Central Bank of Somalia Act, No. 130 of 2012;

"Competent authority" means a public authority other than a self-regulatory body with designated responsibilities for combating money laundering and/or financing of terrorism;

"Control" in relation to a Financial Institutions means a situation where:

- a. One or more persons acting in concert, directly or indirectly, own, control or have the powers to vote five percent or more of any class of voting shares of the business;
- b. One or more persons acting in concert, control in any manner, the election of a majority of the directors, trustees, or other persons exercising similar functions, of the business; or
- c. Any circumstances exist which indicate that one or more persons acting in concert, directly or indirectly, exercise a controlling influence over the management, policies or affairs of the business;

"Customer" means a person (including both originator of account holder or recipient of money transfers) with whom the Financial Institutions establishes a business relationship;

"Customer Record", in relation to Financial Institutions, means a record of the customer identity information as held by a Financial Institutions;

"Director" includes any person occupying the position of director of a Financial Institutions by whatever name called and includes a person in accordance with whose directions or instructions the officers of a Financial Institutions are accustomed to act and includes an alternate or substitute director;

"Enhanced due diligence" means customer due diligence that should be conducted by a Financial Institutions where the money laundering/financing of terrorism risks are assessed as higher risk;

"Financial Institution" means any natural or legal person who conducts as a business activities defined in the Financial Institutions Law, 2012 or one or more of the following activities or operations for or on behalf of a customer:



- 1) Acceptance of deposits and other repayable funds from the public, including private banking;
- 2) Lending, including consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting);
- 3) Financial leasing, not extended to financial leasing arrangements in relation to consumer products;
- 4) The transfer of money or its equivalent, including financial activity in both the formal or informal sector;
- 5) Issuing and managing means of payment (e.g. credit and debit cards, checks, traveler's checks, money orders and bankers' drafts, electronic money transfers);
- 6) Financial guarantees and commitments;
- 7) Trading in money market instruments (checks, bills, certificates of deposit, derivatives etc.); foreign exchange; exchange, interest rate and index instruments; transferable securities; or commodity futures;
- 8) Individual and collective portfolio management;
- 9) Safekeeping and administration of cash on behalf of other persons;
- 10) Otherwise investing, administering or managing funds or money on behalf of other persons;
- 11) Money and currency changing;
- 12) Electronic money also known as e-money services.
- 13) The acceptance of cash, checks, and other payment instruments, mobile money (also including other stored-value products), in one location, and payment of a corresponding sum in cash or other form to a beneficiary in another location. Transactions performed by such services can involve one or more intermediaries, participation into a system, and a final payment to a third party, and may include any new payment method.
- 14) Participation in the securities issues and the provision of financial services related thereto
- 15) Underwriting and placing of life insurance and other investment related insurance.

"Financial Institutions Law" means the Central Bank of Somalia Financial Institutions Law No. 130 of 22 April, 2012;



"Financing of terrorism" means the act of, directly or indirectly, providing or collecting funds, or attempting to do so, with the intention that they should be used or in the knowledge that they are to be used or in whole or in part for any purpose:

- a. in order to carry out a terrorist act; or
- b. by a terrorist; or
- c. by a terrorist organization; or
- d. to finance a foreign terrorist fighter

"Large Cash Transactions" transactions or series of transactions (linked transaction) that appear to be linked which exceed the designated threshold of USD \$10,000 or the equivalent in any currency as described in Article 14 of the AML/CFT Act 2016.

"Money laundering" means the conversion or transfer of any property including money, knowing it is derived from a criminal offence, for the purpose of concealing or disguising its illegal origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of its actions ; the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property knowing that it is derived from a criminal offence; or the acquisition, possession or use of property knowing at the time of its receipt that it is derived from a criminal offence;

"Non face-to-face customer" means a customer with whom the Financial Institutions has not had direct interaction at the time of opening a customer record;

"Non-profit organization" means any organization, whether or not a legal person or arrangement, that

primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes or any other similar activity;

"Occasional transaction" means a money transfer transaction carried out other than as part of a business relationship;



"Officer", in relation to a Financial Institutions , means a director or any other person, by whatever name or title he may be called or described, who carries out or is empowered to carry out functions relating to the overall direction, in Somalia, of that Financial Institutions or takes part in the general management thereof in Somalia;

"Person" means any natural or legal person, business entity or non-profit organization;

"Politically exposed person" or "PEP" means any person who is or has been entrusted with a prominent public function in the Federal Republic of Somalia or in other countries, for example, heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned entities, important political party officials and senior staff of nongovernmental organizations. All family members of such persons, and close associates who have business or financial relationships with such persons are also included herein;

"Shell bank" means a bank that has no physical presence in the country in which it is incorporated or licensed, and which is not affiliated with a regulated financial services group, that is subject to effective consolidated supervision. Physical presence means having meaningful decision making structures and management located within the jurisdiction, which is responsible for supervising and regulating the company.

"Reasonable measures" means appropriate measures which are commensurate with the money laundering or financing of terrorism risks;

"Sanctioned person" means a person prohibited from doing business with financial institutions;

"Suspicious transaction" means a transaction described in Article 14 of the AML/CFT Act 2016.

"Sender/originator" means a customer who requests a Financial Institutions to send money or an asset to transfer to another person;

"Stored-value product" means a card or other tangible object for which a person pays in advance a sum of money to the issuer in exchange for an undertaking by the issuer that on production of the card or other tangible object to the issuer or a third party (whether or not some other action is required), the issuer or the third party, as the case may be, will supply goods or services or both goods and services;

"Structuring" means to conduct or to attempt to conduct one or more transactions in any amount at one or more financial institutions on one or more days in any manner for purposes of evading the reporting requirements set in these Regulation;

"Sub-agent" means a person who acts under the direction of an agent to provide financial services to customers.

"Terrorist act" means an act, which constitutes an offence within the scope of, and as defined in any one of the treaties listed in the annex to the 1999 International Convention for the Suppression of the Financing of Terrorism; and any other act that is intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.





## 2. Article 2: AML/CTF Compliance Policies and Procedures

1. Financial Institutions should develop risk-based internal policies, procedures, systems and controls to combat money laundering and terrorism financing. The internal policies and controls must indicate the Institution commitment to comply with this regulation and AML/CFT Act, 2016 to prevent any transaction that facilitates ML/TF activities.
2. Policies, procedures and controls should address risk assessment of the customer, products, services, geographic locations, and delivery channels as well as transactions.
3. Financial institutions should monitor transactions, including identifying unusual or suspicious transactions.
4. Financial Institutions should report Suspicious Transaction and Large Cash Transaction to FRC
5. Written compliance policies and procedures should be developed and implemented by the enterprise-wide and subject to Somalia's AML/CFT Act.
6. The compliance policy and procedures shall be in a written form, periodically revised.
7. The organization's written Policy and Procedures outlines the AML/CFT obligations applicable to Entity's business. It must also reflect the corresponding process and controls the organization make them in place and in principal, the entity must have committed to comply the regulations.
8. Internal audit arrangements to check compliance with and effectiveness of the measures taken to apply this regulation. Persons responsible for internal audit shall also be responsible for assessing the overall adequacy of the anti-money laundering program in terms of risks identified in internal risk assessments and evaluating compliance with the program.
9. Financial Institutions Compliance Policy and Procedures should cover the following as by per requirements.
  - a) **Customer identification** and conduct related due diligence
  - b) **Keeping records** is part of the AML/CFT requirements. Retain copies STR/CTR, disbursement of funds. Internal memo, measures taking for high risk customers including management sign off.



- c) **Transaction reporting** requirements; all applicable report types; the filing of suspicious transaction reports, large cash transactions reports, or other electronic outgoing fund transfer reports.
10. Each Financial Institution's should have policies and procedures depends on the size, structure and complexity of the organization, expected level of exposure to ML/TF risks. The policies and procedures developed by financial institutions will play a pivotal role on the compliance program as they set out the standards that employees, agents, and others authorized to act on its behalf must meet.
11. Compliance programs should be clearly communicated, understood and followed by all those authorized to act on behalf of the financial institution; employees, agents , transactions and technical supports and operations.
12. Financial institution policies and procedures should be reasonably accessible to the relevant stakeholders. It is important to note that CBS will not only look at the policies and procedures, but will also focus on the completeness and, the Financial Institutions demonstrate how they are effectively implemented during an examination.

## **2.1 Designation of Compliance officer**

1. Compliance Officer is responsible for the implementation of the Financial Institution's compliance program: policies and procedures, staff training, risk assessment, conduct periodic and effectiveness review.

### **The duties of the compliance officer:**

- a) The Compliance Officer should assume the necessary authority and access to resources to implement an effective compliance, so s/he can make desired changes. S/he should have the knowledge and the experience about the Entities business functions and structures. S/he should have the knowledge about Money Laundering and Terrorist Financing in the industry, the trends and the dynamics of the related criminal activities. S/he must be cognizant the regulatory and legislative requirements of the AML/CFT Act for Somalia and International bodies.
- b) The designated compliance officer can be the manager of the business, owner and depending the size and risk of the organization, a senior manager may be



designated for the position. Senior management and the Board should avail the necessary resources and make a commitment to support the Compliance Officer.

- c) A compliance officer may choose to delegate certain duties to other staff members. But, delegating certain compliance duties will not relinquish the compliance officer the ones to rightly and effectively implement the Company's compliance program. Compliance officer should report compliance related matters in writing and on regular basis to the Board of Directors or through senior management.
- d) Compliance Officer should periodically report to the Board Directors or through senior management.

## **2.2 Financial Institutions Risk Based Approach and Risk Assessment Requirement**

Financial Institutions are required to Develop and implement Risk Based Approach applicable to the entire AML/CFT Compliance program. they are also obligated to assess their risk exposures and develop procedures to prevent step by step, risk identified, mitigation measures and strategies used to manage the risks.

A Written compliance training program, reviewed periodically, and provided to all staff members, regulatory guide to test the effectiveness of the entity's compliance and implementation program are considered part of the preventive measures to risk exposure.

Know your Customer requirements applicable to verifying client identity, politically exposed persons, beneficial ownership when dealing with non-personal business activities, and verifying transactions whether the business activities is conducted on behalf of a third party.

## **2.3 Risk assessment**

A risk assessment is an analysis of potential threats, vulnerabilities and consequences that could expose the Financial Institution ML/TF activities. This regulation should be the basis for your organization to identify Financial Institutions' inherent risk and those authorized to act on their behalf in developing mitigation measures to deal with exposed risks.



The outcome of the risk assessment process and action taken should reflect the reality of the business, be documented and as a best practice include all the elements, applicable to the Financial Institution. The complexity of the risk assessment will depend on the size and risk factors of the business. Consideration is given to the following:

- a) Financial Institution business relationships aligned with their activity patterns and geographic locations;
- b) The products, services and delivery channels offered;
- c) The geographic location(s) where the entity conduct business activities;
- d) New technologies and their impacts on the customers, business relationships, and products or delivery channels used by the customers;
- e) other relevant factors affecting your individual business and also risks exposed or identified by other financial services entities for example; Insurance or Takaful entities, non-bank organizations. Professional and Associations who are subject to reporting obligations.

### **2.3.1 Retaining document for risk assessment**

1. Central Bank of Somalia requires that a financial institution demonstrates that all factors of the business risk exposure to Money Laundering and Terrorist Financing are considered, shall document all the risks considered and the mitigation measures taken to prevent identified high risk situation.
2. Financial Institutions are also required to show the risk assessment is reviewed, updated and documented every year, and mitigation measures as applicable. For example, if the financial institution offers a new product, Regulator expects that consideration has been taken to document any potential or actual ML/TF risks associated with the new product, and have identified and applied measures to deal with the identified risks.
3. Enhanced measures are the development and application of written policies and procedures to mitigate high risks identified within business and the customers. When customer is identified as potential a high-risk customer, a financial institution must:
  - a. Take additional steps to identify those risk factors attributed as the bases of the risk factors.
  - b. Conduct enhanced ongoing monitoring of your business relationships for the



purpose of:

- I. Detecting suspicious transaction that are required to be reported to FRC.
- II. Keeping client identification information, beneficial ownership (if applicable), and the purpose and intended nature of the business relationship records up-to-date;
- III. Re-assessing the customer's risk level based on their documented transactions and activities; and
- IV. Determining whether the transactions or activities are consistent with "what you know" about that client.

1) **Take any other enhanced measure to mitigate the risks. This could include:**

- a) Obtaining additional information on a client (e.g. volume of assets, information available through public databases, Internet, etc.);
- b) obtaining information on the source of funds or source of wealth of a client;
- c) obtaining information on the reasons for attempted or conducted transactions;
- d) increasing the frequency of the monitoring of higher-risk transactions, products, services and channels;
- e) gathering additional documentation, data or information, or taking additional steps to verify the documents obtained;
- f) establishing transaction limits;
- g) increasing internal controls for high-risk business relationships;
- h) Obtaining the approval of senior management for products and services that are new for customer, or use any other measures you deem appropriate.

Financial Institutions should have processes to identify, assess, monitor, and mitigate money laundering and terrorism financing risks. Effectively assess the risk a business relationship may expose or will involve, money laundering or terrorist financing. The risk assessment and any underlying analysis and information shall be documented in writing, be kept up-to-date and readily available for examination for the Central Bank of Somalia.

1. Financial Institutions shall be able to demonstrate to the examiner "CBS" that their CDD measures are appropriate taking into consideration the risks of



money laundering and terrorist financing and that it has gathered relevant information to carry out the risk assessment requirement.

2. Financial Institutions shall keep records of risk assessments and keep them up to date.

**The following factors are to be considered by Financial Institutions when conducting their risk assessments:**

- a) The full customer's details including, nature of their business, occupation, or
- b) Anticipated transaction activity.
- c) Country in which customers operate or the place of origination or destination of transactions.
- d) The source and origin of the customer's funds and delivery channels.
- e) The purpose of an account or relationship and products and services requested (i.e. risks that may be associated with the products and services offered)
- f) Assessment of the risks associated with the size of transactions or deposits of the customer.
- g) Assessment of the risks associated with the frequency of transactions or duration of the relationship.

#### **2.4 Staff Training and Awareness**

1. Financial Institutions shall implement suitable training program for their staff and management, which should be documented, in order to effectively implement the regulatory requirements and financial institutions own policies and procedures relating to AML/ CFT. Also, refresher training should be arranged at regular intervals i.e. at least annually to ensure that staff do not forget their responsibilities.
2. Employees training shall continuously and effectively update their skills and enable them to understand the new developments, money laundering and financing of terrorism techniques and methods.
3. Employees training shall be included real-world examples of transactions that constituted money laundering and terrorist financing, and an awareness of the role that staff play in the overall process of detecting and punishing money launderers and terrorist financiers



#### **2.4.1 Ongoing Training Requirement**

- a) Develop and implement ongoing compliance training program, required from Financial Institutions to offer their employees, agents or individuals authorized to act on their behalf. Also, those who deal with customers in relations with their functions, duties including the support.
- b) Training program must be in writing, periodically reviewed and kept up to date.

#### **2.4.2 Those acting on behalf of the financial institutions, training program should address, individual participants must understand;**

- a. Organization's obligations, as a financial institution under the regulations;
- b. Covering the ways and how the entity could be vulnerable to ML/TF activities;
- c. Financial Institution's policies and procedures stemming from your obligations under the AML/CTF; and
- d. Employees/agents roles in detecting and deterring ML/TF activities, ranging from low to high risk situations.

#### **2.4.3 Training program should be delivered and tailored to the following people:**

- a. contact with clients such as front line staff or agents;
- b. are involved in client transaction activities;
- c. Handle cash or funds in any way; and responsible for implementing or overseeing the compliance program (such as senior management, information technology staff or internal auditors).

#### **2.4.4 At minimum, training program shall address the following:**

- a. Understand ML/TF concepts, have background information on ML/TF in relation with financial institution business, offer definitions of ML/TF, why criminals choose to launder money and how the process for ML/TF usually works. Introduce regulator website and information about CBS and Financial Report Centre and their legal roles.



- b. Entity compliance policies and procedures for preventing and detecting ML/TF, utilizing internal control guide, customer identification, identification of the beneficial owner, transaction reporting, know-your-client, and record keeping obligations.
- c. Ensure participants adequate understanding with respect to their responsibilities, give examples, how the entity's particular business could be used to launder money or financing of terrorism or other illicit financing.

While the organization has the flexibility on how training program is delivered, electronically, face to face meeting, through software or attending local and international conferences, written train manual must be document,

Part of the written document, financial institutions must indicate; who needs to be trained, type of training, topics covered, frequencies, such as, annual or twice a year. Employee must not handle company business until they are trained. There must be a training log sheet showing, participant names, and their initials, date, started-end time and location.

## **2.5 Review the effectiveness of the AML/CFT compliance and procedures.**

Effectiveness review is an evaluation that is conducted periodically, testing the efficacy of the elements of a financial institution's compliance program, the policies and procedures, risk assessment and the training program. Frequencies of independent testing may conducted every two years, however, a financial institution may conduct internal review more frequent for internal control purpose. For best practice, review must be designed to allow for the identification and documentation of any gaps and weaknesses within the compliance program and implementation to ensure that the business process is effectively detecting and preventing money laundering and terrorist financing activities.

- a. In the case of the policies and procedures and training program, a review is required to assess that the entity is effectively meeting their requirements under the AML/CFT regulations.

- b. In the case of the risk assessment, a review is required to determine whether the risk assessment is effective at identifying and mitigating the risks exposed regarding



Money Laundering and Terrorist Financing and relating to customers, agencies or affiliates products and services offered, delivery channels and geographic locations where the financial institution is doing business including their branches and where customer transfer funds or receive funds.

- c. The methods and scope used to test the effectiveness of the compliance program depends on the nature, size and complexity of a financial institution's business. Testing process must be documented as part of the review. The review should consider the completeness of all the components of your compliance program in addition to their effectiveness.
- d. The findings, frequency and timing of the review must be sufficiently documented and identify the root cause of the deficiencies identified by the institution reviewer. When any changes are necessary impacting the compliance policies and procedures, risk assessment or training program. The entity should ensure that the resulting compliance documents are updated timely, be available before next planned review.

**Example: review is included the following:**

- a. Interviews with those handling transactions to evaluate their knowledge about the policies and procedures and record keeping, client identification and reporting obligations.
- b. A review criteria and process for identifying and reporting suspicious transactions.
- c. A sample of account opening records followed by a review to ensure that client identification policies and procedures are being followed.
- d. A sample of large cash transactions followed by a review of the reporting of these transactions.
- e. A sample of electronic funds transfers followed by a review of the reporting of these transactions.
- f. A sample of clients followed by a review to see if the risk assessment was applied correctly.
- g. A sample of the clients followed by a review to see if the frequency of ongoing monitoring is adequate.

- h. A sample of high-risk clients followed by a review to ensure that enhanced mitigation measures were taken.
- i. A review of a sample of records to ensure proper record keeping procedures are being followed.
- j. A review of the risk assessment to ensure it reflects current operations.
- k. A review of the policies and procedures to ensure they are up-to-date with the current legislative requirements.

### **Acceptable Reviewer**

Internal or external auditor must conduct the review. However, if entity does not have such an auditor, entity is allowed to conduct their own review, which should be done by an individual who is not directly involved in the compliance program activities, and who has an adequate working knowledge of the obligations under the AML/CFT Laws. Documentation should also specify who conducted the review.

The review must address whether the policies and procedures, risk assessment and training program are effective, and whether the practices comply with legislative and regulatory requirements, regardless who performs it.

### **Reporting review results**

The following must be reported in writing to a senior officer, in writing s/he must instruct remedial action with a timeline:

- a. The findings of the review (e.g. deficiencies identified, planned corrective actions, an implementation timeline, etc.);
- b. any updates that were made to the policies and procedures during the reporting period; and
- c. The status of the implementation of the updates made to policies and procedures




### 3. Article 3: Customer Identification and Due Diligence Requirements

1. Financial Institutions shall conduct Due Diligence such measures taken by Financial Institutions shall achieve the following objectives:

- a) Identify the customer and verify that customer's identity using reliable, independent source documents, data or information;
- b) Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner such that the Financial Institution is satisfied that it knows who the beneficial owners are and it understands the ownership and control structure of the customers in case of legal persons, business entities or non-profit organizations;
- c) Verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person;
- d) Understand and as appropriate obtain information on the purpose and nature of the business relationship;
- e) Conduct on going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Financial Institution' knowledge of the customer, their business and risk profile, including where necessary the source of funds.

2. Financial Institutions shall identify and verify the identity of their customers when:

- a. Establishing business relationships;
- b. Carrying out occasional transactions or one off transactions equal to or exceeding the designated threshold of USD \$10,000 or the equivalent in any currency;
- c. Sending or receiving cash of any amount, or any transaction of any amount where money laundering or terrorist financing is suspected;
- d. In receipt of electronic transfer that does not contain complete originator information; and
- e. The Financial Institution has doubts about the veracity or adequacy of previously obtained customer identification data.

 Financial institutions shall ascertain the identity of the customer and have detailed

knowledge of the customer's business before entering into the business relationship. 7

### **3.1 CDD measures used when Establishing Business Relationship**

Financial institutions shall perform the following CDD measures when Establishing Business Relationship:

- a) Conduct Customer Due Diligence when establishing Customer Business relationship; verify their identity using reliable, independent source documents, data or information.
- b) -Identify whether is a third party individual (s) is involved in the transaction.
- c) Obtain information on the purpose and intended nature of the business relationship.
- d) Specify whether you are dealing with personal transaction or business accounts/transactions
- e) Monitor the business relationship on an on-going basis and examine any transactions carried out to ensure they are consistent with prior information obtained. For commercial activities conduct risk profiling and evaluations and where applicable, ask and record customer sources of funds.

### **3.2 On-going Monitoring**

1. Financial Institutions shall conduct ongoing monitoring on the business relationship with customers.
2. Financial Institutions shall, during the course of a business relationship with a customer, observe the conduct of the customer's record and scrutinize transactions undertaken throughout the course of the business relationship, to ensure that the transactions are consistent with the Financial Institutions background and knowledge of the customer, its business and risk profile, including the source of funds and intended purpose and nature of services.





3. For the purposes of ongoing monitoring, a Financial Institutions shall put in place and implement adequate systems and processes, commensurate with its size and complexity, to:
  - a. Monitor its business relationships with customers; and
  - b. Detect and report suspicious, complex, unusually large or unusual patterns of transactions undertaken throughout the course of business relationships.
4. Financial Institutions shall ensure that the customer due diligence data, documents and information obtained in respect of customers, natural persons appointed to act on behalf of the customers and beneficial owners of the customers, are relevant and kept up-to-date by undertaking reviews of existing customer due diligence data, documents and information, particularly for higher risk categories of customers.
5. The frequency of the on-going monitoring shall be commensurate with the level of money laundering and financing of terrorism risks posed by the customer based on the risk profiles and nature of transactions.
6. The findings and related documents shall be made available to the regulator upon request and in a timely manner.

#### **4. Article 4: Customer identification for Personal Accounts or Transactions**

1. A Financial Institution shall verify/ascertain the identity of their individual customers and in the case of Legal Entities, the person representing the Entity must be identified. The financial institution shall ensure that the customer is the person he/she claims to be. Third party verification for customer information on behalf of the financial institutions is only acceptable in the instances where the Financial Institution has a written agreement between them prior to identifying or verifying information for a customer on behalf of the Financial Institution.
2. Financial Institutions shall verify the identity of customer who is acting on behalf of a personal customer or legal entity. For legal persons, the following information should be obtained:
  - a) Name, legal form and proof of existence of the legal persons (revised; legal entity).

- b) The principal place of business of the legal person.
- c) Resolution of the Board of Directors to open an account and identification of those individuals who have authority to operate the account and names of relevant persons holding senior management positions.
- d) Mailing and registered address of legal person.
- e) Nature and purpose of the business.
- f) The identity of the beneficial owner.
- g) Verify and obtain information regarding beneficiary ownership
- h) Verify whether individual owners and executive officers are Politically Exposed Persons.

**5. Article 5: Identification of Natural Persons Acting on behalf of a customer**

1. For natural persons representing a legal entity, Financial Institutions shall verify the identity by using reliable, independently sourced documents, information.
2. The Financial Institutions shall identify any person acting on behalf of the customer is authorized to do so and shall be verified through documentary evidence including specimen signature confirming the customer is a legal person.
3. Monitor the business relationship on on-going basis and examine any transactions carried out to ensure they are consistent with their knowledge of the customer, commercial activities and risk profile, and where required, the source of funds.
4. For legal persons, understanding and documenting the beneficial ownership and control structure of the customer.

**5.1 Obtaining and recording information regarding Beneficial Owners**

1. Financial Institutions shall obtain information from beneficial owners and identify and verify the identity of the beneficial owners.
2. In the cases where financial institution decides that the customer is acting on behalf of beneficial owner, then they should take measures to verify the identity of the beneficial owner by using relevant information or data obtained from a reliable source such that



the financial institution is satisfied with the identity of the beneficial owner.

3. In the cases, Where the customers are other legal entities, the Financial Institutions shall obtain the ownership and control structure of the customer, including the natural person who ultimately owns or controls the entity as detailed below:

a) With respect to such legal entities identification should be made of each natural person that:

- i. Owns or controls directly or indirectly of the legal entity;
- ii. Is responsible for the management of the legal entity; or
- iii. Exercises control of the legal person through other means.

b) With respect to legal arrangements, identification should be made of the settlor, trustee, protector, and beneficiary or of persons in similar positions.

c) For Non-Governmental Organizations (NGOs) and non-profit organizations (NPO) (such as societies, charities etc.) the financial institution shall satisfy itself as to the legitimate purpose of the organization, including by reviewing its charter governing document.

## 6. Article 6: Enhanced Due Diligence

1. Financial institutions should apply enhanced due diligence measures to persons and entities that present a higher risk. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Following are the enhanced CDD measures that should be applied for high risk customers:-

a) Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.



- f) 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.

**7. Article 7: Suspicious Transactions Reporting (STRs) Requirements.**

1. Financial Institutions shall comply with the provisions of AML/CFT Act, 2016 and this regulation by implementing appropriate internal policies, procedures and controls on suspicious transaction monitoring and reporting.
2. Financial Institutions shall pay close attention to all unusual large transactions, and unusual patterns of transactions, which have no apparent economic or visible lawful purpose.
3. The completed STR should be reported to the FRC in the prescribed within fifteen (15) days from date of the transaction for completed or attempted suspicious transactions.
4. The STRs submitted to FRC shall contain full information about the transactions as recorded in the time of transaction.
5. If information received is incomplete or further details are missing, the Financial Institution will be notified about the insufficiency of the data. A Financial Institution must return the requested information, providing the time line that may not exceed 15 days prescribed for the filing Suspicious Transaction Reports to FRC.
6. When deemed necessary, the Central Bank of Somalia in consultation with FRC may change the STRs reporting timeline.

**8. Article 8: Large Cash Transactions (LCTs) Threshold Reporting Requirements**

1. Financial Institutions shall report to the FRC any transactions or series of transactions (linked transaction) that appear to be linked which exceed the designated threshold of USD \$10,000 or the equivalent in any currency under Reporting obligations Art. 14 of the AML/CFT Act, 2016.





2. Financial Institutions shall report the full details of large Cash Transaction Report (LCTR) to the FRC, within fifteen (15) days.
3. Financial Institutions shall include their report all required information as set out in the LCTR form. If incomplete report or carelessly filled out LCTR forms is submitted to FRC, the form shall be returned to provide further information.
4. When deemed necessary, the Central Bank of Somalia in consultation with FRC may change the LCTs reporting timeline.

**9. Article 9: Wire Transfers (Fund Transfers, incoming/outgoing) reporting requirements**

1. Financial institutions, when undertaking wire transfers, shall:
  - a. Obtain and maintain the name of the originator and, for wire transfers equal to or above USD \$1,000 or the equivalent in any currency, identify and verify the identity of the originator;
  - b. Obtain and maintain the account number of the originator, or, in the absence of an account number, a unique reference number;
  - c. Obtain and maintain originator's address or, in the absence of an address, originator's the national identity number or date and place of birth; and
  - d. Obtain the name and account number, or a unique reference number, of the beneficiary;
  - e. Include information from (a) through (d) above in the message or payment form accompanying the transfer.
  - f. In the event that the identity of the originator or the beneficiary equals persons or entities designated under UN Security Council resolutions 1267 and 1373, send a report without delay to the Financial Reporting Center.
2. Notwithstanding the requirements of subsection (1), a financial institution is not required to verify the identity of a customer with which it has an existing business relationship, provided that it is satisfied that it already knows and has verified the true identity of the customer.

3. When a financial institution acts as an intermediary in a chain of payments, it shall ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.
4. If financial institutions receive wire transfers that do not contain the complete originator information required under that paragraph, they shall take measures to obtain and verify the missing information from the ordering institution or the beneficiary. Should they not obtain the missing information, they shall refuse acceptance of the transfer.
5. Financial Institutions have to report incoming and outgoing international electronic funds transfers (EFTs) of \$10,000 USD or more or with equivalent currency to FRC within 15 days.
6. When deemed necessary, the Central Bank of Somalia in consultation with FRC may change the EFTs reporting timeline.





## **10. Article 10: Politically Exposed Persons (PEPs)**

1. In relation to Politically Exposed Persons (PEPs) and their family members or close associates, the Financial Institutions shall establish appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP, and if so, apply the following EDD measures;
  - a) Obtain approval from senior management before establishing or continuing a business relationship with such a person or beneficial owner, where the customer or a beneficial owner is PEP or subsequently becomes a PEP;
  - b) Taking all necessary steps, Identify the sources of wealth, sources of funds, and obtain information from individuals identified as PEPs
  - c) During the course of business relations, apply enhanced on-going monitoring to the business relationship.
2. Procedures for determining whether a customer or beneficial owner is a PEP, include the following:
  - a) Seeking relevant information from the customer or beneficial owner.
  - b) Accessing and reviewing available information from reliable source about the customer or beneficial owner. (Use publicly available data from governments, international organizations, Google may all publish reliable information)
  - c) Searching and accessing commercial or non-confidential electronic databases of PEPs, further information may also be available through Google engine).


## **11. Article 11: Shell Banks**

1. Financial Institutions shall not establish or continue a correspondent or business relationship with a shell bank and they must satisfy themselves that respondent Financial Institutions do not allow their accounts to be used by these shell banks.
2. The above obligations shall be applied by Financial Institutions to cross border correspondent banking and similar relationships established before the authorization of this Regulation and or the AML/CFT Act 2016.

## **12. Article 12: NGOs, NPOs and Charities' Accounts**

1. When establishing relationship with Non-Governmental Organizations (NGOs), not-for-Profit Organizations (NPOs) and Charities, the Financial Institution should conduct EDD to ensure that these accounts are used for legitimate purposes and the transactions are matching with the objectives and purposes of the entity. The individuals who are authorized to operate the accounts and members of their governing body are subject to enhanced CDD. Information obtained from NGOs/NPO and Charities organizations should be monitored and reviewed on an ongoing basis, their authorized personnel, members of their governing body including executive officers should be periodically updated. When discrepancies are noticed management must be alerted. And if necessary, STR may also be filed by the Financial Institutions' compliance Officer.
2. Financial Institutions are obligated to follow enhanced due diligence including obtaining and verifying relevant information about Directors and officers of the organization must be met before relationship is established. Timing of identifying customer and gathering information must take place before accounts or any transactions are conducted. In cases, where potential customer refuse, provide inconsistent information or resists to offer detailed information, Financial Institutions may file Suspicious Transaction Report, even if information on hand is incomplete.

## **13. Article 13: Prohibited relationships**

1. Financial Institutions are prohibited from establishing or maintaining business relationships with a shell bank (or any financial institution with no physical presence) in the jurisdiction in which it is incorporated or licensed.
  2. Financial Institutions are prohibited from doing business with sanctioned persons or entities imposed by the Ministry of Finance or other international authorized bodies..
-  Financial institutions are required to develop detailed policies and procedures that



identify sanctioned persons or entities.

**14. Article 14: Prohibition of anonymous accounts**

Financial Institutions shall not keep anonymous accounts or accounts in obviously fictitious names. Any such accounts in existence prior to enactment of the AML/CFT Act shall be closed by a date stipulated by the Central Bank of Somalia, unless all identification requirements in the AML/CFT Act and this regulation are fulfilled.

**15. Article 15: Reliance on Third Parties Intermediaries**

1. Financial Institutions should pay a close attention to jurisdiction risks associated with the third party the entity is entering into a business relationship.
2. Financial Institutions should know that ultimate responsibility for customer identification and verification shall remain with them and not with the third party they are relying on.
3. Financial Institutions may only rely on third party intermediaries to perform the CDD requirements of this regulation if the following conditions are met:
  - a. They are satisfied that the third party is regulated, supervised or monitored for and has measures in place for compliance with the customer due diligence and record keeping requirements;
  - b. They are satisfied that copies of identification data and other documents relating to customer due diligence measures will be made available from the third party upon request and without delay.

**16. Article 16: Correspondent Banking Relationships**

1. Financial Institutions shall take the following measures, before entering into a cross-border correspondent banking relationship or other similar relationships:



- c. Collect sufficient information about the respondent bank to understand

the nature of its major business activities.

- d. Know their geographical local jurisdiction of correspondence.
  - e. Evaluate the money laundering and financing of terrorism prevention and detection measures and controls implemented by the respondent bank.
  - f. Assess the integrity of the respondent institution and the quality of supervision to which it is subject, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action in the respondent's country.
  - g. Fully recognize and document the respective AML/CFT responsibilities of each bank.
  - h. Acquire approval of senior management, before establishing new correspondent banking relationship.
2. Financial Institutions shall take extra precautions when establishing or continuing relationship with correspondent banks or Financial institutions which are located in jurisdictions that have been identified by FATF for having inadequate AML/CFT standards in the fight against money laundering and financing of terrorism.

## **17. Article 17: Record Keeping Requirements**

1. Financial Institutions shall maintain records on customer transactions, other information obtained when conducting the transaction. (e.g. inquiries to establish the background and purpose of unusual large transactions)
2. All records of identification data obtained through CDD process (such as; copies of identification documents, account opening forms, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a minimum period of five years after the business relationship is ended.
3. Financial Institutions shall establish and maintain a customer record for all customers when establishing a business relationship or before carrying out a transactions.
4. Financial Institutions shall keep customer records accurate and periodically updated.
5. Financial Institutions shall not keep anonymous customer records or customer records



in obviously fictitious names. Any such customer records in existence prior to the issuance of these Regulation shall be closed within three months of these Regulation' adoption unless all identification requirements in these Regulation and other relevant regulations are fulfilled.

6. Financial Institutions shall maintain, for at least five (5) years from the date of execution, all necessary records on transactions, both domestic and international.
7. Financial Institutions shall keep all records obtained through the customer due diligence process, including client files and correspondence records in accordance with subsection (1) above as well as the results of any client analysis undertaken for at least five years after the business relationship has ended or after the date of the transaction or ones the business relationship ceased.
8. The identification data, transaction records, customer due diligence information, client analysis etc. in client files and related correspondence shall be made available to the Central Bank of Somalia upon request and in a timely manner.
9. Financial Institutions shall maintain all copies of STRs sent and related documents for at least five years.

#### **18. Article 18: Tipping-off Offences**

Under Part II of AML/CFT Act, 2016 it is a criminal offence to inform or warn someone that he or she is under suspicion of money laundering or STR/SAR forms about their transaction or attempted transaction are being filled with FRC.

1. Employees and the directors of the financial institution are required by law to maintain confidentiality in respect of such investigation and any suspicious transaction report that may be filed with FRC or informed to the law enforcement agencies. Tipping off (doing or saying anything that might inform someone else that he is under suspicion of money laundering), is a criminal offence under the provisions of the money laundering law and financing terrorists.
2. No criminal, civil, disciplinary or administrative proceedings for breach of banking or

professional secrecy or contract shall lie against Financial Institutions or their respective directors, principals, officers, partners, professionals or employees who in good faith submit reports or provide information in accordance with the provisions of this regulation.

#### **19. Article 19: AML/CFT Regulation on Asset Seizure and Confiscation**

1. Proceeds of an offence, cash, instrumentalities of that offence, or any terrorist property can be subjected to seizure and confiscation through competent authorities as per the rules of AML/CFT Act, 2016.
2. Financial Institutions should therefore develop and implement procedures to ensure compliance with these requirements at all times. These requirements include:
  - a) Procedures to freeze without delay funds, property, instrumentalities and assets held by the financial institution, in response to directions received from competent authorities.
  - b) Procedures to monitor attempted access by customers or other parties to the funds, property or assets.
  - c) Procedures to allow access to the funds, property or assets held in response to directions from competent authorities.
  - d) Funds, Proceeds of an offence, instrumentalities of that offence, or any terrorist assets in response to directions from competent authorities.
3. Financial Institutions should submit a report to FRC without delay in relation to any attempt to access the funds, property, instrumentalities of the offence or assets which are subject to an order under this section.

#### **20. Article 20: Cooperation with Law Enforcement**

1. Central Bank of Somalia and Financial Reporting Centre augment to the criminal investigation by providing information on the money trail- that is uniquely available in the Financial Institutions. FRC receiving large number of transaction reports will assist the law enforcement agencies to connect the money or the assets to the crime.



2. FRC receives and analyzes information related to Money laundering or Terrorist Financing activity financing to assist in the ongoing investigations. Therefore, financial institutions shall assist the investigative efforts of the agency.

## **21. Article 21: Sanctions;**

1. AML/CFT legislative measures against Terrorists, Terrorist groups and other listed and sanctioned individuals are contained in the law. These imposes prohibitions, disclosures and the other compliance obligations targeting specific countries, individuals, and entities and their financial activities. These legislative measures apply to Somalis including those residing outside Somalia, and more particularly, including the regulated financial institutions. Somalia's sanctions law addresses measures that; designated persons, prohibited activity with respect to assets of designated persons, require disclosure of information concerning the assets to law enforcement authorities. In compliance with Somalia's CFT law requires Financial Institutions implement The Following types of control measures.

- a. Verifying whether customer records contain for individuals and entities designated by the law and subject to financial sanctions.
- b. Determine whether your organization is in possession or control of property of designated person or entity.
- c. Preventing prohibited activity with respect to property of Designated Persons (by freezing assets) and monitoring for and preventing prohibited transactions.
- d. Disclosing information to the relevant authority and filing Suspicious Transaction report to FRC.

2. Information about individuals and entities that Financial Institutions collect and develop in the "know your client" process, and any other information at their disposal, must be used to determine whether an individual or entity on their records is a Designated Person or sanctioned entity or a jurisdiction.

## 22. Article 22: Penalties for AML/CFT Non-Compliance

1. Any natural or legal person who violates the directions mentioned in this regulation is liable to sanctions provided in Articles 27, 28 and 29 of the AML/CFT Act, 2016. Sanctions and penalties imposed upon a legal entity or natural person can constitute any or all of the sanctions or penalties in any combination deemed appropriate based on the severity of the violations. Criminal penalties may be enforced against natural persons connected to the commission of an offence, in addition to the following penalties for ML or TF:
  - a) Imprisonment for not less than a year;
  - b) Fines of not less than USD \$1,000 or the equivalent in any currency and up to three times the amount of the money laundered; or combination of both.
2. Civil and or administrative penalties appropriate to the seriousness of the violation:
  - a) Fines of not less than USD \$1,000 or the equivalent in any currency and up to three times the amount laundered.
  - b) Temporary or permanent suspension of license or authorization to operate based on registration requirements.
3. Financial institution and their executive directors found to have failed to comply with this regulation, the regulator "CBS" may require, depending the extent of the violation to correct the situation within an agreed period of time. The entity must commit in writing procedures that the organization will take and precise actions showing a timeline. Civil and or administrative penalties appropriate to Entity and their administrators depending the seriousness of the violation be as follows:
  - a) All penalties and sanctions stipulated above for natural persons.
  - b) Imprisonment upon officers, directors, managers or board members who neglected their responsibility for prohibiting, preventing and implementation of effective systems to detect and prevent violations.
  - c) Monetary penalties not less than USD \$25,000 or the equivalent in any currency and not more than ten times the amount of the money laundered.



4. Violations to comply with ML/TF regulation which may lead to enforcement actions mentioned above include, but are not limited to:
- a) Failure to develop and AML/CFT Compliance Program pertinent to Risk relevant to the entity.
  - b) Failure to designate compliance officer.
  - c) Failure to report LCTs/EFTs or STRs to the FRC, as required.
  - d) Tipping off to customers that reports are being filed about them to the FRC or other competent authority.
  - e) Failure to respond inquiries of the regulator, or law enforcement rightly authorized for investigation.

### **23. Article 23: Supervision**

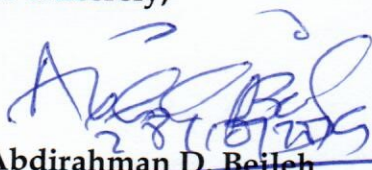
- 1. The Central Bank of Somali shall exercise supervisory powers over financial Institution and shall conduct onsite examination, offsite surveillance and may request for any information from Financial Institutions.
- 2. The Central Bank of Somalia shall be responsible for AML/CFT supervision over Financial Institutions, both on site and off site, and shall adopt a risk-based approach.

### **24. Article 24: Issuance of Circulars and Guidelines**

- 1. The Central Bank may issue circulars regarding the application or implementation of any provision of these Regulations to financial Institution.
- 2. The Central Bank shall issue guidelines regarding-
  - a) measures to be adopted in furthering the implementation of these Regulations
  - b) the adoption of any international standards, principles or practices relating to AML/CFT.

This regulation will come into effect with signature of the Minister of Finance of the Federal Republic of Somalia:

Yours Sincerely,

  
Dr. Abdirahman D. Beileh

