

የኢትዮጵያ የካተታ
ገቢያ ባለሥልጣን

ETHIOPIAN CAPITAL
MARKET AUTHORITY

**GUIDANCE FOR ECMA LICENSEES ON CUSTOMER DUE DILIGENCE AND
REPORTING UNDER AML/CFT**

November 2025

Contents

ACRONYMS	i
Definition of Terms.....	ii
1. Purpose and scope of this document.....	1
2. Guidelines for Capital Market Participants regarding ML/TF issues with their clients.....	3
2.1. AML/CFT requirements for onboarding and monitoring Investor accounts with Capital Market Service Providers	3
2.1.1. Due Diligence applicable by customer type	6
2.1.2. Customer's Identity and Beneficial Owner(s) identity	27
2.1.3. Important Red Flags and Suspicion Indicators to watch out for when establishing and monitoring a Business Relationship with an Investor	27
2.2. AML/CFT onboarding and monitoring requirements for Capital Market Participants whose clients are other Capital Market Professionals	31
2.2.1. Minimal checks to be performed on Licensed Market Participants.....	33
2.2.2. Potential specific vulnerabilities, Red Flags, and answers regarding some Licensed Market Participants	33
2.2.3. Relevant additional direct or indirect AML/CFT checks and measures for the most important CMSP and Market Intermediaries regarding their internal organization.....	34
2.3. Measures to freeze or seize assets (based on International Sanctions)	39
2.4. Specific Provisions for Securities Issuers.....	40
2.4.1. Designation of an Intermediaries	40
2.4.2. Additional checks about the origin of funds at the book-building stage.....	41
3. Reporting obligations to the Authority	41
3.1. Presentation of the Business and Activity	43
3.1.1. Type of Company, Legal Form, and Shareholding Structure.....	43
3.1.2. Products and Services, Customers and Distribution Channels.....	43
3.1.3. Professional Related Parties.....	43
3.2. AML/CFT Compliance Organization	43
3.2.1. Human Resources	44
3.2.2. Information System	44
3.2.3. Description of the internal AML/CFT Organization for each line of Business	44
3.2.4. Description of the Customers' ML/TF Risk Assessment Process	45
3.2.5. Description of the Internal Controls Organization	46

3.3 ML/TF Risk Assessment, Remedial Measures and Resulting Risks	47
3.3.1. Business Line ML/TF Risk Mapping	47
3.3.2. Business Processes ML/TF Risk Mapping.....	47
3.4 Quantitative and Qualitative Reporting.....	47
3.4.1. Information on the Annual Report production process.....	48
3.4.2. Human Resources	48
3.4.3. Criteria and Thresholds.....	49
3.4.4. Permanent controls (Level 1)	49
3.4.5. Periodic controls (Level 2).....	49
3.4.6. Database screening and transaction monitoring tools.....	49
3.4.7. Clients.....	50
3.4.8. Business Lines Risk Assessment	50
3.4.9. Suspicious Transactions Reports (STR)	50
3.4.10. Outsourced task in relation to ML/TF issues.....	51
3.4.11. Reporting conclusion	51
Appendix 1 – Content of the Annual Control Report.....	52
Minimum content.....	52
Type of Company, Legal Form, and Shareholding Structure	52
Products and Services, Turnover and Distribution Channels	52
Clients	53
Suspicious Transactions Reports (STR)	53
Full potential content.....	53
Appendix 2 – Content of a Suspicious Transaction Report (STR)	54

ACRONYMS

AML	Anti-Money Laundering
BI	Business Introducer
CDD	Customer Due Diligence
CIS	Collective Investment Scheme
CFT	Combating Financing Terrorism
CMSP	Capital Market Service Providers
CRS	Common Reporting Standard
CSD	Central Securities Depository
DARS	Document Authentication and Registration Service
(E)CMA	Ethiopian Capital Market Authority
ESX	Ethiopian Securities Exchange
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Taks Force
FIS	Financial Intelligence Service (former Financial Intelligence Centre)
IOSCO	International Organization of Securities Commissions
IPO	Initial Public Offering
KYC	Know Your Customer
ML	Money Laundering
MoTRI	Ministry of Trade and Regional Integration
NBE	National Bank of Ethiopia
OTC	Over the Counter
PEP	Politically Exposed Persons
SOE	State Owned Enterprises
SRO	Self-Regulatory Organization
TF	Terrorist Financing
UBO	Ultimate Beneficial Owners

Definition of Terms

Annual control report	Report that covers detailing AML/CFT systems and the results achieved, risk control in particular appropriate measures have been taken in the event of default
Authority	Means the Ethiopian Capital Market Authority established under the Capital Market Proclamation No. 1248/2021
Beneficial owner	Means any natural person who ultimately owns or controls a customer or an account, the person on whose behalf a transaction is being conducted, or the person who ultimately exercises effective control over a legal person or arrangement
Business Introducer	Means a physical or legal person who enter an agreement with a CMSP in order to introduce potential customers and receive commissions in return
Enhanced due diligence	Means additional consideration of situations that present a higher risk of Money Laundering or Terrorist Financing including steps additional to those in customer due diligence measures which should be taken depending on the situation that is present.
High Risk	Means customers, businesses or transactions that need to be subjected to more regular reviews, particularly against the know-your-customer information held by Financial Institutions the activity in the account. Such categories shall include, but not be limited to: The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer), non-resident customers such as those staying in the country for less than one year or those in short visit or travel, legal persons or arrangements such as mutual funds that are personal asset holding vehicles, Companies that have nominee shareholders or shares in bearer form, Business that are

cash-intensive, complex, unusual or large transactions including the ownership structure of the company appears unusual or excessively complex given the nature of the company's business and Politically Exposed Persons (PEPs) and persons or companies related or close associated to them, Country or Countries identified by credible sources, such as FATF mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems, Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations, Countries identified by credible sources as having significant levels of drug production, trafficking or smuggling, corruption or other criminal activity, Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have terrorist organizations operating within their country, Private banking, Anonymous transactions (which may include cash), cross-border business relationships, wire transfers or non-face-to-face business relationships or transactions and Payment received from unknown or un-associated third parties.

Identity

means features which can uniquely identify a natural or legal person and includes a set of attributes such as name(s) used, date of birth and the residential address at which the customer can be located.

KYC

Is a mandatory process of identifying and verifying the client's identity.

Low Risk

For this guideline, low risk customer shall mean CMSP's and other Capital Market Participants regulated by ECMA, Banks, insurances and financial institutions regulated by NBE, listed companies on ESX, state owned enterprises (SOE's) and CIS authorized by ECMA.

Medium Risk

Medium risk customer means any businesses and persons outside the low risk and high-risk customer category

Politically Exposed Persons

means any natural person who is or has been entrusted with prominent public functions in any country or in an international organization as well as a member of such a person's family or any person closely associated with him. For the purpose of this guideline PEP lists including individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of State owned corporations and political party officials and persons or companies related or close associated to them, individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of Government, senior politicians, senior government, judicial or military officials, senior executives of State owned corporations and political party officials and persons or companies related or close associated to them; and persons who are or have been entrusted with a prominent function by an international organization and includes members of senior management such as directors, deputy directors and members of the board or equivalent functions other than middle ranking or more junior individuals.

Periodic Control

Means an internal audit on the overall effectiveness of governance, risk management and Internal control.

Permanent Control

Means a system that the licensee defines and implements to ensure compliance with laws and regulations, and to control its operations and resources efficiency.

Professional

is an individual or institution, such as a broker, dealer, investment advisor, or any person employed by an organization engaged in the buying and selling of

financial instruments like stocks, bonds, options, futures contracts, or other trading vehicles.

Simplified due diligence means measures taken where the risks of money laundering or terrorist financing is lower considering the nature of the risk.

Standard due diligence Is a form of Customer Due Diligence that applies on most customers that fall outside the lower risk or higher risk categories.

Suspicious transaction means one which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering, predicate offense or terrorist financing methods.

Source of Fund Means a particular fund or other asset which is the subject in the business relationship

Source of Wealth Means the origin of the entire body of wealth or total asset

1. Purpose and scope of this document

The primary goal of Money Launderers is to make their transactions indistinguishable from legitimate transactions. The specificity of the securities Industry is that it can be used both to launder illicit funds obtained elsewhere and to generate illicit profits within the industry itself through additional fraudulent activities such as market manipulation, insider trading, etc. However, the number of Suspicious Transactions Reports originating in this sector is usually relatively low¹ compared to others in the banking and financial industry.

Typical securities-related laundering schemes often involve a series of transactions that do not match the investor's profile and do not appear designed to provide an effective return on investment. This, cumulated with the fact that Money Laundering in the Securities Industry usually occurs at the layering and integration stages, makes the Risk-based Assessment and the KYC Due Diligence even more important when establishing a Business Relationship and later during the monitoring phase.

Therefore, the purpose of this document is to draw Guidelines for licensed CMSP's and Market Intermediaries regarding their obligations in terms of AML/CFT checks and reporting towards the ECMA when establishing a Business Relationship and during this relation. In addition, it focuses on the AML/CFT Due Diligence obligations for Securities Issuers, which includes risk-based assessment principles.

This is done in accordance with the provisions of Proclamation 1248/2021 that establishes ECMA as the Regulator of the ESX, as well as the other Capital Markets Participants², the FATF's "Guidance for a risk-based approach in the Securities Sector" and IOSCO's 8th Principle "Enforcement of Securities Regulation" which:

- Characterizes Money Laundering as activities and processes intended to obscure the source of illegally obtained money and to create the appearance that it has originated from a legitimate source and
- States that Capital Markets Regulators should consider the sufficiency of domestic legislation to address the risks of Money Laundering (ML) and

¹ It must also be noted that the reported number Money Laundering suspicions in the securities Industry far outweighs those related to Terrorist Financing

² The overall objectives of the Capital Market Authority, as per Article 3-5 of Proclamation 1248/2021, and the IOSCO 30 Principles are: i) to protect investors, ii) to ensure the existence of a Capital Market Environment in which securities can be issued and traded in an orderly, fair, efficient and transparent manner, iii) to reduce the systemic risk by ensuring the integrity of the Capital Market and transactions and iv) to create promote and facilitate a robust Capital Market environment fit for long term investments.

- Entail the Regulator to require that Market Intermediaries and CMSPs have in place efficient policies and procedures designed to minimize the risk of them being used as a vehicle for Money Laundering. In addition, it recommends not considering that AML/CFT checks and controls required for Market Intermediaries and CMSP are redundant with those carried out within the financial institutions through which the funds intended for investment on the Capital Market transit upstream.

The following Guideline is built on the principles of a Reasonably Designed Risk-Based Approach, which requires:

- To efficiently identify the proper criteria to measure potential ML/TF risks associated with an activity, a type of Customer, a product or service, a transaction, etc.
- To document and periodically review and update this risk assessment approach
- To focus on the Customers and transactions identified to potentially pose the most significant risks of ML/TF and efficiently monitor them.

This Guideline³ allow Market Intermediaries and CMSP to adopt AML/CFT policies and procedures that are proportionate risks associated with the nature, scale, and complexity of their activities. They also help the Authority to set clear expectations of the criteria that firms should consider when identifying and assessing ML/TF risks and deciding the appropriate level of Due Diligence, which includes:

- Customer acceptance and KYC norms
- Standard list of documents which can be accepted as evidence of the information provided by the Customer
- Identification of the source of funds

Nothing in this Guideline is intended to limit or otherwise restrict any additional or supplementary guidance, circulars, notifications, memoranda, communications, or other forms of guidance or feedback—whether direct or indirect—that may be issued from time to time by ECMA or in relation to any specific CMSP.

³ In addition to the existing Ethiopian legislation, these Guidelines are based on current practices in abroad, notably Guidelines from the FCA UK, the ESMA, the Basel Supervision Committee and the Wolfsberg Group. In addition, this guideline should not be construed as legal advice or legal interpretation. Supervised institutions should perform their own assessments of the way they should meet their statutory obligations, and they should seek legal or other professional advice if they are unsure of the application of the legal or regulatory frameworks to their circumstances.

2. Guidelines for Capital Market Participants regarding ML/TF issues with their clients

As defined in Article 2/6 of the Ethiopian Capital Market Authority Proclamation 1248/2021, Capital Market Participants include the following:

- Capital Market Infrastructures⁴.
- Capital Market Service Providers⁵.
- Issuers of Securities.
- Investors.
- Eligible Counterparties to eligible contracts⁶.

At the stage of entering a business relationship, the information required from the Customer and the checks to be performed differ depending on whether the Customer is the Investor – whether a Natural or Legal Person – or itself a Capital Market Professional. The same distinction is to be made for ongoing monitoring and annual renewal of required checks and supporting documents.

When entering a Business Relationship with a Capital Market Service Provider, Investors are subject to a complete initial analysis in terms of ML/FT risks. In contrast, the Capital Market Professionals above-mentioned already had their risk profile and processes scrutinized when their License was initially granted or later renewed by the Authority.

All ECMA licensees shall retain customer data for ten (10) years, and such data shall be subject to inspection by ECMA.

2.1. AML/CFT requirements for onboarding and monitoring Investor accounts with Capital Market Service Providers

Investors – whether being Natural or Legal Persons - are those which hold the funds that are going to be invested in Securities, either:

- Via a trading account or portfolio managed directly by the Customer himself or with the help of an Investment Adviser

⁴ Such as Securities Exchanges, Securities Central Depository and Securities Clearing Houses.

⁵ Such as Securities Brokers, Securities Digital Sub-Brokers, Securities Dealers, Securities Broker-Dealers, Securities Market Markers, Securities Appraisal Firms, Credit Rating Agencies, Collective Investment Schemes, Collective Investment Scheme Operators, Securities Portfolio Managers, Securities Investment Managers (whether Individual or Corporate and Sharia compliant or not), Securities Robo-Advisers, Crowdfunding Intermediaries, and Investment Banks (whether part of a Banking Group or not).

⁶ Which relates to Derivative Products.

- Via a licensed Portfolio Manager
- Or through Collective Investment Schemes or comparable Investment Vehicles.

By and large, the categories of Capital Market Service Providers facing these Investors may include:

- Collective Investment Scheme operators
- Securities Portfolio Managers
- Securities Investment Advisers (whether being Individuals or Corporations)
- Robo-Advisers
- Crowdfunding Intermediaries
- Securities Brokers and Digital Sub-Brokers
- Investment Banks

Investors are required to go through AML/CFT procedures when entering a Business Relationship with a Capital Market Services Provider. For example, this will be the case when an Investor opens an account with a Securities Broker to trade securities, subscribe shares of a Collective Investment Scheme or initiates a Business Relationship with a Financial Investment Adviser or a Portfolio Manager.

For each Customer category of ML/TF risk level, the requirements and checks listed below represent the maximum compliance checks that can be performed by CMSP.

The ban on funding a trading account with cash deposits is a highly effective measure in the AML arsenal and it shall be applied by brokers and other CMSP's in Ethiopia.

For a small Individual Investor opening a trading account with a Broker with a deposit of funds below a certain threshold, a Level 1/lighter KYC or simplified due diligence may be sufficient. This would include the following information:

- Name and Surname and Identity Verification via the FAYDA digital ID or passport for foreign investors with an embedded picture.
- address
- Date of birth
- Occupation
- Nationality and Country of Residence
- A deposit threshold shall be set at ETB 50,000 (Fifty Thousand). Where a customer holds accounts with multiple brokers, the threshold shall be

applied on a consolidated basis, as the Central Securities Depository consolidates all accounts held by the same customer.

Additional information such as income level and risk tolerance are elements of the KYC used to determine if proposed products are adapted to the customer but could also be further used to determine if his/her trading behaviour requires enhanced monitoring in terms of ML risks.

As part of the KYC onboarding process, a Politically Exposed Person (PEP) declaration is required. The declaration must also cover immediate family members of a PEP, including spouse, parents, children, siblings, in laws and uncles/aunts and close associates.

At the initial stage of KYC, a declaration of source of funds and source of wealth is required and may be subject to further verification if deemed necessary.

At this stage, unless the CMSP has doubts about the authenticity of the information provided in addition to the FAYDA digital ID, the principle of self-declaration can be considered sufficient. In case of doubt, it can ask for additional evidence from the relevant government institution.

An upgrade to a Level 2 KYC or Standard due diligence – with a full check of Customers' Identity - would be required:

- After 1 year of activity
- In case of outgoing transfer of the held securities and liquidities to another Broker
- In case of incoming transfer of additional funds or securities causing the initial threshold to be exceeded
- In case of suspicious activities detected by the Securities Broker or the Authority, that could raise questions regarding ML/TF issues.

Where physical appearance for KYC checks is not feasible, a Capital Market Service Provider (CMSP) may identify and verify the customer through electronic KYC (e-KYC). The CMSP shall ensure it is equipped with the necessary infrastructure to conduct e-KYC and shall have access to the FAYDA digital ID database or the related digital ID database.

During the conduct of electronic Know Your Customer (e-KYC) procedures, Capital Market Service Providers (CMSPs) shall ensure that all required documentation is duly collected, recorded, and preserved in accordance with the applicable regulatory standards. Such documentation shall be made readily accessible for review and verification by the Authority for the purpose of monitoring, supervision, and compliance assessment.

2.1.1. Due Diligence applicable by customer type

PHYSICAL PERSONS – Individuals

TYPE OF DUE DILIGENCE	IDENTIFICATION AND VERIFICATION OF THE IDENTITY		UNDERSTANDING THE NATURE AND THE PURPOSE OF THE BUSINESS RELATIONSHIP	
	Obligation to Identify	Obligation to verify the Identity	Information required to understand the purpose of the Business Relationship	Additional Due Diligence / Information / Documentation specific to the Product / Service, Customer Type, Distribution Channel or Transaction
Standard Due Diligence	YES	YES	Residential Address Activity, net annual revenue, and wealth Type of Products and/or Services offered to Customer. Tax Identification Number Exposure to International Sanctions	PEP checks if applicable
Simplified Due Diligence	YES	FAYDA digital ID sufficient	Tax Identification Number if applicable	N/A

PHYSICAL PERSONS - Professionals

TYPE OF DUE DILIGENCE	IDENTIFICATION AND VERIFICATION OF THE IDENTITY		UNDERSTANDING THE NATURE AND THE PURPOSE OF THE BUSINESS RELATIONSHIP	
	Obligation to Identify	Obligation to verify the Identity	Information required to understand the purpose of the Business Relationship	Additional Due Diligence / Information / Documentation specific to the Product / Service, Customer Type, Distribution Channel or Transaction
Standard Due Diligence	YES	YES	<ul style="list-style-type: none"> • Residential Address • Activity and annual turnover • Type of Products and/or Services offered to Customer. • Tax Identification Number • Exposure to International Sanctions 	PEP checks if applicable.
Simplified Due Diligence	YES	FAYDA digital ID sufficient	Tax Identification Number if applicable	N/A

DATA AND SUPPORTING DOCUMENTS (Individual and Professional Natural Persons)

DATA AT ONBOARDING	SUPPORTING DOCUMENTS AT ONBOARDING	EXPIRY DATE OF THE DOCUMENT PROVIDED BY THE CUSTOMER AT THE ONBOARDING	DATA OR SUPPORTING DOCUMENTS TO BE COLLECTED DURING A REVIEW
Identity Information:	Identity documents meeting the following requirements:	Document needs to be valid in accordance with the laws where such document was issued	No renewal, unless there is an indication of a change in circumstances:
Title, Full Name, Date of Birth, Place of Birth (country and/or city), Identification Number, Nationality(ies)	Photography, Full Name, Date of Birth, Place of Birth, Type of Document and date and place of issuance, Name and capacity of the Authority or person who issued the document and, if deemed appropriate, has authenticated it. (Such as passport for foreign nationals)		Optionally: the consultation of public sources mentioning a change
	FAYDA digital ID		Compulsory: information brought to the attention of the Customer Relationship Officer (e.g. return of mail, account status, Customer exchange, etc.)
			Where applicable, the change in situation must be documented or confirmed by the Customer (when only a self-declaration is required at the beginning of the relationship)
Residential Address:	"Kebele Digital ID" for local nationals	Expiry date of the "kebele Digital ID"	No renewal unless there is an indication of change in circumstance

Country, City, Number and Name of the street	Any document bearing the required information (Driving license and utility bill for foreign nationals)	Expiry date of the document	Optionally: the consultation of public sources mentioning a change
	If using a residence certificate, the 3 following documents:		Compulsory: information brought to the attention of the Customer Relationship Officer (e.g. return of mail, account status, Customer exchange, etc.)
	Letter signed by the Landlord certifying that the person has been living at the address indicated for more than 3 months.		Where applicable, the change in situation must be documented or confirmed by the Customer (when only a self-declaration is required at the beginning of the relationship)
	Copy of a valid Identity document of the landlord		
	Recent proof of address in the name of the landlord (residential address certification or location plan issued by the competent authority or any other document usually used to determine the home address)		
Financial situation – For Individuals considered low or medium risk: Activity	Activity: self-declaration or information available	1 year	It is not necessary to contact the Customer when elements relating to the Customer's financial situation may be collected from an existing trading account or a bank account to which the CMSP has access. Otherwise, renewal of self-declaration or supporting documents where applicable.
Net Annual Revenues	Wealth: Not required, except in case of doubt about the origin of the funds. In this case, it is necessary to collect the information and keep track of it in the Customer's KYC file.		For retired Customers, once identified as such and does not self-declare nor earn revenues above 20% of the total revenues of the Customer, the information will no longer be required.
Wealth	In all the above cases, self-declaration is not sufficient if there is any doubt about the veracity of the information provided by the client. In this case, it is necessary to collect supporting documents.		
	For non-emancipated underage Customers, no information is required		
Individuals rated High Risk	Activity: self-declaration or information available		

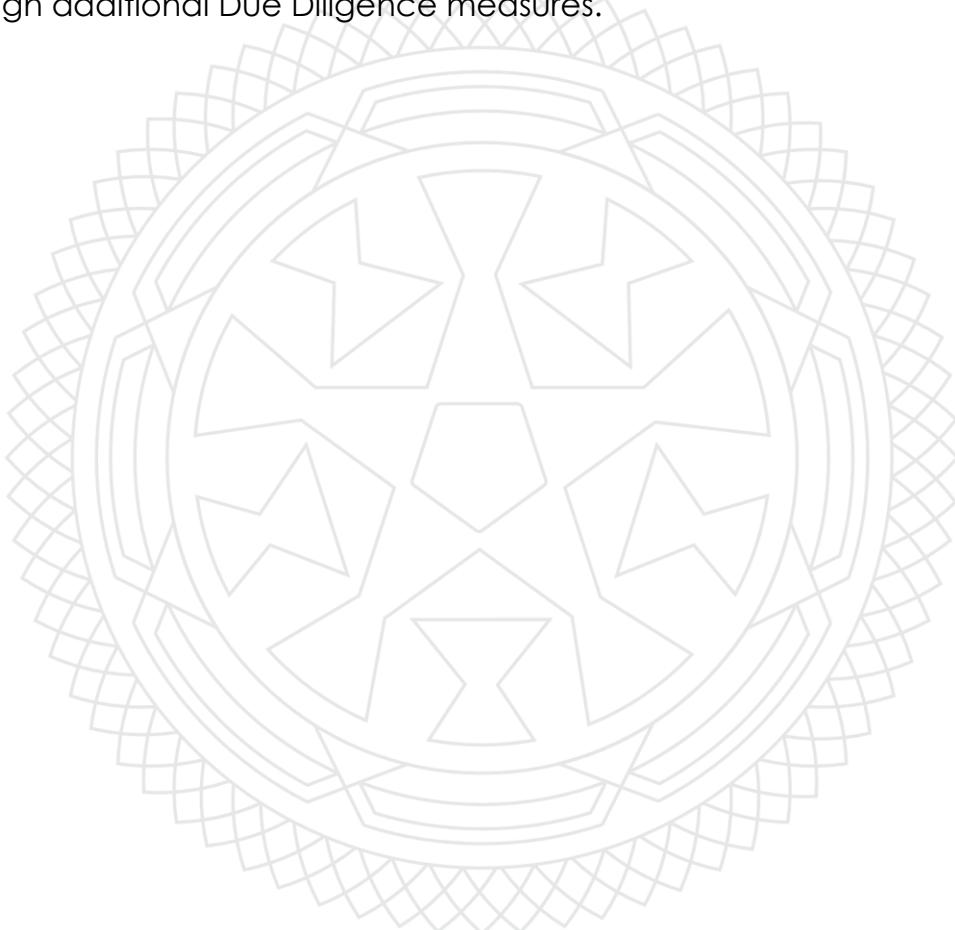
Individuals rated High Risk Source of Wealth	Revenues: Relevant Documentary evidence	1 year	It is not necessary to contact the Customer when elements relating to the Customer's financial situation may be collected from an existing account (for example, when the financial assets are held on a known account). Otherwise, renewal of self-declaration / supporting documents where applicable.
	Wealth: self-declaration		For non-emancipated underage Customers, no information is required if the following two conditions are met:
	In all the above cases, self-declaration is not sufficient if there is any doubt about the veracity of the information provided by the client. In such a case, it is necessary to collect the supporting documents.		i) The Legal Representative of the Customer is also an Individual Customer of the CMSP, with a compliant KYC file and
	For non-emancipated underage Customers, no information is required if the Legal Representative of the Customer is also an Individual Customer of the CMSP with a compliant KYC file.		ii) The overall Account Analysis of the accounts of the underage Customer does not raise any inconsistency.
	Activity: signed self-declaration		Remark: The Overall Account Analysis is the analysis of the coherence between the Customer's account activity, its situation, and the purpose of the Business Relationship. It is carried out at the KYC review, regardless of the Customer's risk rating.
Source of Wealth	Revenues: supporting documents		It is required to compare the elements regarding the financial situation of the Customer obtained from the account with the information initially collected. This diligence may be performed through the Overall Account Analysis required for Customers who are flagged as PEP.
	Wealth: signed self-declaration		If the comparison is consistent, it is not necessary to contact the Customer.
	Source of Wealth: signed self-declaration.		If the comparison is not consistent, it is necessary to contact the Customer to obtain explanations and / or supporting documents. A detailed signed report

			from the Chief Compliance Officer must be formalized.
	Source of Wealth: signed self-declaration.		If the client does not provide explanations and/or supporting documents, the Chief Compliance Officer performs a formalized analysis considering the elements gathered. Whether its opinion is positive or negative, the case is escalated to the Management for validation.
	In the cases above, a self-declaration is not sufficient if there is any doubt about the veracity of the information provided by the client, especially in case of doubt about the process of wealth. In such a case, it is necessary to collect supporting documents.		
	If the Customer does not sign the self-declaration or does not provide consistent supporting documents, the Compliance Department (first Line of Defense) must perform a formalized analysis considering the elements gathered. In case of a positive opinion, the case is escalated to the Chief Compliance Officer for additional checks.		
	Final approval from the management is required.		
Professionals rated low to medium risk.	Self-Declaration	1 year	It is not necessary to contact the Customer when elements relating to the Customer's financial situation may be collected from the existing account. Otherwise, renewal of Self-Declaration / supporting documents when applicable.
Nature of the primary business / economic sector			
Annual turnover			
Professionals rated High-Risk	Documentary evidence	1 year	It is not necessary to contact the Customer when elements relating to the Customer's financial situation may be collected from the existing account. Otherwise, renewal of Self-Declaration / supporting documents when applicable.

Nature of the primary business / economic sector	Additional provisions if the professional is a PEP		
Annual turnover Wealth/Fund Management Customers: Estimated Net Annual Revenues Wealth Source of Wealth Remark: these rules constitute the minimum framework in terms of knowledge of the financial situation of clients and Beneficial Owners to be implemented at the beginning of a Business Relationship	<p>For low to medium risk Customers:</p> <p>Activity: Self-Declaration</p> <p>Income: Self-Declaration (ask for supporting documents in case of doubt)</p> <p>Wealth: Self-Declaration (ask for supporting documents in case of doubt)</p> <p>Origin of Wealth: Self-Declaration and/or supporting documents</p> <p>For High-Risk Customers:</p> <p>Activity: Self-Declaration</p> <p>Income: Supporting documents</p> <p>Wealth: Supporting documents</p> <p>Origin of Wealth: Self-Declaration and / or supporting documents</p>	1 year	<p>It is not necessary to contact the Customer when elements relating to the Customer's financial situation may be collected for the existing account, and the CMSP is not aware of any change in the financial situation. Otherwise, renewal of Self-Declaration / supporting documents where applicable.</p> <p>Regarding existing clients who, during the Business Relationship, become eligible for the "Wealth Management Segment", the completion of a KYC file is a prerequisite, and the CMSP shall collect the same documents as those required when entering into a relationship and / or verify the documents already collected from the client.</p> <p>An Overall Account Analysis, understood as the analysis of the coherence between the account activity, the Customer's situation and the purpose of the business relationship, is carried out at the KYC review, regardless of the Customer's risk rating.</p> <p>A KYC review must be triggered when a client acquires a High-Risk rating as a result of a change of the risk rating of the Business Relationship.</p>

Specificities and Additional Due Diligence Measures for Wealth/Fund Management Customers

Wealth Management and Private Banking clients are considered riskier than ordinary clients regarding ML/TF risks. They potentially expose the CMSP to threats related to Money Laundering, corruption, trafficking, financial Sanctions violation, especially when also being PEPs, when using Legal Person as a dedicated Investment Vehicle to detain their assets and / or being non-resident from countries at risk⁷. Particular attention is therefore required to the analysis of the legality of the origins of the client's assets through additional Due Diligence measures.



⁷ This could particularly concern members of the Ethiopian diaspora wishing to invest in securities listed on the Ethiopian Securities Exchange.

Rules on knowledge of the Business Relationship	THEMES	ADDITIONAL DUE DILIGENCE
	Identification of the Ultimate Beneficial Owner(s) (UBO)	<p>Whatever the risk rating of the Customer: collect an official identity document Such as FAYDA digital ID for the Ultimate Beneficial Owner(s) as well as a corroborative document (e.g. articles of association, minutes of a general assembly, organization chart certified by an independent expert, etc.).</p> <p>It should be noted that this rule is in addition to the consultation of the Register of the Beneficial Owner(s) when applicable.</p> <p>If it is not possible to obtain an official identity document, then the Business Relationship shall not be established.</p>
	Domicile of the Ultimate Beneficial Owner(s)	<p>Collect proof of domicile for:</p> <p>The non-resident BO of Legal Entity clients whatever the risk rating of the client</p> <p>The BO(s) of Legal Entity clients rated high risk.</p> <p>For other levels of risk, information on the domicile of the BO(s) is required.</p>
	Identification of the Legal Representatives	Collect an official identity (FAYDA digital ID) document for Legal Representatives.
	Domicile of Client Representatives	Collect information on Representative's residence by any available mean
	Information of a tax nature	<p>For any risk level, a self-declaration of tax compliance signed by the prospect / client or BO is required.</p> <p>For non-resident high risk Customers collect an additional document proving tax compliance:</p> <ul style="list-style-type: none"> i) Either a certificate from a specialist adviser, according to which the client complies with his tax obligations in his country of tax residence, about his income and assets either ii) A tax return or a tax notice or any other documentary evidence consistent about his income and assets. <p>When the clients are not covered by an automatic exchange of information procedure, new supplementary proof of tax compliance shall be obtained from them.</p> <ul style="list-style-type: none"> i) after 3 years or ii) in the event of a change in circumstances.

	Check for Public Information on financial and/or professional situation	For all levels of risk, the CMSP must research reliable Public Information on the financial situation and/or professional situation of clients or Beneficial Owners: <ul style="list-style-type: none"> - In the absence of such Public Information, escalation within the Compliance line of responsibilities is required if not confident in the information declared by the client. - In the presence of this information, if it seems inconsistent with the client's statements, proof must be requested from the client. In case of doubt, the case should be escalated along the Compliance line of responsibilities.
	Check for negative information	Whatever the assessed level of risk of the client, a search for negative information is required with regard to the following people: <ul style="list-style-type: none"> - For Natural Person clients: the account holder, joint account holders, agents, guarantors, curators, tutors, any holder of rights allowing transactions to be carried out on the account(s). - For Legal Entity Customers: the Legal Entity, the Ultimate Beneficial Owners, the Legal Representatives, the Natural or Legal person shareholders holding more than 5% of the entity, on a consolidated basis, the agents, the guarantors, and any holder of rights enabling transactions to be carried out on the account(s). The names of the people referred to above will be periodically filtered using dedicated tools to detect negative information during the course of the relationship.
	Nature and purpose of the Business Relationship	Collect information on the expected operations of the account before the relationship is entered (e.g. number of flows, nature and purpose of the projected investments, etc.)
	Documentation of the origin of wealth	For natural person clients rated Medium / High Risk, as well as for the Beneficial Owners of Legal Entity clients rated Medium / High Risk (except of the Beneficial Owner in last resort): Collect supporting documents on the origin of wealth.
Miscellaneous	PEP non-face-to-face onboarding	In order to board a non-face-to-face Business Relationship with a PEP or High-Risk client, it shall be compulsory that the first inflow of money for the transactions be made from an account opened in the client's name with a reputable bank. In our opinion, it would make sense – in terms of AML/CFT – that it is also compulsory that the money is sent from an account opened in the client's name with a domestic Ethiopian Bank. In addition, it is necessary to apply at least two of the following measures: <ol style="list-style-type: none"> i) Obtain a copy of an official identity document. ii) Implement verification and certification measures for the copy of an official document or an official register extract by a third party independent of the person to be identified.
	Bearer shares	In the case of a Custodian, at each (annual) review, obtain confirmation that has been no change in the detention and conservation.

	PEP declassification	One year after leaving the PEP functions, a new status of "inactive PEP" can be attached to the Customer for 10 years. The "contagion" rules for family members and close business associates of the "inactive PEP" can be lifted if the remaining risk is considered low.
	On the official identity document	Identity documents used for verification of identity must be signed.

CORPORATES - Private Companies and Listed Companies

CRITERIA	IDENTIFICATION AND VERIFICATION OF THE IDENTITY		IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER'S IDENTITY		UNDERSTANDING THE NATURE AND THE PURPOSE OF THE BUSINESS RELATIONSHIP	
	Issuers of Securities on the Securities Exchange	Obligation to Identify	Obligation to verify the Identity	Obligation to Identify the UBO	Obligation to verify UBO Identity	Information required to understand the purpose and the nature of the Business Relationship
YES	YES	NO	NO	NO	Ownership and Management structure Corporate purpose (type of activity, line or nature of business or industry) Activity and annual turnover List of Controlling Parties Type of products and / or services offered to Customers Exposure to International Sanctions Tax Identification number	For PEP see the corresponding KYC indications below For Business Introducers see specific KYC requirements below
NO	YES	YES	YES	YES	Ownership and Management structure Corporate purpose (type of activity, line or nature of business or industry) Activity and annual turnover List of Controlling Parties Type of products and / or services offered to Customers Exposure to International Sanctions Tax Identification number	

Additional measures and Specific KYC requirements for PEPs

It is highly advisable for a CMSP to include an obligation for PEPs to identify themselves as such in their contractual relationship documents when entering a business relationship with a CMSP. Otherwise, the existence of a PEP status can be suspected based on the Customer's answers to questions when the Business Relationship is established and lead to additional questions that may confirm or discard this information. Checks can also be made using commercial databases, provided that once a person has been flagged as a PEP in one of those databases, an analysis must be conducted to confirm or waive this information.

Due to their position, PEPs present a risk linked to corruption and bribery and must, therefore, be systematically flagged. A specific database of Customers and BOs flagged as PEPs must be maintained.

Enhanced Due Diligence measures shall be implemented when the Business Relationship or its Beneficial Owner is a PEP or becomes a PEP during the Business Relationship. These measures not only apply to PEPs, but also to their (direct) family members and persons known to be closely associated with the PEP.

Persons closely associated with a PEP are either of the three types of individuals covered by the following three situations:

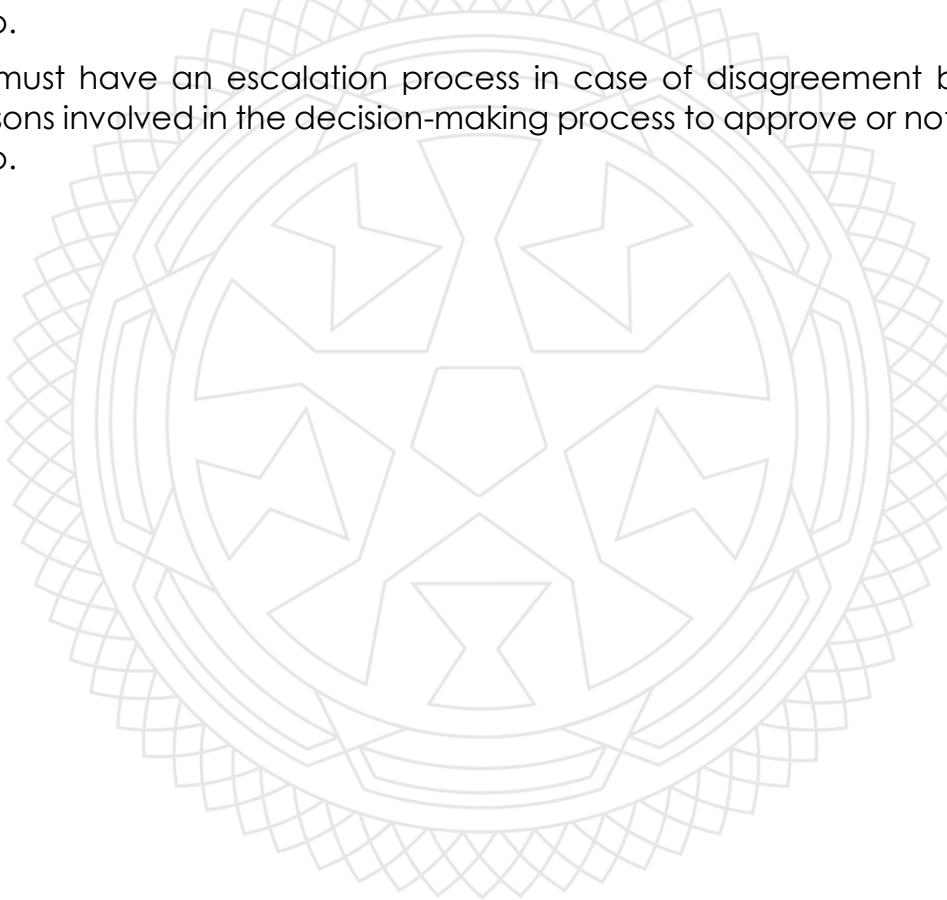
- A Legal Person is a Customer with a PEP among its Beneficial Owners:
 - This Legal Person and the Beneficial Owners must be flagged as "PEP" in the database.
 - If there is any other Beneficial Owner who is not a customer itself, its source of wealth must be searched on a Risk-Based Approach, unless there is no suspicion of Money Laundering.
- When an individual is the only UBO of a Legal Person established for the sole benefit of such PEP:
 - Considering that Legal Entities may be used by a PEP to conceal assets obtained illegally, special attention must be paid to entities that lack significant assets, business activities and employees (and to trusts, however they are not applicable in Ethiopia).
 - When such a Legal Entity is a Customer of a CMSP, Enhanced Due Diligence must be applied with respect to both the Legal Entity and the PEP (see below)
- When a person is known to have a "close business connection" with a PEP. This person can be a person providing ongoing representation for the PEP and who

is compensated for that service, a customer, a provider, a lender, a guarantor, etc.

In these three situations the person "closely associated with the PEP"⁸ must also be recorded in the Customer Databases as PEP.

The responsibility to onboard a Business Relationship with a Natural Person Customer categorized as PEP or with a Legal Entity categorized as PEP Presence, or to maintain a Business Relationship with such Customers, rest with the Senior Management of the CMSP, considering that: The Senior Manager must have sufficient knowledge of ML/TF and Bribery/Corruption risks to which the CMSP is exposed due to this Business Relationship.

The CMSP must have an escalation process in case of disagreement between the various persons involved in the decision-making process to approve or not the Business Relationship.



⁸ Immediate family members of a PEP, including spouse, parents, children, siblings, in laws and uncles/aunts and close associates.

In addition to Customer standard Due Diligence, the applicable Enhanced Due Diligence regarding Natural Person Customers who are PEP is as below:

Approval by CMSP Senior Management	<p>Approval by CMSP Senior Management The decision to board a Business Relationship with a PEP must be taken by an appropriate (i.e. ML/TF risk-aware) Senior Manager within the CMSP</p>
Revenues, Wealth and Source of Wealth	<p>Regarding Individual Customer PEP, it is necessary to search for information on:</p> <ul style="list-style-type: none"> – The Customer's revenues, which implies collecting information on the origin of the revenues involved in the Business Relationship and – The Customer's wealth, split by asset categories (real estate, securities, pension plan, art, etc.) in a sufficiently precise manner and – The source of wealth (for instance, inheritance, selling of a business, professional revenues, etc.) <p>If it is not possible to collect this information from the Customer, the CMSP may use information or documents from other sources (including commercial databases) to confirm all or part of the information that may have been collected.</p>
Exemption to Enhanced Due Diligence	<p>Enhanced Due Diligence is not mandatory when two of the following cumulative conditions are met:</p> <ul style="list-style-type: none"> – There is no ML/TF suspicion and – The Business Relationship with the Customer is established for the purpose of acquisition or subscription of one or more products eligible to regulatory-based Simplified Due Diligence due to the nature of the product or transaction (e.g., Monetary Market Funds). – SOE'S

The implementation of Enhanced Due Diligence measures described above may be adjusted according to an assessment of the risk profile of the Customer, considering that certain PEPs may have a greater or lower risk profile. Such an assessment is based on any other information relating to the PEP that is available, the products or services that are purchased or subscribed and the transactions that are envisaged or that have been conducted.

In addition to Customer standard Due Diligence, the applicable Enhanced Due Diligence regarding Legal Person Customers who are classified as PEP Status or PEP Presence, is as below:

Approval by the CMSP Senior Management	The decision to board a Business Relationship with a PEP must be taken by an appropriate (i.e. ML/TF risk-aware) Senior Manager within the CMSP
Revenue, Wealth and Source of Wealth of Beneficial Owner of Legal Person Customers with PEP Status	When the Customer who is a Legal Person has a PEP Status, it is necessary to search for information (or supporting document when required) on the Revenues, Wealth, and Source of Wealth of its Beneficial Owner (information from public sources and / or self-declaration). In the absence of such information or in case of doubt as to the veracity of the information obtained, the KYC file must be escalated along the Compliance line within the CMSP.
Exceptions to Enhanced Due Diligence	Enhanced Due Diligence is not mandatory when the following two cumulative conditions are met: There is no suspicion of ML/TF The Business Relationship is established either with a company that issues securities listed on the ESX or with a customer who procures or subscribes to products eligible to regulatory-based simplified Due Diligence due to the nature of the product or transaction (e.g., Monetary Market Funds).

PEP's Enhanced Due Diligence during the Business Relationship:

- Detecting new PEPs:
 - Customer Databases must be regularly screened to detect Customer with new PEP's status.
 - When the Customer's circumstances change during the Business Relationship and the Customer is newly qualified as a PEP, the Enhanced Due Diligence process shall be performed.
- The Transaction Monitoring framework must include the following elements:
 - The setting of a No cash funding transfer threshold both for wire transfers and securities transfers

- It will be forbidden to open a trading account with a cash deposit, this provision may be circumvented by making a deposit via an Electronic Money Issuer (EMI) which, through its agents, would accept cash deposits. Setting an e-money deposit threshold would help contain the ML/TF risks potentially associated with this type of transaction.

Reviews:

- Periodic reviews of business relationships with Politically Exposed Persons (PEPs) and high-risk customers shall be conducted at least annually—initially on the anniversary date of onboarding, and subsequently by the anniversary of the previous review. For medium-risk customers, periodic reviews shall be conducted every three years, and for low-risk customers, every five years.
- Event-based reviews must be conducted when the CMSP is informed or have the knowledge about the occurrence of a trigger event such as:
 - A change of Customer category (e.g. becomes a PEP)
 - The withdrawal of a regulated or listed status
 - The Customer is part of a merger / acquisition transaction
 - The Customer reactivates its inactive account
 - A Suspicious Transaction Report relating to the Customer is established
 - A change in the shareholding structure, notably in respect of the Beneficial Owner
 - A formal Request for Information from a competent administrative or judicial authority
- Full reviews must contain:
 - The updating of data in the information system and supporting documents. The information and documentation that must be collected depends on the category to which the Customer and the Business Relationship belong.
 - An analysis and implementation of checks in terms of ML/TF risks (e.g. PEP screening, Sanctions screening, Negative news checks⁹, etc.).
 - An Overall Account Analysis whose purpose is to identify and explain discrepancies between the information given on the Customer (income, activities, situation, etc.) and the information collected when monitoring the transactions on Customer's trading accounts. It is required when:
 - For Periodic Reviews: the Customer is rated High Risk or The Customer has a PEP status

⁹ In addition to the proprietary applications regarding PEP verification CMSP's shall use internet search engines.

- For Full Event-Based Reviews: a Suspicious Transaction Report has been carried out, the Customer is subject to a restrictive measure, the Customer is rated High Risk, or the Customer is a PEP

A full review must include a re-assessment of the Business Relationship's ML/TF risk rating profile based on the updated information collected during the review and the analysis and checks made on this occasion. A partial review is possible in the frame of an Event-Based Review. The frequency of periodic reviews depends on the nature and / or the profile of the Business Relationship.



Required Data and Supporting Documents for Private Companies and Listed Companies

ATA AT ONBOARDING	SUPPORTING DOCUMENTS AT ONBOARDING	EXPIRY DATE OF THE DOCUMENT PROVIDED BY THE CUSTOMER AT THE ONBOARDING	DATA OR SUPPORTING DOCUMENTS TO BE COLLECTED DURING A REVIEW
Identification Identity information	Extract from the official company registry (MoTRI)	3 months	No renewal of documentation required, except of a change in situation which could result from: The consultation of information in reliable public sources (e.g. Customer's website, official register, press, etc.) or In the absence of change, a confirmation by the Customer's Relationship Officer. In case he is unable to confirm this absence of change, a request for the same purpose is made to the client, as follows: The Customer confirms that there is no change by a declaration (KYC certification letter) or The Customer informs that there is a change of situation: renewal of documents / information under the conditions provided for when entering a Business Relationship
Full legal name Registered address Principal place of business (if different from above) Registration information (number, registering date and registering Authority)	Extract from the official company registry. Certification of this extract by an Authority might be considered	3 months Up to one year if the document is certified (optional).	
Ownership structure If listed on the ESX, mention of the transparency requirements	Letter of compliance from the ESX Chief Compliance Officer	3 months	Renewal
Ultimate Beneficial Owner Identification: Title Full name Date of birth Place of birth Other identifying information that may be collected Country of residence	For clients rated low to medium risk: Official documents authenticated by DARS (extract of the companies' registry, up-to-date articles of association, filed annual accounts, etc.) Document issued by the client (organization chart, annual balance sheet, etc) accompanied by a declaration from the client	No expiry date if the document is up to date. Checks can be carried out either on a representation of the document by the Customer or on Public Information.	No renewal of documentation required, except of a change in situation which could be detected from The consultation of information in reliable public sources (e.g. Customer's website, Official register, press, etc.) where these exist and appear in the searchable databases or In the absence of available information from reliable public sources, information relating to the knowledge of the client available to the client Relationship Officer, the absence of change of situation If the client Relationship Officer is unable to confirm the absence of change, a request for the same purpose is made to the client, as follows: The Customer confirms that there is no change by a declaration (KYC certification letter) or

	<p>Information from an external database accompanied by a declaration / confirmation from the client</p> <p>Consultation of the UBO register alone is insufficient, unless the information contained in the UBO register is corroborated by a document issued by the client (organization chart, annual report, etc.), or a client statement or external database.</p> <p>For clients rated high risk:</p> <ul style="list-style-type: none"> Official documents, except UBO register (extract of companies' registry, updated articles of association, etc.)_all authenticated by DARS Document issued by the client (organization chart, annual report, etc.) certified by a person practicing a regulated profession 		<p>The Customer informs that there is a change of situation: renewal of documents / information under the conditions provided for when entering into a Business Relationship.</p>
Other information relating to UBOs	<p>When the Legal Person Customer appears to have been established for the sole benefit of a PEP who is the Customer's UBO specific documents are required (see above PEP specific information to be collected)</p>	No expiry date if the document is up to date (either based on a representation from the Customer or on Public Information)	

Identification of Direct shareholders Full legal name Country of Incorporation	The collection of the relevant information relating to Direct shareholders may be based on the same "appropriate measures" as for UBOs		Same provisions as those regarding Ultimate Beneficial Owners
Corporate purpose Type of activity, line or nature of business or industry	Articles of incorporation, prospectus or equivalent document	No expiry date if the document is up to date (based either on a representation from the Customer or on Public Information)	No renewal
List of Controlling Parties (Beneficial owners) Title Name Date of birth Place of birth	Extract from official registry, DARS authenticated articles of association, annual report, prospectus or equivalent document		<p>No renewal of documentation (no obligation to collect a new official document), except in the case of change of situation resulting from:</p> <p>The consultation of information in reliable public sources (e.g. Customer's website, official register, press, etc.) where these exist and appear in these search databases, or</p> <p>In the absence of available information from reliable public sources, information relating to the knowledge of the client available to the client Relationship Officer, confirming the absence of change of situation</p> <p>If the client Relationship Officer is unable to confirm this absence of change, a request for the same purpose is made to the client, as follows:</p> <p>The Customer confirms that there is no change by a declaration (KYC certification letter) or</p> <p>The Customer informs that there is a change of situation: renewal of documents / information under the conditions provided for when entering into a Business Relationship</p>

Type of Business Activity and turnover or revenues	Customers rated low to medium risk or eligible to Simplified Due Diligence: Self-declaration (not acceptable in case of doubt regarding consistency of transactions with regard to the activity and revenues of the Customer, in which case Supporting Documentation is required) Customer rated High Risk: Supporting Documentation such as annual report, accounts or equivalent document		It is not necessary to contact the Customer when information relating to the activity and their revenues may be collected from the account Otherwise, renewal of self-declaration and / or Supporting Documents where applicable
Type of products or services offered to Customer	Self-declaration	1 year	No need to revert to the Customer when information relating to the activity and their revenues may be collected from the account. Otherwise, renewal of self-declaration from Customer
Exposure of the person to International Sanctions	Sanctions questionnaire applicable to a Legal Person Who has completed at least one tax year, and That perform international transactions	1 year	Renewal The answers to the Sanctions questionnaire must be updated at the same frequency as the Review
FATCA / CRS status and, as the case may be, Tax Identification Number	CRS: Self-certification and Tax Identification Number of non-resident Customers FATCA: Self-certification or US tax form W8-BEN-E or other W8 for non-US persons or W9 for US persons and waiver of banking secrecy in some cases and Tax Identification Number (TIN) of US Persons	1 year	No renewal, unless there is a change relating to the identity of the Customer, its country of residence, legal form or ownership structure
Remark: not applicable till foreign investors are allowed to invest in securities listed on the ESX			

2.1.2. Customer's Identity and Beneficial Owner(s) identity

Individual Customers are identified by the collection of their first and last names, as well as their date and place of birth. A Legal Entity Customer is identified by collecting its legal form, name, registration number and registered office address.

The checks to be carried out to certify identity are the following:

- For Natural Persons:
 - By presenting their biometric ID- the Fayda digital ID) or
 - By presenting the original or a certified copy of a valid official document bearing the individual's photograph, or a copy of such a document with mention of the name, surnames, date and place of birth, date and place of delivery of the document and name of the public authority that authenticated the document.
- For Legal Persons:
 - By submitting the original or a certified copy of any deed or an extract from an official register dated within the last three months, showing the company's name, legal form, registered office address, and the identities of its partners and directors or
 - Submission of a certified copy of a document issued by the relevant Registrar of Companies, such as the Ministry of Trade and Regional Integration (MoTRI), duly authenticated by the document Authentication and Registration Service (DARS)

2.1.3. Important Red Flags and Suspicion Indicators to watch out for when establishing and monitoring a Business Relationship with an Investor

The activation of a Red Flag does not necessarily mean that it is advisable not to enter - nor to terminate - a Business Relationship. But, as part of a Risk-Based Approach to combatting ML/TF, it does require Market Intermediaries and CMSPs to carry out Enhanced Due Diligence and further investigations, which in practice shall go as far as issuing a Suspicious Transaction Report to the FIS.

Whether related to a Natural or a Legal Person, these potential Red Flags include situations where:

- The Investor is reluctant to provide personal information.
- The Investor is reluctant or unable to explain either:
 - Their business activities and corporate history
 - The identity of the (Ultimate) Beneficial Owner

- Their source of wealth or funds
- Why they are conducting their activity in a certain manner
- The nature of their business dealings with third parties and who they are transacting with (particularly third parties that are in foreign jurisdictions)
- Individuals or connected persons who either:
 - Insist on the use of an intermediary (either professional or informal) in all interactions without sufficient justification
 - Are actively avoiding personal contact with the Customer Relationship Officer without sufficient justification
 - Are foreign nationals
 - Refuse to cooperate or provide information, data, and documents usually required to facilitate the establishment of a Business Relationship
 - Are PEP or have a family or professional association with a PEP
 - Are conducting transactions that appear strange given an individual's age (this is particularly relevant for underage Customers or elder people who should be more risk-averse due to their age)
 - Have previously been convicted of fraud, tax evasion, or serious crimes, or are under investigation or have known connections with criminals
 - Have been previously prohibited from holding a directorship role in a company
 - Have declared income that is inconsistent with their assets, transactions, or lifestyle
- Legal persons (or Legal Arrangements) that either:
 - Have demonstrated a long period of inactivity following incorporation, followed by a sudden and unexplained increase in their financial activities
 - Describe themselves as commercial business but cannot be found on the internet or social business network platforms
 - Are registered under a name that does not indicate the activity of the company or, conversely, under a name that indicates that the company performs activities or services that it does not provide
 - Are registered under a name that appears to mimic the name of other companies, particularly high-profile multinational corporations

- Use an email address with a domain name they obviously don't own (such as Gmail, Yahoo, Hotmail, etc.)
- Are registered under an address that does not match the profile of the company or that cannot be located or that is a mailbox service
- Where the director(s) or controlling shareholder(s):
 - Cannot be located or contacted
 - Do not appear to have an active role in the company
 - And / or Beneficial Owner(s) are listed against the accounts of other Legal Persons (or Legal Arrangements), indicating the use of professional nominees
 - Have declared an unusually large number of Beneficiaries and other controlling interests or have authorized numerous signatories without sufficient explanation or business justification.
- Are incorporated in a jurisdiction that is considered to pose a high risk of Money Laundering or Terrorism Financing, or in low-tax jurisdiction or international trade or finance center
- Conduct large value transactions with a small number of counterparties
- Conduct transactions with international companies without sufficient corporate or trade justification
- Maintain relationships with foreign professional intermediaries in the absence of genuine business transactions in the professional's country of operation
- Receive large sums of capital funding quickly following incorporation, which is spent or transferred elsewhere in a short period of time without commercial justification
- Maintain a bank balance of close to zero, despite frequent incoming and outgoing transactions
- Conduct financial activities and transactions inconsistent with the corporate profile
- Are incorporated in a jurisdiction that does not require companies to report Beneficial Owners to a central registry

- Operate using accounts opened in countries other than the country in which the company is registered
- Involve multiple shareholders who each hold an ownership interest just below the threshold required to trigger enhanced due diligence measures.
- Involve complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense
- Use professional intermediaries to establish simple investor relationships with securities brokers
- There is a discrepancy between the supposed wealth of the Investor and the amount dedicated to its investments.
- Natural or Legal persons:
 - Make frequent payments to foreign professional intermediaries
 - Are using multiple bank accounts – whether domestic or located abroad - without apparent reason or using brokerage accounts as long term depository accounts
 - Appear focused on aggressive tax minimization strategies
 - Demonstrate limited business acumen or appear uninterested in the structure of the company they are establishing, or have a complex company structure without sufficient business rationale
 - Perform excessively quick transactions and / or seem to trade illiquid securities – or OTC derivatives – to transfer value between several entities or redeems a long-term investment within a short period of time
 - Appear engaged in market manipulation (e.g. "pump and dump schemes or boiler room operations)
 - Require introduction to financial institutions to help secure banking facilities
 - Have not filed correct documents with the tax authority
 - Provide falsified records or counterfeit documentation
- Examination of business records indicates:
 - Fabricated corporate ownership records
 - Inflated asset sales between entities controlled by the same Beneficial Owner
 - Agreements for nominee directors and shareholders

- Family members with no role or involvement in the running of the business are listed as Beneficial Owners of Legal Persons
- Employees of professional intermediary firms acting as nominee directors and shareholders
- The resignation and replacement of directors or key shareholders shortly after incorporation
- The location of the business changes frequently without an apparent business justification
- Officials or board members change frequently without any apparent rationale
- Frequent changes of Beneficial Owner(s), or circular ownership for a group of Companies, or several changes in % of shares held by Beneficial Owner(s), which could be methods to transfer ownership abroad
- The Legal Person is suspected to be a shell company
- Orders are routed through Direct Market Access (DMA) accounts, resulting in a break of the Audit Trail
- Unexplained high number of wire transfers to and from the trading account:
 - With no apparent rationale
 - From and to third parties
 - Routed through nostro accounts or omnibus accounts at the request of the Customer
 - Suggest that the trading account is being used as a depository account or a conduit for transfers

2.2. AML/CFT onboarding and monitoring requirements for Capital Market Participants whose clients are other Capital Market Professionals

Proclamation 1248/2021 requires Capital Market Professionals – including Capital Market Service Providers and Market Intermediaries – to obtain a License from the Authority to carry out their activities.

These categories of Licensed Capital Market Participants with potential business relationships with other Professional Licensees may include:

- For Capital Market Infrastructures: Securities Exchanges, Securities Central Depositories, Securities Clearing Houses
- Licensed Self-Regulated Organizations

- Capital Market Service Providers (CMSP), such as:
 - Securities Brokers and Digital Sub-Brokers
 - Securities Dealers
 - Securities Market Makers
 - Securities Appraisal Firms and Credit Rating Agencies
 - Collective Investment Schemes Operators
 - Securities Portfolio Managers
 - Securities Investment Advisers (whether Individuals or Corporations)
 - Securities Robo-Advisers
 - Crowdfunding Intermediaries
 - Investment Banks (whether Independent or part of a Banking Group)

As an example, a Securities Broker will establish a business relationship with the Securities Exchange for transactions, the Central Depository for depositing the Securities and the Clearing House for the settlement of the transactions. All these Market Participants have in common to have successfully completed the Authority's licensing process.

Therefore, it is logical that CMSPs and Market Intermediaries should be able to establish business relationships with other parties licensed by the Authority, without having to carry out the same checks as those already carried out by the Authority regarding ML/TF issues, when granting or renewing their license.

2.2.1. Minimal checks to be performed on Licensed Market Participants

In this perspective, minimal checks to be made could be the following - if relevant in both ways - for each ECMA's licensed CMSP or Market Intermediary willing to establish a business relationship with another licensed Market Professional:

TYPE OF MARKET PARTICIPANTS	REQUIRED DOCUMENTS OR CHECKS
ECMA's Licensed CMSP or Market Intermediary independent from a Banking or Insurance group	Certified copy of the initial and/or renewed License or recent No-Objection Letter from the ECMA
If a Member of a Self-Regulating Organization	Certified copy of the initial and/or renewed License and No-Objection Letter from the SRO
If a subsidiary of a Bank (domestic)	Certified copy of the initial and/or renewed License and No-Objection Letter from the National Bank of Ethiopia (NBE)
If a subsidiary of an Insurance Company (domestic)	Certified copy of the initial and/or renewed License and No-Objection Letter from the NBE

This will allow to check the existence and the exact type of License delivered by the Authority to each of the CMSP / Market Intermediaries and to know the authorized perimeter for their activities.

The main advantage of a No-Objection Letter is that it enables a regulator or an SRO to give an opinion at a more recent date than that corresponding to the granting or annual renewal of its License to the Market Participant.

2.2.2. Potential specific vulnerabilities, Red Flags, and answers regarding some Licensed Market Participants

Central Securities Depository and Securities Clearing Houses

These Market Intermediaries can be used to introduce illicit assets into the Financial System. Once this is done, these assets can be transferred out or used to purchase securities. If illicit assets are successfully placed with depository institution, a CMSP may rely on the depository institution CDD/KYC investigation and assume that the investor poses no ML/TF risks.

In this regard, the vulnerabilities awareness and suspicious indicators associated with payment and securities transfer methods, Direct Market Access and Securities Intermediaries should all remain applicable.

2.2.3. Relevant additional direct or indirect AML/CFT checks and measures for the most important CMSP and Market Intermediaries regarding their internal organization

If applicable, a Group Risk-Based approach is required. Group rules should apply to Group Entities regardless of the location or type of activity. They must also comply with their own local regulations. Between the two, the most restrictive regulation must prevail.

1. Checks on internal organization and processes for combating ML/TF

The CMSP must ensure that its AML/CFT system is adapted to its size, the nature of its activities and the risks identified during the risk classification process. It must be equipped with the tools, material and human resources needed to effectively implement all Due Diligence obligations and to detect cases requiring additional Due Diligence.

The rules and procedures to follow relate to:

- The experience, qualifications, training and hierarchical position of the people involved in implementing the AML/CFT system.
- The checks to be carried out as part of the recruitment process for these people.
- External Service Providers who may be entrusted with carrying out all or part of the activities relating to the obligations of the AML/CFT system (this requires the existence of a written contract defining the terms and conditions of outsourcing).
- Procedures defining the organization of the internal control system, including criteria and thresholds for identifying significant incidents and system shortcomings, and internal control activities.
- Permanent and periodic controls.
- Corrective measures to remedy incidents and system shortcomings.
- Annual reporting to the Authority on the organization of the internal control system, the monitoring of the activity and the results of internal controls, and on any shortcomings observed in the system. This annual report must be approved by the Board of Directors of the Market Intermediary / CMSP and transmitted to the Authority.

- Informing the management body without delay of any significant incidents identified within the framework of internal control procedures.
- Where applicable, CMSP's governing body reports any significant incidents or shortcomings to the group's parent company.

2. Checks related to the establishment of the Business Relationship with Third Parties

A Business Relationship for a CMSP can be a direct Customer or a Customer brought in by a Business Introducer (BI), an Agent, or a Distributor. In the case the Customers remain the Customer of the BIs, Agents or Distributors, it is required that the CMSP also carries out the AML/CFT diligences on them before dealing with their customers.

If the BI / Agent / Distributor presents a low ML/TF level of risk, for example, if it is itself regulated in a way equivalent to the Regulation to which the CMSP is subject itself, then the CMSP must ascertain the existence and relevance of the BI / Agent / Distributor's AML/CFT system by mean of an appropriate questionnaire. If not, it is required that the CMSP applies its own AML/CFT Enhanced Due Diligence procedures to the BIs / Agents / Distributors before establishing a Business Relationship with them. Given the reputational risk that can arise from ML/TF fraud, it is necessary to systematically conduct Enhanced Due Diligence – including Fit and Proper verification – on unregulated potential Business Introducers, Agents, or Distributors. This must include the search for PEP shareholders or executives or for persons on Sanctions Lists.

Should a Self-Regulating Organization (SRO) issue a No-Objection Letter for one of its members, it should also be its responsibility to carry out these enhanced checks and keep them up to date.

3. Anti-Corruption and Anti-Bribery

Because of the potential links between Corruption or Bribery and Money Laundering issues, it is necessary to pay attention to its Anti-Corruption provisions when establishing a Business Relationship with a CMSP or a Market Intermediary.

Corruption offences are generally committed for the purpose of obtaining private gain. The proceeds of corruption are often laundered so that they can be enjoyed without fear of detection or confiscation. Accordingly, corrupt officials and individuals deploy strategies to disguise their identity and the original source of funds in order to place funds derived from corruption in the financial system

without detection and are therefore would be investors in Ethiopian Securities. Likewise, it is current in corruption cases that bribe payers tend to disguise the financial links between them and the corrupt officials - including the destination of the funds - using Money Laundering Schemes.

Therefore, Money Laundering can be a potential side-effect of Corruption and vice versa, through techniques such as mirror trading, front running, insider trading, market manipulation or commissioning, etc. Consequently, it is useful to ensure that business partners have Anti-Bribery and Anti-Corruption prevention measures in place when a new relationship is established, and subsequently. This requires to be able to check and formulate an opinion regarding:

- The existence and the completeness of a risk-mapping process, based on processes analysis, which identifies and evaluate the corruption risks associated with the types of business relationships with customers, suppliers and intermediaries.
 - e.g. if external Agents and Distributors are used and remunerated to bring in new clients, which might be the case for Brokers, CIS, crowdfunding intermediaries and also Investment Banks.
- Measures taken to address and mitigate these risks and if their current relevance and efficiency.
- The existence of:
 - An action plan and its implementation to deal with remaining risks.
 - A Code of Conduct for internal purposes and for relations with external partners.
 - Awareness and training programs for staff with details about proper conduct as examples.
- The evaluation process of the integrity of stakeholders and risks associated with them.
- Prevention measures regarding presents from suppliers and to customers, for example:
 - Pricing policies regarding customers (e.g. to detect a Portfolio Management mandate offered by a sales representative at an abnormally low rate) or
 - Detection of sudden profitable transactions on a client account belonging to or related to a PEP.
- Implementation of consistency checks in the IT tools used to record the parameters of the contracts in order to detect anomalies or exceptions.
- Existence of Red Flags checks such as:

- Presence of a PEP among the shareholders or the management of the business partner. Idem for a person that would be put on a Sanction List during the course of the Business Relationship.
 - Partner's reluctance to pass on detailed information about his business.
 - Low level of technical expertise of the selected partner in his professional field.
 - Unfavourable public information, allegations, lawsuits, or convictions concerning the partner or its managers regarding Corruption and Bribery issues.
 - High degree of economic dependence of the service provider on its customer.
- Existence of a whistleblowing procedure that:
- Guarantees the confidentiality of its identity for the whistleblowers, whether internal or external.
 - Has been communicated internally, together with the details of how to submit a report, communicate with the person responsible for collecting it and inform the whistleblower of the action taken. This communication can be integrated within the Code of Conduct of a given potential partner and / or a Self-Regulated Organization.
 - Allows to inform the CEO / General Manager of the most prominent alerts.
- Clear procedure not to enter or to end a Business Relationship if certain conditions are not met.

Additional remarks:

- It is important to respect the principles of proportionality between the estimated risks and the Due Diligence requirements.
- It may be decided to assess only the most important potential partners, rather than implement a full risk-based approach for each of them.
- An initial pre-assessment of the potential partner's Corruption prevention and detection measures can be carried out by means of a questionnaire sent to the potential partner.
- When the potential partner is part of a Group, it might be of some interest to assess the Anti-Corruption Group policy as well.
- As with other risk assessment procedures, it is necessary to update this Anti-Corruption assessment annually or in the event of any new element likely to have an impact on it (e.g., the public disclosure of a corruption scandal or in the perspective of a merger with another CMSP / Market Intermediary).

- Investigations carried out and documents obtained during risk assessments regarding actions taken and their results must be archived.

For each identified risk of Corruption or Bribery that could lead to ML/TF issues, the following process is recommended for Risk Assessment:

- Risk Mapping for each process to assess

Description of the Risk Situation	
Scoring / Assessment of the degree of risk <u>before</u> taking remedial / mitigation measures into account	
Existing remedial or mitigation measures	
Scoring / Assessment of the degree of risk <u>after</u> taking remedial or mitigation measures into account	
Compliance Department / Management opinion on the acceptability of the residual risk	

- Action Plan for each of the assessed processes

Additional measures to be taken	
Person(s) in charge	
Lead time	
Implementation of indicators and means of control	

4. Measures to deal with Conflicts of Interest

A Conflict of Interest can be defined as a situation in which an employee, exercising his/her rights and powers, could be placed in a situation that allows him to place his/her own personal interest before the company's or client's interest.

Conflicts of Interest too can have side effects related to ML/TF issues, whether they are actual or potential. How a CMSP, Market Intermediary or SRO prevents and manages Conflicts of Interest is therefore another relevant indicator of ML/TF risks. For example, through front running techniques or pairing orders, a Broker can be against its clients' interest.

Proper management of Conflicts of Interest should be carried out or provide:

- The mapping of risks – comparable to the above mapping - within the CMSP or Market Intermediary.
- The design and implementation of a prevention policy embedded in the organization's processes, in a way that is aligned with other risk reduction policies of the firm.
- Training and awareness development for all employees and provide employees with a self-assessment tool.
- The declaration of potential conflicts of interest by all employees to a Compliance or Ethics Officer. For small businesses, this can be outsourced.
- Building Conflicts of Interest detection measures into third-party Due Diligence procedure (i.e. at the KYC stage):
 - The organization could insert a clause into its contracts requiring third parties to declare potential conflicts of interest.
 - Check whether there are any personal relationships (i.e., interests) between the third party (and their Beneficial Owners) and its own employees, Directors, and Beneficial Owners.
 - Where a third party acts as a business intermediary (such as a Business Introducer, an Agent, or a Distributor), these checks could be extended to include pre-existing relationships between the third party and the end customer (and its Beneficial Owner).

Appropriate remedial measures shall be applied, proportionate to the nature and severity of the issues identified.

2.3. Measures to freeze or seize assets (based on International Sanctions)

Unlike other provisions, asset freezing and seizure measures are not based on a Risk-Based Approach but on an obligation to achieve results. They are also more likely to be related to Terrorist Financing issues, in addition to potential Money Laundering issues. Confiscation prevents criminal property from being laundered or reinvested either to facilitate other forms of crime or to conceal illicit proceeds.

According to Proclamation No. 780/2013, Article 37(3), the funds belonging to terrorists, those financing terrorism, and terrorist organizations designated by the United Nations Security Council under Chapter VII of the UN Charter must be frozen by a decision of the Council of Ministers. Following this decision, financial institutions and designated non-financial businesses and professions are required to immediately freeze any such funds in their possession that are linked to the specified individuals and entities and report them to FIS. By way of analogical interpretation of this provision, Capital Market Service Providers (CMSPs) shall be deemed financial institutions and, accordingly, shall be obligated to freeze any funds or assets associated with terrorist financing.

2.4. Specific Provisions for Securities Issuers

As per article 2/37 of Proclamation 1248/2021, an Issuer is defined as "any person who issues or proposes to issue any security; and shall include a government, company or other legal entity that offers securities to the public".

The Issuer is ultimately responsible for all compliance issues, including ML/TF compliance issues, despite the use of intermediaries to carry out the transactions. And that the Authority shall also monitor the compliance of the various stakeholders.

Whether the transaction involves shares or bonds, a private placement by an investment bank or a crowdfunding intermediary, an IPO, or a subsequent offering, it is recommended that the same rules and due diligence requirements outlined below apply in principle, with only minor variations depending on the specific context. At this stage, it is also recommended that simplified AML/CFT due diligence to be applied to 'Emerging Growth Companies' or to companies listed, or planning to be listed.

2.4.1. Designation of an Intermediaries

Although the Issuer holds responsibility for appropriately managing money laundering and terrorist financing (ML/TF) risks, it is recommended that the Issuer appoint an intermediary to handle all operations related to the issuance of securities, including the oversight of ML/TF risks. Consequently, the Issuer must ensure that the appointed intermediary is 'fit and proper' and possesses the necessary capacity to manage these ML/TF-related obligations.

Such intermediary could be the Investment Bank selected by the Issuer, a Crowdfunding Intermediary, or an Independent Listing Sponsor. In the case the selected Professional is already Licensed by the Authority, the checks mentioned above in part 2.1.1 are sufficient.

Regarding Investors, a specific situation might arise in the case of a Private Placement, which should normally only be accessible to Professional Investors (such as Collective Investment Schemes) and to “Qualified Investors”. Regarding the latter, it is up to the intermediary, or a third party to whom he has delegated this task, to ensure that the potential Investor is eligible for the status of “Qualified Investor” and that the proper AML/CTF Enhanced Due Diligence is duly conducted.

For crowdfunding intermediaries, which are Licensed by the Authority, when dealing with non-qualified investors they will have to carry out Due Diligence on their Customers themselves.

The usual provisions should apply to PEPs willing to participate in a Private Placement or an IPO.

2.4.2. Additional checks about the origin of funds at the book-building stage

Whether at the Initial Public Offering or in case of a subsequent capital increase, by applying the appropriate due diligence the Investment Bank in charge of the Book Building Operations should also ensure that the invested funds are licit.

Record Keeping

Records of all ML/TF Due Diligence operations conducted with Investors and Market Professionals on behalf of the Issuers should be kept by the Issuer and the Coordinator and be available for the Authority. The same should apply to all contracts established between the various stakeholders involved in the operations.

These elements must be considered as part of the audit trail, in the same way as those relating to transactions.

3. Reporting obligations to the Authority

The principal legislation regarding AML/CFT is Proclamation on Prevention & Suppression of Money Laundering and Financing of Terrorism no. 780/2013 as amended no.1387/2015. Capital Market Service Providers (CMSPs) and Market Infrastructures shall report Suspicious Transaction Reports (STRs) to the Financial Intelligence Service (FIS). Failure to comply with this obligation shall entail legal consequences as stipulated under the applicable proclamation. Furthermore, the Ethiopian Capital Market Authority (ECMA) shall verify compliance with this reporting requirement during its inspections.

Regarding the fight against ML/TF, it is standard practice for Financial Market Authorities to receive an Annual Control Report from Market Participants detailing their AML/CFT systems and the results achieved. The report covers compliance, risk control (permanent and periodic) and whether appropriate measures have been taken in the event of default.

This is an essential source of information for the Authority to assess the degree of compliance of the various Capital Market Professionals with AML/CFT regulations and ensure the quality and the effectiveness of the internal control system, including when all or part is outsourced. This report also provides comparisons not only between the various players, but also overtime, in terms of the degree of maturity and progress of AML/CFT systems. In addition, it enables the Authority to fine-tune the preparation of its annual Audit and Inspection program, and to identify specific issues that could be the subject of Inspection missions on cross-functional themes.

This annual AML/CFT report should be transmitted to the Authority in the quarter following the end of the calendar year and must be signed by the CEO or General Manager of the Market Intermediary / CMSP. The AML/CFT report may be submitted together with other reporting obligations stipulated under ECMA directives.

This report is both a means for the Regulator to monitor the ML/TF risks to which the Market Intermediaries / CMSPs are exposed, and to ensure that their administrative and supervisory bodies are properly informed about the effectiveness of the internal AML/CFT system. The Authority may ask questions and seek clarification on this report. The involvement of the Chief Compliance Officer and management is required in drawing up and validating the answers provided to the ECMA. When applicable, the report should also be made available to the Statutory Auditors.

For Capital Market Participants that are subsidiaries of a Banking or Insurance Group, the Annual Control Report must also include the AML/CFT measures implemented at the group or parent company level. The same applies to members of Self-Regulating Organizations, when applicable. Conversely, in application of the principle of proportionality, for small CMSP such as individual Financial Advisers, it may be possible to lighten the content of their Annual Control Report.

Elements of the previous report that are still relevant may be repeated, but it is recommended that attention be drawn to new elements (new businesses, new products or services, new customer segment, etc.) and to changes in the AML/CFT system (changes in risk classification and risk assessment, in dedicated

staff, or deployment of new tools or procedures, etc.) compared with the previous year.

The recommended content and structure for this annual report to the Authority are as follows:

3.1. Presentation of the Business and Activity

3.1.1. Type of Company, Legal Form, and Shareholding Structure

The following information is required:

- Name and legal form of the Legal Person / Natural Person
- Amount of Capital and Shareholder's equity
- Date of creation, Address
- Identification of all shareholders holding more than 5% of the capital, directly or indirectly:
 - Presence of foreign shareholders, including foreign Nationals
 - Presence of PEPs
 - Information about the parent Company when applicable

3.1.2. Products and Services, Customers and Distribution Channels

- Lines of Products (e.g. Portfolio Management, Collective Investment Scheme, Crowdfunding, Investment Advice, etc.)
- Global Turnover, Turnover split by Customer's segments, and number of Customers per line of Business
- Distribution Channels (e.g. direct distribution, introducing agents, distributors, etc.)

3.1.3. Professional Related Parties

- Identification of all related parties involved in the Business Activity (e.g. A Portfolio Management Company will have relations with the Banks or Financial Institutions from where the funds will be incoming, one or several Brokers, which will themselves be in relation with Securities Depositories, Clearing Houses...).
- Identification of all companies to which tasks are being outsourced (see below for Stakeholders involved in AML/CFT related tasks)
- Identification of the Statutory Auditors

3.2. AML/CFT Compliance Organization

The risk management policy must be duly documented, explaining the measures and procedures used to measure and manage risks, the measures taken to

safeguard the independence of the control function, the risk management techniques used, and details of the allocation of responsibilities within the Market Intermediary / CMSP relating to operational responsibilities and procedures.

3.2.1. Human Resources

- Description of the various Lines of Responsibilities involved in the AML/CFT system:
 - Management / Board Members / Audit Committee
 - Chief Compliance Officer / AML Officer
 - Compliance Officers
 - Internal Audit Resources
 - Functional organization chart showing the names and functions of key personnel
- Academic and Professional skills of all persons involved in the AML/CFT system and Personnel recruitment checks
- Description of Training Actions and Plans

3.2.2. Information System

- Internally developed tools
- Of the shelf tools (e.g. Monitoring software, STR Automation tools)
- Outsourced AML/CFT tasks
- Record-Keeping tools
- Knowledge-management Software and Documentation Policy
- Elements in place to guarantee the audit trail

3.2.3. Description of the internal AML/CFT Organization for each line of Business

E.g. Organization of responsibilities, documentation, reporting and controls for a Market Intermediary / CMSP:

Group Entity Management		Business Unit	General Management
Responsibilities			
Normative Documentation	Applying Group Normative Documentation in the Group Entity, whether directly or under its declination by operational procedures	Applying Group Normative Documentation and deploying the AML/CFT management program within the Business Unit	Ensuring that the Group acts in accordance with applicable laws and regulations by establishing an independent Compliance function
Internal Reporting	Supervision of the production and monitoring of relevant data and indicators: being responsible for the quality of such information, reporting such data to the management of the business unit and sharing it with the AML Officer of the Group entity	Consolidating, summarizing and monitoring the relevant data and key indicators, and being responsible for the quality of such information, and reporting them to the Chief Compliance Officer of the Business Unit	Analyzing relevant data regarding the Group's risk (such as the Compliance Risk Assessment)
Controls	Ensuring that Level 1 controls are applied and that each hierarchical level applies the relevant operational procedures	Organizing in collaboration with the Chief Compliance Officer of the Business Unit, Level 1 control procedures at Group Entity Level	Ensuring that internal control committees review the AML/CFT program

3.2.4. Description of the Customers' ML/TF Risk Assessment Process

- Detailed Customer Risk Assessment Process when entering a Business Relationship
- CDD/KYC Procedures:
 - Conditions to be eligible for Simplified Due Diligence
 - PEPs and Sanctions List Identification and Screening Procedures

- Identified Red Flags and / or Trigger Events
- Negative information search process
- Monitoring Procedures:
 - Description of the framework for reporting incidents of non-compliance
- Decision Process for not entering a Business Relationship and / or transmitting a STR to the FIS

3.2.5. Description of the Internal Controls Organization

- Level 1: Permanent Controls, i.e. day-to-day checks by operational staff:
 - Existence of cross-checks (four-eyes policy)
 - Description of the escalation process for detected anomalies
 - List of automated control processes
 - Identified flaws and corrective measures taken
- Level 2: Periodic Controls performed by the Internal Audit
 - Description of the Audit Procedures, Methodology and Documentation, including:
 - Frequency of Audits
 - Selection and Sampling Criteria
 - Control sheets
 - Decision process regarding the Annual Audit Plan
 - Structure and content of the Internal Audit's Reports
 - Contradictory presentation and follow-up processes of Audit Reports
 - Training role of the Internal Audit Department
- Outsourced Control tasks:
 - List and nature of Outsourced Control tasks
 - Identification process of potential conflicts of interest regarding Outsourced Control tasks
 - List of checks applied to subcontractors at the time of selection and during the life of the business relationship, particularly regarding compliance with AML/CFT regulations
 - Main features of the subcontract

3.3 ML/TF Risk Assessment, Remedial Measures and Resulting Risks

It is necessary to assess the ML/TF risks both in terms of the nature of the products and services offered to customers by Market Intermediaries / CMSP, and in terms of the business processes implemented within them.

3.3.1. Business Line ML/TF Risk Mapping

For each Business Line, an intrinsic Risk Evaluation must be conducted in order to assess the level of ML/TF risk of the activity. This requires:

- To evaluate the level of threat and the probability of occurrence due to the nature of the business
- To identify the various checks implemented to mitigate these risks
- To evaluate the residual risks for the Business Line

However, it is possible to implement checks and measures that can significantly reduce this risk, such as:

- Obligation to deposit funds with a domestic Ethiopian bank
- Prohibition on opening an account with a Legal Entity based abroad
- Ban on cash deposits
- Obligations for outgoing transfers to be made to the bank from which the funds originate Etc.

3.3.2. Business Processes ML/TF Risk Mapping

A Risk Mapping exercise must also be carried out for each business process, including:

- An identification of ML/TF risk situations by process
- An evaluation of the likeliness of occurrence and of the consequences before implementation of control measures
- A list of implemented checks and mitigation measures
- An evaluation of the remaining risks after implementation of such measures

The risk assessment process must be:

- Fully documented so as to be able to demonstrate its relevance to the Authority
- Regularly reviewed and updated (at least once a year)

3.4 Quantitative and Qualitative Reporting

The provision of quantitative data – in addition to Qualitative information – will enable the Authority to make analysis and comparisons over time, and between the various Capital Market Professionals. The information provided to the Authority

by the Annual Report enables better knowledge and monitoring of Licensed Market Professionals and Financial Products. Their completeness and accuracy is therefore essential. The following elements shall be included in the Annual Report:

3.4.1. Information on the Annual Report production process

Operations / Duties	Description of processes and staff implicated (including external when applicable)
Data collection and reporting	<p>Which are the Departments involved in the data collection process?</p> <p>How is it automatized at the stages of collection and consolidation?</p> <p>What external assistance is involved?</p> <p>Is the data collection and consolidation process reliable?</p> <p>Description of technical means and methods involved in the reporting production process</p>
Review of the draft version of reporting	<p>Who oversees reviewing the draft reporting within the Compliance Department?</p>
Validation of reporting	<p>By the Chief Compliance Officer or other?</p>
Transmission of reporting to the Authority	<p>By the Chief Compliance Officer, CFO, or other C level?</p>

3.4.2. Human Resources

- Number of employees (full-time equivalent) in charge of:
 - Permanent 1st-level controls and compliance with AML/CFT procedures
 - Periodic 2nd-level controls and compliance with AML/CFT procedures
 - If Permanent and / or Periodic controls are outsourced the same figures are required
- Staff training actions:

- Average hours of AML/CFT-related training in the last calendar year
- Number of employees who have had their AML/CFT level checked or assessed during the last calendar year

3.4.3. Criteria and Thresholds

- Description of the criteria and thresholds defined in your internal control procedures to identify significant incidents and major AML/CFT deficiencies
- List of recurring patterns sought by control units
- List of used Red Flags and Trigger Events

3.4.4. Permanent controls (Level 1)

- Scope, date, and frequency of inspections carried out during the last calendar year
- Major incidents and shortcomings
- Corrective measures implemented, with a planned completion date and status of implementation as of the date of the report

3.4.5. Periodic controls (Level 2)

- Scope and date of inspections carried out in the last calendar year
- Major incidents and shortcomings over the past calendar year
- Corrective measures implemented, with a planned completion date and status of implementation as of the date of the report
- Follow-up procedures for corrective actions (tools, people in charge, etc.)

3.4.6. Database screening and transaction monitoring tools

- Indicate whether database and flow filtering is automated or manual, and in particular:
 - For customer database filtering, the categories of customers whose identifiers are filtered and the number of customers concerned
 - For filtered transaction flows, indicate whether the system covers incoming flows, outgoing flows, transactions, principals, and beneficiaries
- Give further indications about:
 - The frequency with which databases are filtered, and the filtering methods used when entering into a business relationship or carrying out a transaction for an occasional customer or a customer whose account was previously inactive

- The lists used to filter databases and flows, specifying whether they come directly from a competent authority or are supplied by an external service provider
- Spelling and/or date of birth reconciliation methods used for database and flow filtering
- If the filtering mechanism is automated, indicate whether there is a backup mechanism in case the filtering devices are blocked

3.4.7. Clients

- Number of Legal Persons and Natural Persons
 - Split by investment product or service categories
 - Number of new Customer contracts, including online / remote
- Median length of relationship
- Number of PEPs (Natural Persons and Beneficial Owners of Legal Entities)
 - Number of new PEPs for which an account has been opened during the last calendar year
 - Number of closed PEP accounts during the last calendar year
 - Number of detected PEP who had not self-declared themselves as such
- Number or proportion of dormant accounts
 - Number of dormant accounts reactivated during the calendar year
- Number of clients deemed low-risk and high-risk vs standard-risk
 - Number of clients for which the risk status has been revised during the calendar year
- Number of decisions not to enter into a business relationship with prospects for AML/CFT reasons and reasons for doing so

3.4.8. Business Lines Risk Assessment

- Date of the last risk classification review
 - Emerging risks identified during the last calendar year due to the launch of new products, business lines, or the use of new distribution channels, etc.

3.4.9. Suspicious Transactions Reports (STR)

- Number of STR transmissions to the FIS
- Number of cases that have been detected and investigated

- That led to a STR, including when the Business Relationship was not established
- For which no further action was taken (except change in Customer's risk classification)
 - Short summary of the nature of the transactions that led to writing an STR

3.4.10. Outsourced task in relation to ML/TF issues

- List of outsourced tasks and associated contracts
- List of contracts that include training component
- List of terminated outsourcing contracts

3.4.11. Reporting conclusion

Market Intermediary / CMSP's own view of the strengths and weaknesses of its AML/CFT system

Highlights of the AML/CFT system evolution over the past calendar year

Appendix 1 – Content of the Annual Control Report

In their current form and content, the annual control reports sent by CMSP/MIs to regulators are extremely comprehensive and detailed. As we have already mentioned, this level of requirement may not be appropriate for players in a nascent capital market. It may be advisable, as has been the practice elsewhere, to have a more restricted initial level of requirement and to raise it over the years as the players become more professional and are able to draw on more experience and human resources. For this reason, we have distinguished between a minimum AML/CFT content for the annual control report and optional content that may be added later.

Minimum content

Presentation of the Business and Activity:

Type of Company, Legal Form, and Shareholding Structure

The following information is required:

- Name and legal form of the Legal Person / Natural Person
- Amount of Capital and Shareholder's equity
- Date of creation, Address
- Identification of all shareholders holding more than 5% of the capital, directly or indirectly:
 - Presence of foreign shareholders, including foreign Nationals
 - Presence of PEPs
 - Information about the parent Company when applicable

Products and Services, Turnover and Distribution Channels

- Lines of Products (e.g. Portfolio Management, Collective Investment Scheme, Crowdfunding, Investment Advice, etc.)
- Global Turnover, Turnover split by Customer's segments, and number of Customers per line of Business
- Distribution Channels (e.g. direct distribution, introducing agents, distributors, etc.)

Clients

- Number of Legal Persons and Natural Persons
 - Split by investment product or service categories
 - Number of new Customer contracts, including online/remote
- Median length of relationship
- Number of PEPs (Natural Persons and Beneficial Owners of Legal Entities)
 - Number of new PEPs for which an account has been opened during the last calendar year
 - Number of closed PEP accounts during the last calendar year
 - Number of detected PEP who had not self-declared themselves as such
- Number or proportion of dormant accounts
 - Number of dormant accounts reactivated during the calendar year
- Number of clients deemed low-risk and high-risk vs standard-risk
 - Number of clients for which the risk status has been revised during the calendar year
- Number of decisions not to enter into a business relationship with prospects for AML/CFT reasons and reasons for doing so

Suspicious Transactions Reports (STR)

- Number of STR transmissions to the FIS
- Number of cases that have been detected and investigated
 - That led to a STR, including when the Business Relationship was not established
 - For which no further action was taken (except change in Customer's risk classification)
- Short summary of the nature of the transactions that led to writing an STR

Full potential content

Identical to sections 3.1 to 3.4

Appendix 2 – Content of a Suspicious Transaction Report (STR)

Prior to any transmission of a STR, the CMSP must have designated a declarant and an FIS correspondent (which can be the same person). The STR must contain the following information:

- The declarant's identification and professional contact details.
- The occupation of the person making the declaration.
- The identification details of the customer and, where applicable, of the beneficial owner of the transaction being and, if a business relationship has been established with the customer, the purpose and nature of this relationship. Identification requires the following information:
 - for individuals: business activity and assets.
 - for legal entities: company registration number, legal form, and business sector
- A description of the operation and the analysis that led to the declaration. It is advisable to give priority to characteristic movements and/or the most significant amounts. The following information is required:
 - Reason for writing a STR.
 - Period of events.
 - Total amount involved.
 - Number of individuals or companies covered by the STR.
 - Main financial instruments used.
 - Number of transactions.
 - Transactions status.
 - Scheduled execution date and time for transactions not yet executed.
 - Analysis of facts and indications of money laundering.
- When the operation has not yet been carried out, its completion deadline.
- The declaration is accompanied, where applicable, by any documents required for its processing, particularly trading account statements, if possible, in a format that can be processed electronically or other documents such as those relating to the opening of an account. Additional information likely to confirm, modify, or invalidate the initial suspicion must be brought to the FIS's attention without delay.