**Anti-Money Laundering and Counter Terrorism Financing ("AML/CTF") Manual (Policy and Procedures)**

**History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Release Date** | **Description** | **Initiated/Amended by** | **Reviewed by the RR** | **Approved by the Board on** |
| V. 0.1 | June 2023 | AML/CTF Manual (Policy and procedures) | Benoit Carpentier de Changy | N/A | N/A |
| V. 0.2 | June 2023 | Amendment of the AML/CTF Manual (Policy and procedures) | Bastien Collette | XX/XX/2023 | XX/XX/2023 |

This AML/CTF Manual (the “Manual”) is owned by Bastien Collette in its capacity as RC (as defined below) of Vault AM S.à r.l. (“Vault AM” or the “Company” or the “IFM”). If you have any queries or comments regarding the information contained in this document, please contact the Manual Owner as shown below:

* Name: Bastien Collette
* Function: RC
* Tel: +352 661 65 99 45
* Email : bacollette@palana.lu

Vault AM has assigned to one third party the responsibility as «RC» (“*responsable du contrôle du respect des obligations professionnelles liées à la lutte contre le blanchiment et le financement du terrorisme*” as per Article 4(1) paragraphe 2)a) of the AML/CTF Law).

The RC maintains this Manual and updates it in relation to any changes to the applicable Luxembourg AML/CTF legal and regulatory framework including AML/CTF professional obligations and observed market practices as well change in the business model of the Company.

This Manual will be reviewed at least on an annual basis, to assess, amongst others, if the Manual is compliant with international norms, standards and recommendations as well as with Luxembourg AML/CTF legal and regulatory framework applicable to the sector within which the IFM operates. Where no update is required, the Manual will be applied consistently over time. Where update is required, the formal approval by the Board of Directors of Vault AM (the “Board”) is required.

**Connected documents**

This Manual outlines the Company’s main applicable Luxembourg AML/CTF professional obligations.

It should be read in conjunction, amongst others, with the

* “Vault AM AML/CTF risk appetite statement”
* “Vault AM ML/TF own risk assessment”.
* “Vault operational procedures and KYC checklists of the 1st Line of Defence (“1 LoD”)
* “Vault AML tax compliance policy and procedures”

**Confidentiality level**

This document is strictly confidential. This document is the property of the Company and must not be copied or used for any purpose other than that for which it is supplied. Where clients or other counterparties/business relationships, ask to be provided with a copy of this document they should be invited to contact the Manual Owner. A copy of this Manual should not be provided to any external parties without the explicit permission of the Manual Owner.

**Copyright**

Copyright and all rights reserved by the Company. No part of this Manual may be reproduced or transmitted in any form or by any means (electronic, mechanical, paper copy, recording or otherwise) without the prior written permission of the Manual Owner.

Table of Content

[1. Introduction 6](#_Toc138062095)

[1.1. Definitions and acronyms 6](#_Toc138062096)

[1.2. Background – Identification of the Fund and its investment strategy 6](#_Toc138062097)

[1.3. Purpose and Objectives 6](#_Toc138062098)

[1.4. Parties / stakeholders of the Company 8](#_Toc138062099)

[1.5. Definitions of money laundering and terrorist financing 8](#_Toc138062100)

[1.6. Key AML/CTF legal and regulatory framework 10](#_Toc138062101)

[1.7. Sanctions 10](#_Toc138062102)

[2. AML/CTF Key roles and responsibilities 11](#_Toc138062103)

[2.1. At the level of the IFM 11](#_Toc138062104)

[2.2. At the level of the Fund 11](#_Toc138062105)

[2.3. At the level of the 1st LoD of the IFM 12](#_Toc138062106)

[2.4. At the level of the Distributors 12](#_Toc138062107)

[2.5. At the level of the Depositary Bank 12](#_Toc138062108)

[2.6. At the level of the External Auditor 13](#_Toc138062109)

[**2.** **The Five key Pillars of the AML/CTF Program** 14](#_Toc138062110)

[3.1. Risk-based approach 14](#_Toc138062111)

[3.1.1. AML/CTF risk appetite statement 14](#_Toc138062112)

[3.1.2. ML/TF own risk assessment 15](#_Toc138062113)

[3.1.3. Risks associated to the Customers (including investors, initiators, distributors) / Business relationships 16](#_Toc138062114)

[3.1.4. Geographical Risk 16](#_Toc138062115)

[3.1.5. Risk profile on the assets 16](#_Toc138062116)

[3.1.6. Risk associated to delivery (distribution) channels 17](#_Toc138062117)

[3.1.7. Risk associated to products and the launch of services 17](#_Toc138062118)

[3.1.8. Other ML/TF Risk Factors 17](#_Toc138062119)

[3.2. Adequate internal organisation and management requirements 18](#_Toc138062120)

[3.2.1. Outsourcing 18](#_Toc138062121)

[3.2.2. Appropriate policies, controls and procedures 19](#_Toc138062122)

[3.2.3. Whistleblowing policy and procedures 20](#_Toc138062123)

[3.2.4. Systems 21](#_Toc138062124)

[3.2.5. Appointments of a RR and a RC 22](#_Toc138062125)

[3.2.6. Ongoing training programs (staff awareness, training and recruitment) 24](#_Toc138062126)

[3.2.7. The three lines of defence 24](#_Toc138062127)

[3.2.8. Audit – Internal control functions 25](#_Toc138062128)

[3.3. Customer due diligence obligations 25](#_Toc138062129)

[3.3.1. Customer due diligence 26](#_Toc138062130)

[3.3.2. Identification and verification of the Client 29](#_Toc138062131)

[3.3.3. Identification and verification of the identity of the beneficial owner(s) 32](#_Toc138062132)

[3.3.4. Timing of the identification and verification of the identity 35](#_Toc138062133)

[3.3.5. People purporting to act on behalf of and for the client (proxies, PoA, signatories, etc.) 36](#_Toc138062134)

[3.3.6. Obtaining information on the purpose and intended nature of the business relationship 37](#_Toc138062135)

[3.3.7. Due Diligence – risk scoring and level of due diligence 38](#_Toc138062136)

[3.3.8. Simplified Due Diligence (“SDD”) 39](#_Toc138062137)

[3.3.9. Enhanced due diligence (“EDD”) 40](#_Toc138062138)

[3.3.10. Refusal and exiting a business relationship 43](#_Toc138062139)

[3.3.11. Performance of customer due diligence by third parties 44](#_Toc138062140)

[3.3.12. Tax considerations – AML Tax Compliance 44](#_Toc138062141)

[3.3.13. Record keeping and data protection 44](#_Toc138062142)

[3.3.14. Due Diligence on assets 46](#_Toc138062143)

[3.4. Ongoing monitoring of the business relationship 47](#_Toc138062144)

[3.4.1. Keeping all information and documents up-to date 48](#_Toc138062145)

[3.4.2. Name-screening 49](#_Toc138062146)

[3.4.3. Detection of complex or unusual transactions 49](#_Toc138062147)

[3.4.1. Blocked account 50](#_Toc138062148)

[3.5. Obligations to cooperate with the authorities 51](#_Toc138062149)

[Annex 1. Definitions and acronyms 54](#_Toc138062150)

[Annexe 2– Key AML/CTF legal and regulatory framework (non-exhaustive list) 61](#_Toc138062151)

[Annex 3 – Overview of key predicate offences perpetrated within collective investments 67](#_Toc138062152)

[Annex 4 – Annex II, III and IV of the AML/CTF Law as amended 68](#_Toc138062153)

# Introduction

## Definitions and acronyms

Please refer to Annex 1 of this procedure for further information about the definitions/acronyms used in this AML/CTF Manual.

## Background – Identification of the Fund and its investment strategy

Vault AM S.à r.l. is an alternative investment fund manager incorporated and governed by the laws of the Grand-Duchy of Luxembourg. It is registered with the Registre de Commerce et des Sociétés de Luxembourg under number B276659 and having its registered office at 5, Rue Goethe, L-1637, Luxembourg – Grand Duchy of Luxembourg.

The IFM’s greatest asset is its reputation which it seeks to protect through the highest standards of service and professional conduct.

The IFM is fully committed to comply with legislation to prevent money laundering (“ML”) and terrorist financing (“TF”) and to take all reasonable measures to be in compliance with applicable AML/CTF laws and regulations. Although these measures will not completely eradicate the ML/TF risks the IFM will be exposed to, the risk-based application of the mitigation measures will help reducing these risks, while protecting the Board, the Senior Management, the employees and all business relationships of the IFM from legal proceedings and preserve the Company’s reputation.

## Purpose and Objectives

The IFM is subject to AML/CTF professional obligations.

This AML/CTF Manual has been designed to ensure compliance with the applicable Luxembourg AML/CTF laws and regulations as well as to effectively manage and mitigate the ML/TF risks the IFM may face.

The purpose and objective of this Manual are to set out the rules that must be implemented in order to be in a position to:

* Be compliant with the applicable AML/CTF laws and regulations;
* To establish a robust framework in order to avoid the IFM from being used to commit ML/TF acts;
* Ensure that all members of the IFM (including the Senior Management and the Board) have received an information pack in respect of AML/CTF regulations in force and have had the opportunity to ask questions;
* Guide all members of the IFM (including the Senior Management and the Board) in relation to the ML/TF prevention and detection;
* Protect the IFM and its Board, Senior Management and employees against any corporate or personal liability that might arise under the applicable AML/CTF laws and regulations;
* Perform a sound monitoring of IFM’s and business relationships;
* Proper apply an escalation line process and protect the reputation of the IFM by minimizing reputational and regulatory risks relating to ML/TF related activities.

## Definitions of money laundering and terrorist financing

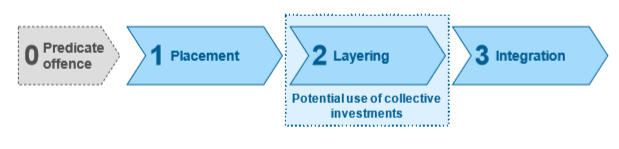
**Money laundering** (“ML”) is a criminal act whereby money that has been obtained through criminal activities is processed in order to conceal the true origin and ownership of the funds[[1]](#footnote-2). If successful, the money can appear legitimate at the end of the laundering process.

The objective of a money launderer is to place illegal money in the financial system, without arising suspicion; move the money around, often in a series of complex transactions and/or crossing multiple jurisdictions, so it becomes difficult to identify its original source; and then move the money back into the financial and business environment, so that it appears as legitimate funds or assets.

In accordance with the Luxembourg legislation, ML means any action as defined in Articles 506-1 of the Penal Code and 8-1 of the Law of 19 February 1973 on the sale of medicinal substances and the fight against drug addiction, as amended.

When dealing with ML, the main issue is the origin of the funds, which are derived from a criminal activity. ML presupposes the existence of a predicate offence whose object or proceeds may give rise to a ML offence. Please refer to the Penal/Criminal Code (“Code Pénal”), for the list of predicate offences.

It should be stressed that a ML offence occurs even where the predicate offence has been committed abroad, provided however, that such offence constitutes a predicate offence both in Luxembourg and abroad.

Money Laundering stages[[2]](#footnote-3):

Generally, money laundering occurs in three stages:

1. cash generated from criminal activities first enters the “financial” system at the "**placement**" stage, where that cash is converted into monetary instruments, such as money orders or traveller’s checks, or deposited into accounts at financial institutions;
2. at the "**layering**" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin;
3. at the "**integration**" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Investment funds are more sensitive to ML/TF risks, especially at the layering stage (stage 2 of the diagram above).

Some predicate offences may be perpetrated within the collective investments industry itself, which increases the likelihood of the three stages of ML also occurring within collective investments.

**Terrorist financing** (“TF”) is the financial support or sponsoring, in any form, of terrorism or of those who encourage, plan or engage in terrorist activities.

Pursuant to the “Luxembourg legislation, "terrorist financing” means any action as defined in Article 135-5 of the Penal Code.

When dealing with TF, one of the main issues is the destination of the funds which are at risk of being used for terrorist purposes. Contrary to ML, the money might come from a licit activity.

Diagram

Description automatically generated

## Key AML/CTF legal and regulatory framework

Please refer to Annex 2 of the Manual for the key Luxembourg AML/CTF legal and regulatory framework applicable to the IFM.

Please refer to the CSSF website for an exhaustive list and further details:

<https://www.cssf.lu/en/anti-money-laundering-and-countering-the-financing-of-terrorism/>

## Sanctions

There are several type of sanctions, such as warning notice, reprimand, public statement which identifies the natural or legal person and the nature of the breach, withdrawal or suspension of authorization to exercise.

A temporary prohibition up to five years: to exercise an activity in the financial sector or to process/complete one or more operations and to exercise a function within the executive/senior management of a professional.

Administrative sanctions[[3]](#footnote-4)

* 1. Credit institutions/financial institutions: maximum of € 5.000.000 or 10 % of the total annual turnover (legal persons)
  2. Natural person: € 5.000.000
  3. A fine between € 250 and € 250.000 to any legal or natural person that contravene the injunctions/the application of the powers of the supervisory authorities, or have knowingly provided documents or information that is incomplete, inaccurate or false in relation to requests or enquiries made by the Luxembourg authorities. The supervisory authorities will publish any decisions that result in sanctions or other administrative measures on their official webpage including the type and nature of the violations committed and the identity of the person(s) concerned. The authorities may refrain from such publication where deemed disproportionate, where it would seriously jeopardise the stability of the financial market or impede an ongoing investigation

Penal / Criminal sanctions[[4]](#footnote-5)

1. Anyone who knowingly breaches the AML/CTF Law is subject to a fine of €12,500 to €5,000,000
2. Terrorist financing: may be punishable by a prison term of 1 year up to life imprisonment and/or a fine of €2,500 to €50,000
3. Money laundering: is punishable by a prison term of 1 to 5 years and/or a fine of €1,250 to €1,250,000

Please refer to the AML/CTF Law for further details.

# AML/CTF Key roles and responsibilities

## At the level of the IFM

IFM’s primary AML/CTF obligation is to perform a risk-based due diligence on the Fund, including, amongst others, the identification and verification of the identity of the initiator of the Fund, the assessment of the Fund’s AML/CTF policy/procedures and of the ML/TF risks of entering into business with the Fund.

The IFM performs initial and on-going due diligence on:

* The Investors through its 1st LoD;
* The Initiator(s) of the Funds it manages;
* The assets/investments performed on behalf of the Funds,
* Any other business relationships of the IFM

The IFM executes directly:

* The tasks relating to AML/CTF (“Know Your Customer”) on the Investors and on the investments/assets performed by the IFM on behalf of the Funds it manages, through its 1st LoD; and
* The AML/CTF name-screening checks on the investors and Fund’s investments.

## At the level of the Fund

It is the responsibility of each Fund to develop and maintain an effective and well documented AML/CTF program which complies with the applicable Luxembourg AML/CTF laws and regulation and which is adequate to the ML/TF risks of the Fund which includes, amongst others: the appointments of a RR and a RC (which must be registered on GoAML), an AML/CTF risk appetite statement, an ML/TF own risk assessment and an AML/CTF policy and procedures.

It is understood that the ultimate AML/CTF responsibility remains with the Board of the Fund.

## At the level of the 1st LoD of the IFM

The 1st LoD of the IFM will perform the due diligence on the investors, on the clients (initiators) and on the investments performed on behalf of the Funds. Each file is reviewed, assessed and validated in writing by the acceptance committee.

The RC and the RR of the IFM controls the reports provided to them and may refuse files provided where there is any doubts or suspicions about the consistency of the KYC documentation.

Due to the fact that Vault AM, as part of its services offered to the Fund, receives the names of the investors who are recorded in the Fund share/unit-register, the IFM performs, amongst others, name-screening, transaction monitoring, initial and ongoing due diligence (including KYC) on such investors applying its own AML/CTF policy, procedures and processes.

Please refer to the AML/CTF operational procedures of the 1st LoD for further details on the operational application.

## At the level of the Distributors

The IFM acts as distributor to distribute the shares or units of the Fund.

The distributor function supports the Funds by marketing and distributing its shares through a variety of channels.

Please refer to the distribution and marketing policy of the Company.

## At the level of the Depositary Bank

Pursuant to the Depositary Agreement, Quintet Private Bank (Europe) S.A. has been appointed as Depositary Bank of the IFM.

The Depositary is responsible, amongst others, for the safe-keeping of assets, the day-to-day administration of assets and for overseeing asset valuations, for subscriptions and redemptions, to carry out manager instructions, for transaction settlement and income distribution.

The Depositary must comply with Luxembourg AML/CTF legal and regulatory framework and its AML/CTF obligations, including but not limited to the identification of the Fund, its beneficial owner(s) and related parties, name screening, transaction monitoring/filtering and cooperation with the authorities.

## At the level of the External Auditor

The External Auditor is in charge of the certification of financial reports and other legal reports.

The audit of the Vault AM annual accounts by the External Auditor (“*réviseur d'entreprises agréé”)* also includes the compliance with the Luxembourg AML/CTF legal and regulatory requirements and provisions.

1. **The Five key Pillars of the AML/CTF Program**

The AML/CTF internal framework of the IFM is articulated around the following 5 pillars:

1. **Risk-based approach** - Obligation to apply a risk-based approach (AML/CTF risk appetite statement, ML/TF own risk assessment, customer risk scoring, country risk assessment, etc.);
2. **Adequate internal organization and management requirements** - Obligation to have an adequate internal organization and management requirements (RR/RC, AML/CTF training, AML/CTF policy and procedures in place, etc.);
3. **Customer due diligence** - Obligation to perform customer due diligence (know your customer, SoF/SoW, etc.) and record-keeping;
4. **Ongoing monitoring of the business relationship** - Obligation to perform an ongoing monitoring of the business relationship including but not limited to pay special attention to certain activities and transactions, name screening and keeping information, data and documents up-to-date);
5. **Cooperation with the authorities** - Obligation to cooperate with the authorities.

It is the responsibility of the IFM to develop and maintain a distribution landscape which complies with the applicable laws and regulations.

## Risk-based approach

The risk based approach (“RBA”) is a prerequisite for compliance with all other requirements. An effective RBA allows Vault AM to identify, assess and understand the ML/TF risks that it may face to and to mitigate them. This assessment is proportionate to the nature, business model and size of the Company.

The main elements which comprise an adequate RBA are the “AML/CTF Risk Appetite Statement” and the “ML/TF Own Risk Assessment”.

### AML/CTF risk appetite statement

As mentioned in article 4 (4) of the CSSF Regulation 12-02, as amended, *“the determination by the professional of its “risk-based approach” shall be based on the definition of the* ***ML/TF risk appetite****, as approved by the Board of Directors and implemented by the authorised management. The strategy shall be consistent with this approach. Policies, procedures and controls with respect to AML/CFT implemented within the professional shall be consistent with the previously defined risk appetite. This definition and strategy shall be communicated in a precise, clear and comprehensible form to the whole staff”.*

The Board defines the risk appetite of the IFM which is the amount and type of ML/TF risks that the Board is ready to accept or not in the course of its business activities in order to meet its strategic objectives.

The risk appetite contains the following statements/has the following purpose:

* Define a robust financial crime risk appetite framework together with its associated ML/TF risk assessment is compulsory and fundamental to any professional subject to the AML/CTF Luxembourg law of 12 November 2004 as amended;
* Is the foundation of the AML/CTF control environment;
* Is the expression of the level of risk that the Board is willing to accept or refuse. The acceptable and unacceptable risks compose the core of the AML/CTF risk appetite statement as approved by the Board;
* The AML/CTF risks that the Board is willing to accept or refuse shall consider the applicable laws and regulation as well as the business and strategic objectives of the Company;
* Require a multi-dimensional review taking into account the strategic objectives of the Company, its knowledge of targeted markets and its capacity to mitigate ML/TF risks.

The AML/CTF risk appetite statement includes the two main categories of ML/TF risks :

* The ones directly prohibited by applicable laws and regulations
* The ones that the Board is willing to take/or not by considering multiple aspects (client’s type, reputational risks, etc.)

The risk appetite statement of the IFM is reviewed annually or on an ad-hoc basis (when needed or in case of trigger events).

Please refer to the AML/CTF risk appetite statement of Vault AM for further information.

### ML/TF own risk assessment

When assessing the ML/TF risks, the IFM identifies, assesses, evaluates, understands and mitigates the ML/TF risks it may face and exercises reasonable business judgment by taking into consideration the risks associated to the customers/business relationships/investors, products, investments, transactions, countries/geographical zones and distribution channels but also to consider all relevant risk factors applicable.

The ML/TF own risk assessment takes into consideration and integrates, amongst others, the following information:

The FATF’s RBA Guidance for the Securities sector dated October 2018;

The other FATF’s Guidelines and publications;

The revised guidelines, by EBA, on money laundering and terrorist financing risk factors (in particular Guideline 16 , as defined under Articles 17 and 18(4) of Directive (EU) 2015/849; which were formally adopted by the CSSF Circular 21/782);

* The joint guidelines issued by the three European Supervisory Authorities (ESMA, EBA and EIOPA) (the “European Supervisory Authorities”) on money laundering and terrorist financing risk factors;
* The AML/CTF Law as amended and in particular the non–exhaustive list of risk factors and cases of potentially higher and lower risks as listed in its appendices II, III and IV;
* The national and supranational risk assessments as well as the CSSF sub-sector risk assessment on collective investments as amended in 2022 and the national vertical risk assessment on terrorist financing and on legal persons;
* The publications from the authorities (for instance: CSSF circulars; etc.);
* Its own assessment of the ML/TF risks.

When carrying out its ML/TF own risk assessment, the IFM takes into account all relevant risks before coming to a conclusion on its global risk level and the types of measures to be taken to mitigate such risks.

The ML/TF own risk assessment is updated each time a significant change occurs to Vault AM activities, to the business, in particular when considering, amongst others, to serve new types of investors, through new distribution channels and from new geographical areas, etc.

The review of the ML/TF own risk assessment could also be triggered following a specific request from specific events but it is updated regularly, once per year minimum as a rule.

Separated documents detailing the inherent ML/TF risks the IFM is exposed to, the controls in place to mitigate these identified ML/TF risks and the residual risks are available for consultation to the authorities. The ML/TF own risk assessment is documented in writing, kept up to date and approved by the Board.

Please refer to the detailed ML/TF own risk assessment for further details.

### Risks associated to the Customers (including “investors, initiators, distributors and all Business relationships”)

Customers ML/TF risk assessment is done at the identification stage prior to customers’ acceptance, and is monitored and adapted accordingly on an on-going basis during the business relationship.

Classification of Fund(s) initiators, advisors, investors, assets in which the IFM invests on behalf of the Fund it manages, parties involved in transactions, etc. is executed during the identification stage prior to acceptance, and is monitored and adapted accordingly on an on-going basis during the relationship.

The ML/TF risks associated to the customers/business relationships are provided by Vault AM and is performed by the 1st LoD of the Company.

### Geographical Risk

The IFM performs a country ML/TF risk assessment and has a AML/CTF country risk scoring for all the countries where a customer, an investment and related parties or any business relationships are based, domiciled.

It assesses by writing whether a member state or a third country imposes equivalent obligations to those provided for by the AML/CTF Luxembourg legal and regulatory framework. The reasons for concluding that a Member State or a third country imposes equivalent obligations are documented in writing when the decision is taken and are based on relevant and up-to-date information. The obligation imposed by a Member State is presumed to be equivalent, except when relevant information gives indication that this presumption is not maintained.

The AML/CTF country risk scoring assessment is performed by the 1st LoD.

Please refer to the AML/CTF country risk scoring assessment of the IFM for further details.

### Risk profile on the assets

The IFM establishes, on a risk-based approach, appropriate due diligence controls by asset class (low risk) or per asset (medium and high risks). The TFS/PF controls (name-screening) on all assets and related parties are performed directly by Vault AM (before the investment and on an ongoing basis/daily).

Please refer to the due diligence on assets procedures of the 1st LoD for further details.

### Risk associated to delivery (distribution) channels

The IFM determines the risks inherent to a distribution channel by considering, amongst others, the ML/TF risk profile of the parties involved in the distribution channel (i.e.: the level of AML/CTF controls it applies as well as the level of supervision it is subject to, the risks associated with the country of domicile or activity, the transparency of the distribution channel, the nature of the business, the source of funds as well as the risks relating to the business relationships) and its ability to monitor and obtain additional information about the business made through the distribution channel.

### Risk associated to products and the launch of services

The risk assessment includes the identification, understanding and assessment of the ML/TF risks that might result from the development of new products/services and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products as well as on a defined ongoing basis to ensure that any change in circumstances is adequately considered.

The IFM takes appropriate measures in order to manage and mitigate those risks. This risk assessment takes place before the launch or use of new products or new business practices. The person in charge in Vault AM of developing the new product/service is responsible for making this assessment, and the compliance is consulted for its opinion during the process and the RR must validate the assessment, by writing, prior the launch of the products/services.

An ongoing monitoring must be performed and a new risk assessment must be performed in case of changes.

### Other ML/TF Risk Factors

ML/TF risk factors like the organization of the IFM are taken into account in the own ML/TF risk assessment of the Company.

The IFM ensures that the proliferation financing and terrorist financing risks are assessed and mitigated in its own ML/TF risk assessment.

The IFM has communication means allowing it to provide information on its risk assessment to the authorities.

## Adequate internal organisation and management requirements

The IFM :

* maintains a permanent and adequate internal organization to effectively mitigate the ML/TF risks the IFM is exposed to, trough, amongst others, policies, procedures and information systems.
* Ensures that the governance and oversight of the AML/CTF program are effectively managed and implemented.

### Outsourcing

Where the IFM outsources a function to a third party (either within the Grand Duchy of Luxembourg or in another country), the Board remains ultimately responsible for the activities undertaken on its behalf and for compliance with the regulations.

The IFM cannot contract out of its statutory and regulatory responsibilities to prevent and detect ML and FT.

Outsourcing examples include but are not limited to:

* + AML/CTF training
  + Collection and validation of CDD
  + Compliance support
  + RC
  + Provision of Directors
  + Record keeping
  + Registered agent
  + Registered Office
  + Sanctions screening

Where the IFM is considering the outsourcing of functions to a third party, it should:

* + Review the CSSF’s guidance notes on outsourcing under relevant Laws;
  + Consider implementing terms of reference or an agreement describing the provisions of the arrangement;
  + Ensure that the roles, responsibilities, and respective duties of the IFM and the outsourced service provider are clearly defined and documented;
  + Ensure that the Board, RC, other third parties and all employees understand the roles, responsibilities, and respective duties of each party;
  + Ensure that appropriate oversight of the work undertaken by the outsourced service provider.

Prior to a decision being made to establish an outsourcing arrangement, the IFM must make an assessment of the risk of any potential exposure to ML and FT and must maintain a record of that assessment as part of its RBA.

The IFM should monitor the risks identified by its assessment of an outsourcing arrangement and review this assessment on an ongoing basis in accordance with its RBA obligations.

The Board must ensure, at the commencement of an outsourcing arrangement and on an ongoing basis, that:

* The outsourced service provider:
* Has the appropriate knowledge, skill and experience;
* Is sufficiently resourced to perform the required activities;
* Has in place satisfactory policies, procedures and controls which are, and continue to be, applied to an equivalent standard and which are kept up to date to reflect changes in regulatory requirements and emerging ML and FT risks; and
* Is screened and subject to appropriate due diligence to ensure the probity of the outsourced service provider
* The work undertaken by the outsourced service provider is monitored, by the Senior Management, to ensure it complies with the requirements and the regulations;
* Any reports or progress summaries provided to the IFM by the outsourced service provider contain meaningful, accurate and complete information about the activities undertaken, progress of work and areas of non-compliance identified; and
* The reports received from the outsourced service provider explain in sufficient detail the materials reviewed and other sources investigated in arriving at its conclusions so as to allow the IFM to understand how findings and conclusions were reached and to test or verify such findings and conclusions.

The IFM cannot place reliance on the outsourced service provider’s reports. The Board should therefore ensure the veracity of any reports provided, for example by spot checking aspects of the reports.

The IFM must ensure that any outsourced service provider has in place procedures which include a provision that knowledge, suspicion, or reasonable grounds for knowledge or suspicion, of ML and/or FT activity in connection with the IFM’s outsourced business will be reported in a timely manner. An exception would be where the outsourced service provider suspects that the IFM itself is complicit in the ML and/or FT activity whereby the outsourced service provider would report their suspicion directly to the CRF.

Where the IFM chooses to outsource or subcontract work to an unregulated entity, the IFM should consider if this increases the risk, in which case appropriate and effective controls to address the risk should be implemented.

The head of compliance must ensure that the compliance review meets the requirements as detailed above and where not, that the deficiencies are advised to the Board for their consideration of the Compliance status and any enhancements that may be required.

Where the Board are unable to meet the requirements above, they must evidence the issue, the remedy to achieve compliance as soon as practicable together with their consideration of informing the authorities if required.

### Appropriate policies, controls and procedures

The IFM puts in place policies, controls and procedures to identify, assess, understand, mitigate and manage effectively the ML/TF risks identified at international, European, national, sectoral and at the level of the IFM itself.

Those policies, controls and procedures, which take into account the ML/TF risks, are proportionate to the nature, specificities and size of the Company. The policies, controls and procedures include amongst others:

1. the development of internal policies, controls and procedures, including model risk management practices, customer due diligence, cooperation, record-keeping, management of personal data, internal control, compliance management and employee screening, the appointment of a compliance officer at appropriate hierarchical level;
2. an independent audit function to test the internal policies, controls and procedures referred to in point a).

This AML/CTF Manual includes and describes the IFM’s AML/CTF professional obligations.

All the following procedures and operational instructions are validated in advance by the authorised management and the RR and is subject to regular monitoring by the latter for the purpose of adapting them to reflect future changes to the legal framework in this field, to IFM’s clientele and to its business activities:

* The Client Acceptance Committee procedure,
* The details of the procedures governing the identification, evaluation, monitoring, management and mitigation of ML/FT risk, centred around a risk analysis procedure that will be reviewed on a regular basis,
* The procedure to be applied in respect of clients who are not physically present when entering into the business relationship,
* The procedure for accepting and monitoring the business relationship with clients when Enhanced Customer Due Diligence measures must be applied,
* The procedure to follow when using the products and services of a third-party introducer pursuant to article 3-3 of the AML Law,
* The procedure to comply with in order to monitor changes in business relationships, as well as transactions carried out on behalf of clients, with a view to detecting suspicious transactions,
* The procedure to follow when there is evidence or grounds to suspect money laundering or terrorist financing,
* The procedure to follow in cases involving companies in the process of incorporation before measures to verify the identity of the clients and related parties have been completed,
* The recruitment procedures as well as the programme for training and raising awareness among staff,
* The exact description of the specific responsibilities inherent in each role occupied by members of staff in terms of AML/CFT,
* The procedure to follow in respect of including information on the payer with fund transfers and wires (Regulation (EU) 2015/847).

Please refer to the IFM’s AML/CTF operational procedures for further details.

### Whistleblowing policy and procedures

Vault AM maintains internal alert arrangements (whistleblowing) which enable the entire staff to draw attention to legitimate concerns about internal governance or internal and regulatory requirements in general.

Employees are protected under the Whistleblowing Law provided:

* They have reasonable grounds to believe that the information reported on the violations was true at the time of the report and that this information falls within the scope of this Act ; and
* They have made a report, either internal or external, or have made a public disclosure.

All forms of retaliation, including threats and attempts to retaliate, are prohibited against individuals who have reported breaches under the terms of this Manual.

These arrangements respect the confidentiality and identity of the persons who raise such concerns and provide for the possibility to raise these concerns outside the established reporting lines as well as within the supervisory body.

It is to be noted that any person, and in particular employees or former employees of entities of the financial sector in Luxembourg, may in good faith submit a report directly to the CSSF in a confidential and secure manner if that person has reasonable grounds for believing that the report will show breaches of applicable regulation by entities or persons of the financial sector which fall under the supervision of the CSSF. The whistleblowing procedure should however not be used for breaches which are clearly of a criminal nature, such as the unlawful exercise of activities of the financial sector. Persons becoming aware of facts which may constitute a crime or an offence are requested to inform the State prosecutor.

Before contacting the CSSF, employees are requested to first use the whistleblowing procedures in their workplace.

The CSSF will, in principle, only consider a written statement of information transmitted by e-mail to the following address: [whistleblowing@cssf.lu](mailto:whistleblowing@cssf.lu).

If this is not possible or if the employee does not feel able to do so for a first contact, the employee may call the secretariat of the CSSF department JUR-GEN (telephone number +352 2625 1 2757) during office hours before transmitting a written statement. The CSSF does not audio record whistleblowing telephone calls.

Please consult the CSSF website for more information on the following links.

<https://www.cssf.lu/wp-content/uploads/whistleblowing_EN.pdf>

Please refer to the Whistleblowing policy and procedures of the Company for further details.

### Systems

The IFM has implemented systems to monitor transactions and identify persons (e.g. persons identified on TFS, PF, black lists, adverse medias and PEP lists) among the share registers, lists of persons with a power of attorney and persons or entities with whom they maintain a business relationship, shareholding companies (if any), beneficial owners and the assets in which Vault AM invests on behalf of the Fund(s) it manages.

The IFM has systems in place that enable the Company to respond fully and rapidly to enquiries from the Luxembourg authorities responsible for combating ML/TF as to whether it maintains or has maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship, through secure channels and in a manner that ensures full confidentiality of the enquiries.

The IFM has its own database in which it tests and assesses the information received/collected.

The IFM completes and maintains up to date a database including, all investors, the person(s) purporting to act on their behalf, the legal representatives (directors, etc.) of the investors, the shareholding companies (if any), their beneficial owner(s). The database also includes all data and information related to the investors’ subscriptions and redemptions as well as the investors’ risk categorisation.

The Compliance of the IFM ensures that the different systems put in are adequate regarding the specificities of the Company and performs a regular report about it to the RC/RR.

### Appointments of a RR and a RC

The IFM has appointed a RR (a person responsible for AML/CTF at senior management level - responsible of the respect of the AML/CFT obligations, “RR”) as well as a RC (an AML/CFT Compliance Officer - responsible of the control of the respect of the AML/CFT obligations, “RC”).

The RR at least:

* Has sufficient AML/CTF knowledge with regard to the applicable Luxembourg and European legislation and regulation and can demonstrate (e.g. trainings) this upon request;
* Is part of the management,
* Is knowledgeable about the investments and distribution strategies of the IFM and about the services offered by it,
* Is available without delay upon contact to the Luxembourg AML/CTF competent authorities,
* Can cumulate its function with one or more other functions provided the accumulation does not impede its independence and objectivity.

The RR is responsible for the overall compliance with the professional obligations as regards AML/CTF.

The RR performs in particular the following duties and obligations (non-exhaustive list):

* Initially validates the AML/CTF supervisory system,
* Defines, reviews on a periodic basis, with the assistance of the RC, and approves AML/CTF control framework (including this Manual, as well as the determination of the AML/CTF risk appetite and the ML/TF own risk assessment of the Company),
* Participates in and authorizes the implementation of the AML/CTF risk appetite framework in coordination with the Board and the RC,
* Approves new correspondent relationships, new or existing relationships with PEP (entry and ongoing basis) and new and existing relationships involving a high-risk country, or establishment and maintenance of higher-risk business relationships/higher risk occasional transaction,
* At its regular Board meetings, monitors compliance of the IFM with this Manual including monitoring the performance by the RC of its duties and consider the reports presented by the RC; takes, where appropriate, any necessary actions or measures as a result thereof;
* Is consulted by the RC for the application of appropriate measures where a suspicious activity or transaction is identified, where appropriate,
* Receives some KPI's/KRI's from the RC (the number of high-risk customers and aggregated statistical data providing an overview of the reasons why customers have been classified as high risk (PEP, etc.), number of STR, name-screening hits, etc.);
* Receives regular reports from the RC,
* Reviews, validates and approves, on annual basis, a summary report on compliance of the IFM with AML/CTF professional obligations prepared by the RC, and, if necessary, decides the content and implementation of a remediation plan for any deficiency identified.

The RC, at least :

* Has the professional experience and knowledge of the Luxembourg AML/CTF legal and regulatory framework, the hierarchy and powers within the entity as well as the availability necessary to the effective and autonomous exercise of his/her function,
* Is located on a permanent basis in Luxembourg.

The RC is in charge of monitoring and assessing the compliance risks and the adequacy and effectiveness of the measures, policies and procedures put in place within the IFM to ensure compliance with the AML/CTF laws and regulations applicable to it.

The RC (non-exhaustive list):

* Prepares, implements and ensures the realisation of the ongoing training and awareness-raising programmes of all the employees (including senior management and the Board) of the Company,
* Regularly controls the adequacy of the AML/CTF supervisory system,
* Makes sure that the AML/CTF framework set by the RR of the IFM is implemented and applied,
* Regularly reviews the adequacy of AML/CTF policy and procedures,
* Applies the AML/CFT policy and procedures of the IFM and has the power to propose to the RR and to the Board, on his own initiative, any measure necessary or useful to this end, including the release of required means,
* Ensures the quality of the AML/CTF controls carried out by 1st LoD and, as the 2nd LoD and verifies compliance with all the AML/CFT professional obligations on Vault AM level,
* Is involved systematically in the acceptance of customers/beneficial owners or persons purporting to act on behalf of them which are/or which involve high risk countries or with high risk profile,
* Is the privileged contact person for the Luxembourg authorities in charge of AML/CTF as regards AML/CTF issues and for the competent authorities and is in charge of the transmission of any information or statement to these authorities,
* Regularly reviews process, rules and controls used for suspicious transaction and suspicious behavior reporting,
* Must be provided with reports on suspicious transactions/persons identified and is solely competent to decide on the application and scope of measures required where a suspicious activity or transaction is identified and their termination. The RR should be consulted where appropriate,
* Can contact directly the authorities or governing body,
* Receives reports from the 1st LoD regarding business relationships entered without the verification of the identity and where it is impossible to verify the identity of the customer and beneficial owner within the timeframe set by the internal rules of the 1st LoD,
* Retains all written reports submitted to him,
* Provides to the RR/ Board regular and ad hoc reports on the follow up of the recommendations, problems and shortcomings and irregularities identified during the course of regular controls and verifications of the compliance with the AML/CTF Manual, Reports specify the related risks and their severity, propose corrective measures and the position of persons concerned,
* Prepares at least once a year, a summary report on his activities and his operation and submit it to the RR / Board,
* Updates the Board and the RR with changes in AML/CTF applicable regulations,
* Formally attests annually that the annual compliance work has been performed (or highlights shortcomings),
* Receives screening/transaction alert reports (i.e. true hit) from the 1st LoD.

The RC is the primary contact point of the 1st LoD with regards to AML/CTF matters.

The accumulation of the function of RC and one or more other functions will not impede the independence, objectivity and decision-making autonomy of the RC. His workload is adapted so that the efficiency of the AML/CTF framework is not compromised.

The RC has timely access to customer identification data and other due diligence information, transaction records, and other relevant information. The RC, in the context of his mandate with the IFM is able to act independently and reports directly to the Board.

The names of the RR and the RC appointed in accordance with the above points have been communicated to the authorities.

### Ongoing training programs (staff awareness, training and recruitment)

The RC ensures that all employees, senior management and members of the Board are aware of and trained in respect to their AML/CTF professional obligations, in line with the IFM’s activity and the provisions contained in the Luxembourg AML/CTF legal and regulatory framework (including data protection).

The RC ensures that the staff concerned is aware and informed about the recent developments in AML tax compliance requirement in order to enable them to identify the transactions that may be linked to the laundering of advantages from predicate tax offences.

To this end, all the employees, senior management and Board members participate, at least on an annual basis, in special ongoing training programs to, amongst others:

* Be aware and be informed of new developments, including information on techniques, methods and trends in ML/TF, and to help them recognise operations which may be related to ML/TF and to instruct them as to how to proceed in such cases,
* Provide them with clear explanations of all aspects of the Luxembourg AML/CTF legislation and professional obligations and, in particular obligations concerning risk based approach, customer due diligence, record-keeping and cooperation with the authorities (which includes suspicious transaction reporting).

The RC maintains records of the trainings (including the presentation and the attendance list).

Compliance ensures that the set-up of recruitment procedures for all the staff fulfils the criteria of adequate professional standing and experience according to the risk of money laundering and terrorist financing related to the duties and functions to be carried out. In particular, information as regards the possible judicial record of the persons concerned is obtained when hiring members of the management by requiring, among others, an extract of the police record or an equivalent document from the person concerned.

### The three lines of defence

Compliance ensures that AML/CTF governance and internal organization of the IFM is organised on the “Three lines of defence” model:

* A first line of defence based on operational units, i.e. the persons in charge of business execution which are in direct contact with customers and which require a good understanding of the ML/FT risks,
* A second line of defence based on the person in charge of controls, including other support, monitoring and compliance functions involved in AML/CTF matters, consisting of providing support, verifying the controls carried out by the first line of defence, and contributing to an independent control of the risks. The level of involvement of the second line must increase with the customer’s risk level,
* A third line of defence based on the audit function which independently assesses the first two lines of defence and also verifies the effectiveness of the professional’s AML/CTF policies, procedures and programs.

### Audit – Internal control functions

The IFM has internal control functions that include the internal audit function, which has sufficient resources and independence to test compliance, including sample testing, with the procedures, policies and controls and to enjoy the independence which is necessary to perform their tasks. These verifications are an integral part of the mission of the internal audit function.

The control of the AML/CTF policy, procedures and process of the IFM is an integral part of the mission of the internal audit function.

One of the mission of IFM internal audit is to:

* Perform the control of the AML/CFT procedure,
* Test the AML/CTF internal policies, controls and procedures,
* Assess the management and control of the risks on an independent basis and report to the authorised management and to the Board by providing them, at least once a year, with a summary report on the compliance with the AML/CFT procedure,
* Ensure that his recommendations or corrective measures are acted upon.

Please refer to the internal audit dedicated procedures and internal audit monitoring plan for further guidance.

## Customer due diligence obligations

AML/CTF due diligence is essential in identifying, assessing, understanding and mitigating the relative ML/TF risks that certain customers (including investors), business activities/relationships and investments may pose to the IFM.

The risk assessment and the due diligence is performed before entering into any business relationship and needs to cover any new investors (including intermediaries) and distributors acting on behalf of underlying investors and their relevant related parties (and including their beneficial owners) and/or before performing an investment on behalf of the Fund the IFM manages.

The AML compliance officer of the 1st LOD assesses and regularly reviews the ML/FT risk of all the business relationships, including amongst others:

* Initiators,
* Investors,
* Potential Distributors,
* Assets (in which the Fund invests),
* Other business relationships of the IFM.

Before entering into any agreement or business relationship, the AML compliance officer of the 1st LoD performs due diligence measures to ensure the ML/TF risks linked to the services provided or business undertaken are duly identified, assessed, understood and mitigated accordingly.

The RC performs ongoing monitoring and oversight of the 1st LoD to assess the continuing adherence to the due diligence requirements defined in this Manual and control the 1st LoD operating effectiveness.

The RR, with the assistance of the RC, oversees the activities of the 1st LoD.

### Customer due diligence

The IFM carries out Customer Due Diligence (“CDD”) measures in any of the following cases:

* When establishing a business relationship (i.e.: before the establishment of a business relationship or the carrying-out of the transaction),
* When carrying out an occasional transaction that:

1. Amounts to EUR 10.000.- or more, whether this transaction is carried out in a single operation or in several operations which appear to be linked, or
2. Constitutes a transfer of funds, as defined in point (9) of article 3 of regulation (EU) 2015/847 of the European Parliament and of the council of 20 may 2015 on information accompanying transfers of funds and repealing regulation (EC) no 1781/2006, exceeding EUR 1,000. This specific case is foresee by the AML/CTF Law but due to the IFM business model and activities, the IFM will not perform or receive occasional transactions on behalf of or for its clients.

* When there is a suspicion or reasonable grounds for suspicion of money laundering, associate predicate offence or terrorist financing, regardless of any derogation, exemption or threshold,
* When there are doubts about the veracity or adequacy of previously obtained customer identification data or documents,
* Before acquiring a portfolio of existing customers.
* For existing customers:
  + through a periodical risk-based review process based on formal cycles;
  + when there is a significant trigger event for example:
  + A transaction of significance takes place;
  + Increase in risk rating;
  + The nature, scope and/or jurisdiction of the business activities of the customer are changing;
  + Change in regulation which requires additional information or documents to be collected.

Customer due diligence measures is carried out in the following cases:

When establishing a business relationship (i.e.: at the time of the subscription / at the time of the signature of a distribution agreement, etc.) and before the establishment of a business relationship or the carrying-out of the transaction or an investment;

When there is a suspicion of ML/TF, regardless of any derogation, exemption or threshold;

When there are doubts about the veracity or adequacy of previously obtained customer identification data;

The customer due diligence process applies to all customers and business relationships and includes, amongst others:

* Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source including, where available, electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, hereinafter referred to as Regulation (EU) No 910/2014, or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities;
* Identifying the people purporting to act on behalf of the customer (proxies, signatories, etc.) and verifying their identities on the basis of documents, data or information obtained from a reliable and independent source as well as knowing the power of representation of the person acting on behalf of the customer;
* Identifying the beneficial owner and taking reasonable measures to verify his identity using relevant information or data obtained from a reliable and independent source, in order to be satisfied that the IFM knows who the beneficial owner is;
* The relevant companies or trust beneficial owner register is consulted when entering into a business relationship with a corporate or other legal entity, or a fiducie, trust or a legal arrangement having a structure or functions similar to trusts which are subject to the registration of beneficial ownership information pursuant to Article 30 or 31 of Directive (EU) 2015/849 and obtain the proof of registration of the beneficial owner(s) or an excerpt of the register in the relevant central registers of ultimate beneficial owners and keeps records of the verification measures undertaken as well as difficulties encountered, if any. It may not exclusively rely on beneficial ownership information contained in the central register to fulfil its customer due diligence obligations. These central registers provide a useful basis of information, which in combination with other verification means, ensures the accuracy and adequacy of the beneficial ownership information (cross-checking);

In the case of customer which are legal entities, it:

1. understands the nature of the customer’s business and its ownership and control structure;
2. verifies the name, legal form and actual existence of the legal person or legal arrangement, notably by obtaining proof of incorporation or similar proof of establishment or actual existence;
3. obtains information concerning the name of the customer, the names of the administrators of *fiducies*, the legal form, the address of the head office and, if different, a principal place of business, the names of the relevant persons having a senior management position in the legal person or legal arrangement, as well as the provisions regulating the power to bind the legal person or legal arrangement;

In the case of beneficiaries of fiducies, trusts or of similar legal arrangements that are designated by particular characteristics or class, it obtains sufficient information concerning the beneficiary to be satisfied that he will be able to establish the identity of the beneficiary at the time of the pay-out or at the time of the exercise by the beneficiary of its vested rights.

* Assessing and understanding the purpose and intended nature of the business relationship and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
* Conducting ongoing due diligence of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information collected under the customer due diligence process is kept up-to-date and relevant including a review of existing records, particularly for higher-risk categories of customers;
* Establishing the source of funds and/or source of wealth, where applicable (on a risk-based approach or when compulsory by Law), of the customer;
* Obtaining a declaration as to whether the customer acts on his own account or on behalf of underlying customers/third parties. If the customer acts on behalf of a third party(ies) or where there exist elements of the transaction, or surrounding circumstances, or reasonable grounds that indicate that the customer is acting on behalf of another person, appropriate inquiries are made to determine if that person falls within the definition of beneficial owner pursuant to the AML/CTF law. Where the beneficial owner is a different person, said individual must be identified and reasonable measures must be taken to verify his/her identity;
* Performing risk assessment of the customer, to determine the level and type of due diligence required and support the decision whether to enter into, continue or terminate the business relationship. When assessing the ML/TF risks relating to types of customers, countries and geographical areas and particular products, services, transactions or delivery channels, it takes into account the risk variables relating to those risk categories set out in Annex II, III and IV of the AML/CTF Law.
* Carrying out name screening on the customer, beneficial owner and proxies and other relevant associated parties as required. The name screening is performed against PEP, TFS/PF lists and also adverse media before the onboarding or establishment of the business relationship or performing the investment and on a daily basis;
* Performing transaction, payments, changes in static data (such as address changes, bank mandates and pledges) monitoring in order to detect suspicious or unusual behaviour.
* Determining whether the client is reportable for FATCA/CRS purposes and is AML tax compliant. Please refer to the AML Tax Compliance policy and procedures as well as to the FATCA/CRS policy and procedures for further details.

If the IFM is unable to comply with the above-mentioned due diligence requirements, it may not carry out a transaction or establish a business relationship, must terminate the business relationship and consider making a suspicious transaction or activity report to the Financial Intelligence Unit (the “FIU”).

The 1st LoD:

* Adopts risk management procedures with respect to the conditions of the AML/CTF Law under which a customer will be able to benefit from the business relationship before the verification of the identity,
* Applies the customer due diligence procedures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis, by taking into account the existence of previous customer due diligence procedures and the moment when they are implemented, or when the relevant circumstances of a customer change, or when they have any legal duty in the course of the relevant calendar year to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owner(s), or if they have this duty under the Law of 18 December 2015 on the Common Reporting Standard (CRS), as amended,
* Does not enter into a business relationship with a shell bank or with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank,
* Pays special attention to any ML/TF threat that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for ML/TF purposes.

Where employees are aware that the customer has failed to complete the due diligence process they must inform the RC and the Senior Management of the IFM including the RR.

### Identification and verification of the Client

Identification

Employees of the 1st LoD must ensure that they obtain or have performed suitable due diligence that meets the requirements of this Manual for all:

• Investors;

• Any person purporting to act on behalf of the customer;

• The beneficial owner of the customer;

• Any person on behalf of whom the customer is acting.

The list of the minimum information to be obtained and recorded for natural and legal persons before entering into business relations are:

* For Natural persons:
* Surname and first name;
* Place and date of birth;
* Nationality;
* Full address of the main place of residence;
* Where applicable, official national identification
* Occupation
* Purpose of the transaction
* Source of income/revenue
* Intended transaction type
* For Legal persons:
  + Denomination;
  + Legal form;
  + Address of the registered office and, if different, of the principal place of business;
  + Articles of association;
  + Where appropriate, official national identification number;
  + Name of directors (dirigeants) and directors (administrateurs) or persons exercising similar positions (for the legal arrangements) and copy of the identification documents;
  + Provisions governing the power to bind the legal person or arrangement;
  + Authorisation to enter into a relationship and investment experience.
  + Purpose of investment & transaction
  + UBO.
* For legal arrangements:

A trust or similar legal arrangements must be identified by the identification of the settlor(s), fiduciaire(s) or trustee(s), the protector(s) (if any) and the beneficiaries (if known) with no threshold or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates and any other natural person exercising ultimate control over the fiducie or the trust by means of direct or indirect ownership or by other means. In case such above listed persons are a legal entity, the Beneficial Owner of such legal entity must be also identified. A trust deed or equivalent document is requested in order to gather the name of the settlor, trustee, protector (if any), and beneficiairies.

The identification and verification is carried out based on at least an official identification document, which is valid, issued by a public authority and containing the signature and a photograph of the investor, such as an investor's passport, identity card or residence permit.

Verification of the identity

* For physical persons:
  + One valid authentic official identification document issued by a public authority which bears the legible signature and picture of the client.
  + Examples of a valid official identification document are, among others, a passport, ID card, residence permit and, if applicable, a driving licence for countries that do not have ID cards

Depending on its risk assessment, the 1st LoD will also apply additional verification measures, such as:

* + Verifying the address indicated by the client by way of proof of address (utility bill, residence certificate),
  + Contacting the client/BO by registered letter with acknowledgement of receipt,
  + Visiting the home of the client/BO within the first months of entering into a relationship,
  + Letter of introduction,
  + Recent bank statement established in the name of the client.
* For legal persons / legal arrangements:
  + The most recent coordinated or up-to-date articles of association (or an equivalent incorporation document),
  + A recent extract from the companies/trade register (≤ three months) or equivalent supporting document,
  + A share register,
  + A BO declaration form / BO statement document,
  + An extract of the RBE (when available).

Depending on the risk assessment, the 1st LoD shall take additional verification measures, such as, for example:

* + Examination of the latest annual report available (management rapport and annual accounts), preferably certified by the approved statutory auditor (réviseur d’entreprise agréé),
  + Verification, after consulting the relevant registers, or any other reliable sources, that the company was not or is not subject to a dissolution, deregistration, bankruptcy or liquidation,
  + Verification of the information collected from independent and reliable sources, such as from public and private databases or with the specialised research firms,
  + Visit to the company concerned or send a registered letter with acknowledgement of receipt.

The verification of these data are made, notably, using information obtained from customers, public registers or any other independent and reliable source available. The 1st LoD takes all reasonable measures to ensure that the real identity of the client, proxies/people purporting to act on behalf of the client and beneficial owner are known. The reasonable nature of these measures are defined, notably, according to the level of ML/TF risks that the IFM considers to be linked to the customer profile or the nature of the business relationship or of the transactions envisaged by the client/BO.

### Identification and verification of the identity of the beneficial owner(s)

Please refer to the Glossary of this AML/CTF Manual for the definition of beneficial owner.

Enquiry whether acting for its own behalf or on behalf of a third party

At the time of the customer identification and for the purpose of the obligations to identify and verify the identity of the beneficial owner, the 1st LoD determines firstly if the customer acts for its own account or on behalf of third party (it is mandatory both for natural and legal persons and must be documented in writing).

Clients shall sign a clear statement (“UBO declaration form”) to this effect and must also undertake to inform the 1st LoD immediately/without delay in writing of any subsequent changes.

If the client acts on behalf of a third party, this “third party” is identified and its identity verified in line with this procedure.

The “UBO declaration form” is included in the client KYC file.

Identification of the beneficial owner

In all the cases, the identification of beneficial owner(s) concerns:

* Surname(s) and first name(s) (including middle name(s) if necessary)
* Date and place of birth
* Nationality(ies)
* Full postal address of the main residence
* Where appropriate, the official national identification number, personal TIN if available
* Information on his/her source of funds and source of wealth.

The verification of these data is made by using information obtained from customers, public registers or any other independent and reliable source available.

The 1st LoD requires to obtain the same level of identification document as for a client => one valid authentic official identification document issued by a public authority which bears the legible signature and picture of the client/BO.

Examples of a valid official identification document are, among others, a passport, ID card, residence permit and, if applicable, a driving licence for countries that do not have ID cards

The IFM takes all reasonable measures to ensure that the real identity of the beneficial owner is known. The reasonable nature of these measures is performed in accordance to the level of ML/TF risks that the IFM considers to be linked to the customer profile or the nature of the business relationship or of the transaction contemplated by the customer. Depending on its risk assessment, IFM will also apply additional verification measures, such as:

* Verifying the address indicated by the client/BO by way of proof of address (utility bill, residence certificate),
* Contacting the client/BO by registered letter with acknowledgement of receipt,
* Visiting the home of the client/BO within the first months of entering into a relationship
* Letter of introduction,
* Recent bank statement of a bank established in an equivalent country and with a bank account in the name of the BO.

These identification and verification have also to be applied, if after the application of the cascading measures, no BO could have been determined and the Senior Manager (dirigeant principal) has to be reported as BO.

The threefold procedure is applied to determine ultimate beneficial ownership:

Identify the natural person(s) who directly or indirectly holds or controls a sufficient percentage, namely 25% plus one, of the shares, voting rights or ownership in an entity,

Identify any person who controls the legal entity via other means (concept of “control through other means” can be assessed based, for instance, on the criteria mentioned in the articles 1711-1 to 1711-3 of the law of 10 August 1915 on commercial activities regarding among others the conditions for the preparation of consolidated accounts: such as the power to exercise a dominant influence by way of an article of a contract or the articles of association; the power to appoint or remove a majority of the management body, etc.),

If after having exhausted all possible means and provided that there are no grounds for suspicion, where no person under points 1 and 2 is identified, or if there is any doubt that the person(s) identified is/are the beneficial owner(s), identify any person who holds the position of senior managing official (dirigeant principal).

Assessments under 1 and 2 have each to be fully completed and formalized before resorting to measure 3 which constitutes an express fallback option only applicable when all possible measures to identify the beneficial owners under 1 and 2 have been exhausted and came to no result.

The persons to be identified as beneficial owners have always to be natural persons.

Where applicable, source of wealth is documented through corroborating documents (for instance: for PEP, high risk clients or high-risk countries, etc.).

Legal entities and legal arrangements

In respect of legal entities and legal arrangements, the obligation to identify the beneficial owner requires taking reasonable measures in order to:

* Understand the ownership and control structure of the client

Determine who are the natural persons that ultimately own or control the client, including those persons who exercise ultimate effective control over a legal person or arrangement or control through any other means. Some customer’s structure can be made of several layers of shareholding companies. In such case, the full shareholding structure must be obtained to identify and verify the identity of the beneficial owner. Each level in the ownership structure (from the customer to the beneficial owner(s) should be identified and verified as follow:

* In addition to a full group structure/chart duly dated and signed (and including the % of ownership), the minimum documents to be requested to the shareholding companies (if any) are:

1. The most recent coordinated or up-to-date articles of association (or an equivalent incorporation document)
2. A recent extract from the companies/trade register (≤ three months) or equivalent supporting document.
3. Certified copy of the share register or equivalent.

In the case of corporate entities, is considered as Beneficial Owner:

* Any natural person who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights or ownership interest in that legal entity, including through bearer shareholdings, or through control by other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of more than 25% shall be deemed sufficient to meet this criterion,
* If after having exhausted all possible means (and provided there are no ground for suspicion), no person under above point is identified, or if there is any any natural person who hold the position of senior managing official (“dirigeant principal”),
* It is noted that control through other means may be determined in accordance with Articles 1711-1 to 1711-3 of the Law of 10 August 1915 on commercial companies, as amended, as well as in accordance with the following criteria:

1. the direct or indirect right to exercise a dominant influence over a customer, on the basis of a contract entered into with that customer or of a clause of the articles of association of that customer, where the law governing that customer allows being subject to such contracts or such statutory clauses;
2. the fact that a majority of the members of the administrative, management or supervisory bodies of the customer, in office during the financial year as well as the preceding financial year and until the preparation of the consolidated financial statements, were appointed through direct or indirect exercise of the voting rights of one natura person;
3. the direct or indirect power to exercise or the actual direct or indirect exercise of a dominant influence or control over the customer, including the fact that the customer is placed under a single management with another undertaking;
4. an obligation, under the national law to which the parent undertaking of the customer is subject, to prepare consolidated financial statements and a consolidated management report.

In the case of trusts, is considered as Beneficial Owner, all the following persons:

* the Settlor(s);
* the fiduciaire(s) or Trustee(s);
* the Protector(s), if any;
* Any natural person who is a beneficiary (no threshold); or,where the individuals that benefit from the trust have yet to be determined, the class of persons in whose main interest the legal arrangementor entity is set up or operates;
* Any other natural person exercising ultimate control over the fiducie or the trust by means of direct or indirect ownership or by other means

In case such above listed person are a legal entity, the beneficial owner of such legal entity must be also identified and verified as illustrated in the CSSF Circular 19/732.

Where the IFM is not able to identify the beneficiary of a trust, fiducie or silimar legal arrangement and where the beneficiary is designated by characteristics or by class, the IFM shall obtain sufficient information concerning the beneficiary to ensure that it will be able to establish its identity at the time of the payout or at the time of the exercise by the beneficiary of its vested rights.

The above information may be found in the trust deed or equivalent document.

The IFM always takes reasonable measures to understand the ownership and control structure of the customer. Where natural persons are not exclusively and/or directly involved in the ownership structure of the customer, it looks through several layers of legal entities to determine whether a natural person owns finally more than 25 percent of shares or voting rights or ownership interests of the legal person and collect proof of registration or an excerpt of the register, compares its information with that of the registers in order to detect either the existence of any erroneous data or the absence of all or part of the data, or the failure to register, modify or delete them. They proceed in a similar manner in the framework of ongoing due diligence of the business relationship.

The threshold of ‘more than 25 percent’ is only indicative entailing that the sole application of this threshold might in certain cases not suffice to identify the correct beneficial owners. Also, where a shareholder holding more than 25 percent has been identified, other beneficial owners might still be present and would need to be identified.

The extend of the specific measures taken to understand the ownership structure and identify the beneficial owners are determined depending on the complexity and the different legal forms and structures to achieve appropriate levels of knowledge and transparency related to beneficial ownership information.

Once the beneficial owner has been identified, the IFM takes reasonable measures to verify the identity of the beneficial owner and to be satisfied that they know who the beneficial owner is and that they understand the structure and ownership of the customer.

Where, despite these measures, they are a doubt as to the real identity of the beneficial owner, and, where this doubt cannot be removed, they refuse to enter into a business relationship or carry out the transaction contemplated by the customer and, “where they know, suspect or have reasonable grounds to suspect that money laundering, an associated predicate offence or terrorist financing is being or has been committed or attempted,” they make a report to the FIU.

The different measures of identification and verification including the list of information and KYC documents to be requested, on a risk-based approach and depending on the AML/CTF client risk scoring attributed to the customer, are an integral part of the KYC checklists.

Where Enhanced Customer Due Diligence is applicable, eventual additional measures to verify the identity of the beneficial owner must be performed.

The IFM does not rely exclusively on the “Registre des bénéficiaires Effectifs “ (“RBE”) to fulfil its customer due diligence requirements and therefore the IFM shall fulfil those requirements by using a risk-based approach.

The customers must sign an explicit declaration and commit to communicate any subsequent changes “of the beneficial ownership” without delay.

Please refer to the operational procedures of the 1st LoD for further details on the operational application.

### Timing of the identification and verification of the identity

Entering into a business relationship before completing the measures for the verification of the identity

If the verification of the identity of the customer, people purporting to act on behalf of the client, and the BO have to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little ML/TF risks occurring, it is to be noted that these procedures shall be completed as soon as practicable after the initial contact.

Such case must be escalated to the RR for prior approval and each of the below conditions must be fulfilled and documented in writing (with a copy added to the client KYC file):

* The ML/TF risk is low and efficiently managed,
* The verification of the identity is carried out at the earliest opportunity after the first contact with the customer. The impossibility to verify the identity of the persons concerned within the timeframe of 2 weeks (10 open days) must be explained in an internal report which will be transmitted to the RR,
* Sufficient measures shall be put in place so that no exit of assets or transactions can be carried out before.

Entity in the process of incorporation

IFM may proceed with the incorporation of a company under the following conditions:

* The founders have been identified and their identities have been verified in accordance with the applicable AML/CTF legal and regulatory requirements and IFM policies and procedures.
* The founders have signed a declaration stating that they act either on their own account or on behalf of BO which they name. In the latter case, measures must be taken to identify and verify the identities of the BO.
* At the earliest opportunity after the incorporation of the company, the company in question must be identified and its identity verified through the information and documents in accordance with the applicable AML/CTF legal requirements and IFM policies and procedures. In such cases, IFM imposes a deadline of 15 days from the date of incorporation of the company for the completion of the identification and verification measures as described above.

In the event that it is not possible to verify the identity of the persons concerned within the 15-day timeframe, a written report must be sent to the RC and RR explaining the reasons for the delay and the problems encountered, with, in addition, the proposed measures to perform the identification and verification of the identity. A copy of this written report must be added to the client KYC file.

As long as the identity of the persons concerned have not been verified, the IFM will not perform any transactions on behalf of the client.

### People purporting to act on behalf of and for the client (proxies, PoA, signatories, etc.)

The identification and verification measures of the identity of the people purporting to act on behalf of the client are subject to the same provisions mentioned above (identification and verification of the client identity).

It is compulsory to know and document the power of representation of the person acting on behalf of the customer and to verify his identity through evidencing documents of which copies are kept. The powers granted to that person must be evidenced and documented in the client KYC file.

The authority to deal, etc. with assets under a power of attorney constitutes a business relationship. Consequently, the identity of the holder of the power of attorney, as well as the principles they represent, are identified and verified.

The signature(s) present in each onboarding documents (including but not limited to the client questionnaire – description of the purpose of the business relationship and the Compliance questionnaire – KYC and declaration of tax compliance) is/are compared to the list of authorised signatories or equivalent document (or the ID card/passport for an individual person) provided by the client to ensure that both specimens are matching.

A proxy that is a legal person (e.g. a Corporate Director, etc.) is subject to the same requirements as the ones applying to a legal entity as mentioned above; it shall be further clarified that the individuals authorised to act on behalf of the customer under the mandate granted to the proxy must be identified and its identity verified in the same way as a natural person customer.

Please refer to the dedicated procedures of the 1st LoD for further details on the operational application.

### Obtaining information on the purpose and intended nature of the business relationship

The IFM’s obligation to know its customer includes the obligation to gather and register, at the time of the customer identification, information about the origin of the customer's funds and the types of transaction for which the customer requests a business relationship, as well as any adequate information allowing the determination of the customer’s purpose of the business relationship/intended nature of the business relationship.

The IFM collects and documents, when identifying the client/BO:

1. Information on the estimated wealth/net-worth,
2. Information on the origin of assets/wealth and the origin of the funds,
3. The types of transactions for which the client/BO requests a business relationship,
4. The purpose of the business relationship sought,
5. The intended nature of the business relationship.

The IFM verifies if the intended purpose of the business is in line with the defined risk appetite of the Company and if the client/UBO and the structure (if any) are AML tax compliant.

On a risk-based approach, the IFM may request corroborating documents.

All the above information/documents allow the IFM to carry out efficient ongoing due diligence in respect of the client/BO throughout the business relationship and to detect, where applicable, transactions that are unusual or not in line with the initial profile established for the relevant client/BO.

Origin/source of the funds and origin/source of wealth: special considerations

Source of the funds consists in the economic origin of the monies invested in the considered business relationship and comprises both the activity that generated the funds used in the business relationship as well as the means through which the customer’s funds were transferred (geographical origin).

Source of wealth means the origin of the estimated customer’s total wealth. It is important to assess and document, during the business relationship, the evolution of the customer wealth.

Gathering information about the origin of the customer’s funds is part of the IFM obligation to know its customers and understand the purpose and intended nature of the business relationship and shall allow IFM to carry out an efficient ongoing customer due diligence.

It is of paramount importance to assess if the origin of the funds as declared by the client is sufficiently explicit, understandable, credible and consistent with the knowledge of the client and its profile (and, as appropriate the BO), and/or the nature and purpose of the relationship, and if the monies invested do not originate from a criminal activity, including aggravated tax fraud and tax swindling.

Please refer to the procedures of the 1st LoD for further details on the operational application.

### Due Diligence – risk scoring and level of due diligence

The risk-based approach results in classification of customer by level of risks. The risk scoring (low, medium or high) leads to different levels of due diligence measures to be applied to different approval process and also drives, among others, the ongoing monitoring to be performed during the business relationship including the frequency of the ongoing due diligence, the transaction monitoring, etc.

The procedural framework of the 1st LoD which applies this Manual provides details on:

* Normal/standard, simplified and enhanced due diligence,
* Documents required for verifying the identity of the customer (investor/intermediary, etc.) and relevant related parties.

The Risk Rating is carried out:

* When new customer is on-boarded before acceptance; and
* Regularly for existing relationships (ongoing due diligence), taking into account the risk factors at that time.

This Risk Rating is not fixed and might evolve over time. During the business relationship, any significant change in the customer (or relevant associated parties)’s situation implies a new assessment of the customer risk rating. A re-assessment of the customer risk rating is carried out at the latest when the business relationship is being reviewed in the context of the periodical KYC review (ongoing due diligence including review of the customer profile, information and documents on file, etc.) that is performed on a regular basis.

Whereas certain types of customer's are considered as risky by law, the high risk classification for others is based on a combination of risk factors as determined according to and linked to the IFM’s business but also inherent to the following categories of risk:

* Customer categories/types,
* Countries or geographical areas,
* Products, services, transactions (or distribution channels) and marketing methods
* (distribution),
* The intended purpose and nature of an account or business relationship,
* The level of assets to be deposited by a cusotmer or the volume of transactions expected or made,
* The regularity or duration of the business relationship,
* The source of funds,
* Other indicators that may give rise to indicators of a tax offence.

The on-boarding of new investors who are risk assessed as “high” is subject to the following escalation process:

* Prior validation of KYC documentation from the 1 LoD,
* Approval of the customer by the Acceptance Committee,
* Review from the RC and approval provided by the RR of the IFM,
* Approval from the Board.

The IFM does not open anonymous or numbered accounts.

The onboarding and ongoing due diligence performed on customers is performed by the 1st LoD. Compliance during its oversight ensures that the above principles have been applied and respected by performing sample-testing and by received dedicated KPI’s/KRI’s that are sent afterwards to the RC and RR.

Following customer's risk classification, the IFM ensures that appropriate due diligence is in place (e.g. simplified, standard or enhanced due diligence).

### Simplified Due Diligence (“SDD”)

Where the IFM identifies a lower ML/TF risk, it may apply SDD measures in accordance with Article 3-1 of the AML/CTF Law as amended.

Before applying SDD measures, it ascertains that the business relationship or the transaction presents a lower degree of ML/TF risk.

When assessing the ML/TF risks relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels, the 1st LoD takes into account at least the factors of potentially lower risk situations set out in the Appendix III of the AML/CTF Law.

The 1st LoD carries out sufficient monitoring of the transactions and business relationship to enable the detection of unusual or suspicious activities or transactions and gathers sufficient information in every circumstance to determine whether the customer satisfies all of the conditions required to apply the SDD measures. The criteria used to apply SDD measures on a customer must be reviewed and documented by the 1st LoD annually.

If there is information available which suggests that the degree of risk is not low, when there is a suspicion of ML/TF or when there is a doubt about the veracity or adequacy of previously obtained data, or in specific cases of higher risks, the application of the regime of SDD is not possible for these customers, geographical areas, particular products, transactions or delivery channels.

Although a simplified due diligence is applied, the following verifications are still applicable:

* Identification and verification of the identity of the customer/business relationship(s),
* Identification of the UBO(s),
* Obtaining information about purpose and intended nature of the business relationship,
* Conducting ongoing monitoring, to ensure transactions are consistent with customer’s business, risk profile and identify the source of the funds.

Please refer to the operational procedures of the 1st LoD for further details on the SDD measures applied.

### Enhanced due diligence (“EDD”)

The IFM applies on a risk-sensitive basis, EDD measures, in addition to the measures referred to normal customer due diligence measures, in situations which by their nature can present a higher ML/TF risk, and at least in the cases described below, to manage and mitigate those risks appropriately.

When assessing the ML/TF risks, it takes into account the factors of potentially higher-risk situations set out in the Annex IV of the AML/CTF law.

The AML/CTF legislation foresees cases where EDD measures must be applied:

1. Non face to face business relationship

It takes the following measures when the customer is not physically present or has not been met:

* 1. Ensure that the identity of the customer is established by means of additional documents, data or identifying information,
  2. Ensure the verification or certification by a public authority of the documents provided,
  3. Obtain a confirmation certificate from a credit institution or a financial institution subject to the Law or subject to equivalent professional obligations in AML/CTF,
  4. Ensure that the first payment for transactions is made by means of an account opened in the name of the customer with a credit institution or a financial institution subject to the Law or subject to equivalent professional obligations in terms of AML/CTF.

1. When dealing, having business relationships or performing transactions with or involving high risk countries

With respect to business relationships or transactions involving High-Risk Countries, it applies the following EDD measures:

1. Obtain additional information on the customer and on the beneficial owner(s) and updating more regularly the identification data of the customer and beneficial owner,
2. Obtain additional information on the intended nature of the business relationship,
3. Obtain information on the source of funds and source of wealth of the customer and of the beneficial owner(s),
4. Obtain information on the reasons/rationale for the intended or performed transactions,
5. Seek for the approval of the IFM’s RR for establishing or continuing the business relationship,
6. Conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

It ensures, where applicable, that the first payment is carried out through an account in the customer’s name with a credit institution subject to customer due diligence standards that are not less robust than those laid down in Directive (EU) 2015/849.

In addition to the measures provided above and in compliance with the European Union’s international obligations, it applies, where applicable, one or more additional countermeasures to persons and legal entities carrying out transactions involving High-Risk Countries. Those measures consist of one or more of the following:

1. The application of additional elements of EDD,
2. The introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions,
3. The limitation of business relationships or transactions with natural persons or legal entities from High-Risk Countries.
4. In the case of cross-border correspondent relationships or other similar relationships with respondent institutions

In addition to the normal customer due diligence measures, it:

1. Gathers sufficient information about a respondent institution (including the country of establishment of the institution, its ownership structure chart, etc.) to understand fully the nature of the respondent's business, including the supervisory authority and regime applicable to the institution and document in writing the decision resulting from the analysis,
2. Determines from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a ML or TF investigation or regulatory action (analysis must be documented in writing),
3. Assesses the respondent institution's AML/CTF controls,
4. Seeks for the written approval of IFM’s RR before establishing new correspondent relationships or similar relationships,
5. Clearly understands and document in writing the respective responsibilities as regards AML/CTF of each institution,
6. Is satisfied that the respondent institution has verified the identity of and performed ongoing due diligence (in accordance with the applicable AML/CTF legal requirements) on the customers having direct access to accounts of the credit institutions, financial institutions and other institutions concerned by such relationships and that it is able to provide relevant customer due diligence data and information to the correspondent institution, upon request,
7. The analysis of the information obtained and the resulting decision will be shared with the competent authorities upon request.

There is no derogation from the application of EDD in the cases set forth in the AML/CTF Law or the Grand Ducal Regulation.

The application of EDD measures is performed to all correspondent relationships, irrespective of the country in which the respondent is situated / located / domiciled / registered.

The provision under the article 3 paragraphs 1 and 2 of the CSSF Regulation 12/02 as amended further extends the obligation to apply EDD measures on intermediaries acting on behalf of one or more third parties:

*“Where the units or shares of an undertaking for collective investment or an investment IFMin risk capital are subscribed through an intermediary acting on behalf of “others”, the undertaking for collective investment, its management company, the investment IFMin risk capital or, where applicable, the respective proxy of the professionals shall put in place enhanced customer due diligence measures for this intermediary which are applied mutatis mutandis pursuant to the terms of Article 3-2(3) of the Law, Article 3(3) of the Grand-ducal Regulation and Article 28 of this regulation in order to ensure that all the obligations under the Law, the Grand-ducal Regulation and this regulation or at least equivalent obligations are complied with.*

*The due diligence measures which apply to the relationship with the intermediary shall be at two levels:*

* + 1. *the intermediary, the persons purporting to act on its behalf and its beneficial owners shall be identified and their identity verified, where applicable, according to a risk-based approach*
    2. *enhanced due diligence measures shall be implemented for the business relationship qualified as similar to correspondent relationship with the intermediary which invests on behalf of others. These enhanced due diligence measures, referred to in the above paragraph 1, aim notably to analyse the robustness of the AML/CFT control framework of this intermediary*.”

Diagram

Description automatically generated

1. With regard to transactions or business relationships with politically exposed persons (“PEP”)

In addition of the normal customer due diligence measures, it:

1. Has appropriate risk management systems, including risk-based procedures to determine if the customer, people purporting to act on behalf of the customer or beneficial owner is a PEP,
2. Seeks for the approval of the IFM’s RR for establishing or continuing, for existing customers, business relationships with such persons,
3. Takes reasonable measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction with such persons,
4. Conducts enhanced ongoing monitoring of the business relationship.

It also applies where a customer has already been accepted and the customer or the beneficial owner is subsequently found to be, or subsequently becomes, a PEP.

With regards to transactions or business relationships with PEPs, the 1st LoD determines if the investor, the people purporting to act on behalf of the customer/investor or beneficial owner is a PEP.

To this end, the 1st LoD:

* + - Screens name of investors, people purporting to act on behalf of the customer, legal representatives and BO with its name screening tool,
    - Performs open-source intelligence if needed/ uses publicly available information,
    - Solicits relevant information from the investor.

Where a natural person who is or has been entrusted with prominent public functions is no longer entrusted with a prominent public function by a European Member State or a third country, or with a prominent public function by an international organisation, it, for at least 12 months, takes into account the continuing risk posed by that PEP and applies appropriate and risk sensitive measures until that person no longer poses particular risks. The measures must be documented in writing.

1. Products or transactions that might favour anonymity

It pays special attention to any ML/TF threat that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for ML/TF purposes.

For instance, it applies EDD in case of foreign companies with capital in the form of bearer shares that would not be subject to disclosure regulations (as the one in Luxembourg) in their country. It adopts procedures to establish the identities of the holders and beneficial owners of such shares and ensure that they are notified without delay whenever a change of holder and/or beneficial owner occurs.

Please refer to the operational procedures of the 1st LoD for further details on the EDD measures to be applied.

### Refusal and exiting a business relationship

The decision to refuse to enter into business relationship with the client must be explained and taken by the Acceptance Committee (which may be for purely commercial reasons, compliance reasons or a combination of the two) in writing and it will be inserted in the KYC files of the prospective client. A copy of this document must be sent to the RC and RR for information.

Should the refusal to enter into business relationship be explained by suspicions or doubts of ML/TL, the case must be escalated immediately to the RR and to the RC.

IFM’s risk appetite enumerates the cases for which a new business relationship has to be refused.

The IFM keeps a trace in writing of every contact with a prospect, even if this contact does not materialize in an effective business relationship, whatever the reason and independently of the way the contact was established.

Any decision to exit a business relationship (which may be for purely commercial reasons, compliance reasons or a combination of the two) shall be documented in writing and kept on file and consideration must be given as to whether a communication to the appropriate authorities is required.

The determination by the RC/RR that the IFM was misled as to the identity of a client/people purporting to act on behalf of the customer, BO should especially be considered as a ground for exiting a business relationship.

The decision to exit a business relationship is always taken by the Acceptance Committee.

Should the decision to exit a business relationship be explained by doubts or suspicions or reasonable grounds for suspicion of money laundering, associated predicate offence or terrorist financing, the RR/RC must file immediately a STR/SAR to the authorities.

In order to be exited, the client KYC file (information, data and documents) must be in good order and up-to-date.

### Performance of customer due diligence by third parties

The IFM does not apply the third party introducer regime.

### Tax considerations – AML Tax Compliance

The tax predicate offence is included in the law of 23 December 2016 regarding the 2017 tax reform and the CSSF Circular 17/650 as amended by the CSSF circular 20/744.

When establishing a new investor account, processing a transaction for an existing investor, and on an ongoing basis, the 1st LoD has a process in place whereby it assesses, whether the investor is AML tax compliant.

The CSSF Circular 17/650 provides for a list of 21 indicators which should be taken into consideration when assessing the tax compliance of an investor.

The CSSF Circular 20/744 which amended the CSSF Circular 17/650 to further includes fund industry specific indicators.

An assessment of these indicators as well as the potential impact have been performed by the 1st LoD.

Please refer to the AML tax compliance policy and procedures of the 1st LoD for further details.

### Record keeping and data protection

The 1st LoD ensures that the documents, data and information are retained for a period of five years for the purposes of preventing, detecting and investigating, by the Luxembourg authorities, possible ML/TF offences.

The record-keeping obligation of documents, data and information covers all documents, data and information obtained under the customer due diligence measures, including the results of any performed analysis:

* in the case of due diligence on the investor, distributor, business relationships, etc. a copy of or references to the documents, data and information which are necessary to comply with the customer due diligence requirements laid down in the AML/CTF Law, including, where available, data obtained through electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities, account files, business correspondence, as well as the results of any analysis undertaken, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction,
* the supporting evidence and records of transactions which are necessary to identify or reconstruct individual transactions in order to provide, where necessary, evidence in the framework of an investigation or criminal proceedings, for a period of five years after the end of a business relationship with the customer or after the date of an occasional transaction.

The retention period here referred to, including the further retention period that exceeds not five additional years, also applies in respect of the data accessible through the centralised mechanisms referred to in Article 32a of Directive (EU) 2015/849.

They retain the information, data and documents concerning the measures taken to identify and verify the identity of the beneficial owners.

Without prejudice to longer retention periods prescribed by other laws, they delete the personal data at the end of the retention period.

In specific cases when necessary for the purpose of carrying out their relevant prudential supervisory duties under the AML/CTF law, the supervisory authorities may require that they retain the data for a further period which cannot exceed five years.

By way of derogation from the above paragraph, they retain the personal data for a further period of five years where this retention is necessary to effectively implement internal measures for the prevention or detection of ML/TF.

The obligation to keep certain documents, data and information relating to business relationships and transactions also includes the obligation to keep the written reports transmitted to the RC and to the RR, as well as the analyses of the transactions and facts included in these reports that the RC drew up, the decisions taken accordingly and the results of any other performed analysis.

Personal data are processed by the IFM on the basis of the AML/CTF Law as amended, only for AML/CTF purposes and are not further processed in a way that is incompatible with AML/CTF purposes. The processing of those personal data for any other purposes, such as commercial purposes, is prohibited.

The processing of personal data is subject to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter referred to as “Regulation (EU) 2016/679”).

The 1st LoD provides new investors with the information required pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 before establishing a business relationship. That information, in particular, includes a general notice concerning the legal obligations of the IFM under this law to process personal data for the purposes of the prevention of ML/TF.

The person who is responsible for the processing restricts or defers the right of access of the person concerned to his personal data where such measure is necessary and proportionate in order to:

* 1. Enable the IFM, the FIU, a supervisory authority or a self-regulatory body to fulfil their tasks properly for the purposes of the AML/CTF Law or its implementing measures; or
  2. Avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of the AML/CTF Law, its implementing measures or Directive (EU) 2015/849 and to ensure that the prevention, investigation and detection of ML/TF is not jeopardised.

For the specific provisions on the management of record-keeping, personal documents, data or information, please refer to the Data Protection policy/procedures or any other relevant policy and procedures of the IFM.

### Due Diligence on assets

The 1st LoD performs a ML/TF risk analysis per class of assets and on a risk based approach for medium and high risk class of assets on each asset.

As regards the risk assessment on the target investments, the results of the analysis will be documented in a memo which summarizes the significant findings and the risk level of the investment.

The following elements, amongst others, shall be analysed:

* The geographical risk;
* The risk profile/type of the asset;
* The results of the name screening performed on the asset/the issuer of the asset and related/linked counterparties.

The due diligence on the assets (including the name screening) is performed by the 1st LoD.

Compliance performs a regular assessment of the name screening tool (as well as its functionalities) and on the due diligence on assets performed by the 1st LoD.

It must be noted that name screening against TFS/PF lists are done on a daily basis on each asset/investment and linked counterparties.

Based on the information collected, each asset will be given a risk scoring (Low, Medium, or High). The risk scoring as well as the type of assets determine the frequency of the on-going due diligence as well as the type of due diligence to be performed (name screening only, collection of information and KYC documents, etc.). The provided risk scoring is reviewed on an annual basis. The extend of the due diligence on assets is determined on a risk based approach:

* if the ML FT risk of the asset is Low, a simplified due diligence may be performed;
* if the risk is Medium or High, an enhanced due diligence must be carried on with further verifications.

When the risk related to the targeted asset is assessed to be high, evidences should be obtained during the due diligence such as documents corroborating the existence of the asset or its good standing.

Compliance establishes appropriate due diligence controls to the asset side to avoid the IFM and Fund could be abused or misused to conceal, or even continue, illegal activities.

Reporting (KPI’s) are received by the RC and the RR and analysed on certain frequency.

Some countries are deemed to be of higher risk and therefore the investments linked to such countries, as a result of the issuers/counterparties/market localisation, will be subject to additional due diligence on an ongoing basis. Other countries will be considered of lower risk, and therefore the investments linked to those countries could be subject to fewer checks by the IFM, provided that the investments are actually assessed as presenting a lower risk.

In the context of each asset, the 1st LoD will implement the due diligence so defined and will report to the RC any issue encountered in the context thereof based on the periodicity and on the KPIs agreed. The RC will in turn report such issues and KPIs to the RR/Board.

Any ‘hit’ (on a TFS lists, PEP lists or any other lists) must be immediately escalated to the RC/RR for further decision / actions.

The documents/information requested in the context of the due diligence performed on the investments will be gathered and kept updated at the same frequency as for the AML/KYC documents/information gathered in the context of the AML/KYC due diligence on the customers.

Please refer to the 1st LoD due diligence on assets procedures for further details.

## Ongoing monitoring of the business relationship

The ongoing monitoring of the business relationship is an essential aspect of effective and sound ML/FT risk management.

The ongoing monitoring of the business relationship with the investors, the assets, distributors and business relationships is performed by the 1st LoD. The transaction filtering is performed by the Depositary/Custodian Bank.

The ongoing monitoring of the business relationship is determined, on a risk-based approach, taking into account the ML/TF risk scoring attributed to each relationship, applies to all relationships and follows different steps:

* 1. Keeping all information, data and documents up-to-date
  2. Re-assess the relevance of the initial ML/FT risk scoring of such relationship
  3. Perform a name screening on PEP, black and TFS/PF lists and on adverse medias before entering into business relationship and on an ongoing basis and document the assessment (e.g. results of name screenings potential hits and other review outputs)
  4. Perform transaction monitoring and filtering (including monitoring of change in static data, etc.). A record is retained evidencing the review.

The ongoing due diligence is a cyclical process, whereby unexpected relationship behaviour, or any other/ad-hoc events, results in requesting additional information and/or documents from or about relationship to update the KYC and customer risk profile and, if necessary, adapt the monitoring and/or take further action.

### Keeping all information and documents up-to date

Ongoing due diligence includes the obligation to verify and, where appropriate, to update, within an appropriate timeframe according to the risk assessment, the documents, data or information gathered while fulfilling the customer due diligence obligations.

The ML/FT Risk Rating drives, amongst others, the frequency of the ongoing customer due diligence.

The investors/customers/business relationships/distributors/assets files are reviewed at a minimum as follows:

* Low risk customers reviewed every 3 years,
* Medium risk customers reviewed every 2 years,
* High-risk customers reviewed annually.

Please refer to the 1st LoD’s KYC procedures for further details.

The IFM:

* Gives particular attention to the activities of customers classified as presenting a high AML/CTF risk profile,
* As the case may be, verifies at least once a year if the Simplified Due Diligence regime conditions still apply.

Additionally, an ongoing due diligence (documents, data and information verified and updated immediately) is conducted where the business becomes aware or has an indication that:

* The identity of the customer, or of a beneficial owner, has changed,
* A transaction is not reasonably consistent with the knowledge that the 1st LoD has about a customer or with the profile of the customer,
* The purpose and intended nature of the relationship with the customer has changed,
* When a situation occurs calling for these measures and, in particular, at appropriate times,
* Any other matter that might affect the ML/TF risk assessment or the ML/FT risk rating,
* Any changes in the applicable AML/CTF legislation.

During the review and update of the documents, data and information on the customers, the IFM may take into account different sources of information, among others:

* Public data and information,
* National ML/TF risk assessment report from the customer’s country,
* Mutual evaluation reports in relation to AML/CTF of the customer’s country,
* Other information obtained from reliable and independent sources.

### Name-screening

Before the entry into business relationship, whenever there is a change in static data and on an ongoing basis, the IFM screens daily, amongst others, the name of all the business relationships and their related parties including beneficial owner(s) against at least:

* Sanction lists including among others, lists issued by the United Nations, consolidated EU lists concerning prohibitions and restrictive measures in financial matters;
* PEP lists
* Adverse media lists

The 1st LoD is in charge of screening the investors (including their related parties and beneficial owners), assets/investments against PEP, TFS/PF and adverse media lists.

New Investors and investment are manually screened at the account opening stage and automatically screened going forward from the night following the creation of their account.

The 1st LoD uses DowJones as name screening tool. This tool automatically and on an ongoing basis screens investors/assets-investments and related parties daily against the various lists.

Screening hits (true and false positive or negative hits) are reviewed applying 4 eyes control principle by the 1st LoD.

Please refer to the 1st LoD ‘s procedures for further details on the software / tools used for name-screening, the exhaustive inventory of controlled lists (PEP, TFS, etc.) and their related update frequency, the escalation procedure and the validation procedure of the hits.

Databases used for name screening purposes are subject to regular updates to take into account without delay any modification of the TFS/PF Lists. Any true hit, together with all supporting documentation and information, is escalated by the 1st LoD to the RC/RR who will determine the actions to be undertaken accordingly. Such analysis and the outcome thereof are documented in writing.

Please refer to the 1st LoD procedures for further details.

### Detection of complex or unusual transactions

As part of its ongoing monitoring obligations, the 1st LoD carries out the scrutiny of investor’s transactions to determine, amongst others, whether they are consistent with profiling information about the investor, its business, risk profile and the nature and purpose of the business relationship.

The extent and depth of transaction monitoring is based on the established risk-based approach.

Defined scenarios and thresholds used for transaction monitoring are reviewed on a regular basis by the 1st LoD to determine, amongst others, their adequacy for the risk levels established, with the business model/activities of the IFM and the risk profile of the investors.

Monitoring measures are in place to flag unusual movements of funds or transactions for further analysis and scrutiny in a timely manner for determining as to whether the funds movements or transactions are suspicious. Criteria applied to decide the frequency and intensity of the monitoring of different customer segments are also readily explicable and the rationale for the monitoring strategy appropriately documented.

The 1st LoD examines, as far as reasonably possible, the background and purpose of any transaction that fulfils at least one of the following conditions:

* 1. it is a complex transaction,
  2. it is an unusually large transaction,
  3. it is conducted in an unusual pattern,
  4. it does not have an apparent economic or lawful purpose.

For instance, the IFM pays special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent economic or lawful purpose such as:

* Significant transactions relative to a business relationship,
* Transactions that exceed certain limits,
* Very high account turnover inconsistent with the size of the balance,
* Transactions which fall out of the regular pattern of the account's activity,
* The importance of inputs and outputs of assets and volume of the amounts involved,

(transactions involving small amounts but with unusually high frequency are also included),

* The existence of deviations from the nature, volume or frequency of transactions normally,

performed by the investor as part of the business relationship or the existence of relevant,

differences in relation to the nature, volume or frequency of transactions usually performed,

under comparable business relationships,

* The existence of deviations from the statements made by the investor during the acceptance procedure in relation to the purpose and nature of the business relationship, including with regard to the origin or destination of the funds involved.

Depending on the nature of the investors present in the registrar at some point in time, the above controls may not all be relevant and only some of the above will be implemented by the 1st LoD.

The Depositary Bank performs transaction filtering of the transfer of funds as required by Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015.

Please refer to the 1st LoD procedures for further details.

### Blocked account

The 1st LoD has procedures in place regarding investor blocked accounts that includes the following:

* Types of blocking;
* Items triggering the blocking of an investor account/rationale for the blocking;
* Information about the manual or automatic character of the blocking process;
* Escalation procedure regarding blocked accounts, and
* Treatment of the blocked accounts

The 1st LoD informs the investors about irregularities or missing information/documentation that might trigger a blocking of their accounts upon receipt of an order or after an unsuccessful periodical documentation review.

The 1st LoD provides compliance and the RC with a quarterly report detailing the blocked accounts in the shareholder register, their undertaken to regularize blocking date, the reasons for blocking the accounts and the measures taken or to be taken to remedy the situation.

## Obligations to cooperate with the authorities

The IFM fully cooperates with the Luxembourg authorities responsible for the fight against ML/TF.

The IFM (represented by the RR and RC) informs without delay, the FIU when they know, suspect or have reasonable grounds to suspect that ML/TF is being committed or has been committed or attempted, in particular in consideration of the person concerned, its development, the origin of the funds, the purpose, nature and procedure of the operation. This report accompanied by all supporting information and documents having prompted the report. The obligation to report suspicious activities or transactions applies regardless of whether those filing the report can determine the predicate offence.

The IFM promptly notifies the Luxembourg FIU (CRF), on its own initiative, if it knows, suspects or has reasonable grounds to suspect that a laundering of a primary tax offense is taking place, has occurred or has been attempted.

The CSSF circular 17/650 as amended by 20/744 provides some examples of the nature of the suspicion, the reporting thresholds, the affected individuals and examples of attempts of money laundering as well as a list of 21 indicators plus 9 indicators (specific for the investment fund industry) that can raise a suspicion of money laundering offense to tax crime. It is to be noted that the examples of indicators are neither exhaustive nor exclusive of other criteria.

The IFM acts according to the following steps:

* If an indicator or a combination of indicators raise a suspicion, a closer examination of the business/transaction relationship is necessary to verify whether this doubt is justified in the context of the transactions and the IFM’s knowledge of the client’s situation (KYC and KYT),
* If doubt persists, the RC/RR report the suspicion to the CRF.

It is to be noted that a single indicator, or even several indicators, are not necessarily sufficient grounds for raising a suspicion of laundering.

The RC/RR also inform the FIU in the case that it has been in contact with a person or entity, or legal entity without that a business relationship has been tied or a transaction has been completed, provided that there is evidence or suspicion of ML/TF.

In cases where the RC/RR form a suspicion that an activity or a transaction relates to ML/TF and reasonably believes that performing its due diligence process will tip-off the customer, it may choose not to pursue that process and to make a suspicious activity/transaction report to the FIU.

The analysis performed to determine if a declaration must be made to the FIU or not, are kept in writing and made available to the competent authorities.

When the RC/RR declare to the competent authority a suspicion on a business relationship or a transaction, enhanced controls/monitoring are performed following the declaration and complementary declaration are communicated in case of new elements known.

According to the CSSF Circular 11/528, the IFM is not required to systematically transmit to the CSSF the information that they communicate to the FIU, except where a suspect is a professional subject to the CSSF's supervision, or is, according to the IFM’s knowledge, a member of the personnel or internal bodies of such a professional or where this information is likely to have a more material impact on the financial sector.

Individuals, including employees and representatives of the professionals, who report suspicions of money laundering or terrorist financing internally or to the Financial Intelligence Unit, are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

Failure to report knowledge or unusual activities is a disciplinary offence, as well as a criminal offence.

Professional confidentiality does not apply with regard to the FIU and there is no liability of any kind when a declaration of good faith has been issued.

The RC will consider all internal reports and make a decision on whether to submit a report (suspicious activity or transaction report) to the FIU and/or to other appropriate authorities and escalate it to the RR where deemed appropriate. Suspicious activity or transaction reports are submitted by the RC/RR via the system goAML.

The IFM has registered his RC and his RR as the person responsible for cooperating and reporting to the authorities on the GoAML platform.

Suspicious transaction and activity reports and responses to information request is generated by GoAML.

The RC and the RR respond to all information requests from the FIU in a timely and comprehensive manner. Responses to FIU requests are processed via GoAML.

Any communications made with or received from the authorities are maintained on file.

The [Law of 19 December 2020](http://legilux.public.lu/eli/etat/leg/loi/2020/12/19/a1072/jo) concerning the implementation of restrictive measures in financial matters defines the legal framework regarding the implementation of financial sanctions.

The designation of countries, natural and legal persons, entities or groups targeted by an annex to legal act of the European Union (“EU”) or of the United Nations (“UN”) and the determination of applicable restrictive measures in financial matters are made automatically by reference to this list.

It has to be noted that the adherence to the restrictive measures is a legal obligation.

The Minister of Finance is competent to deal with questions regarding the implementation of financial restrictive measures from those targeted by these measures as well as those called upon to apply them. Any questions regarding homonyms and unintended consequences of the financial restrictive measures on assets are sent to:

* By post mail to: Ministère des Finances, 3 Rue de la Congrégation, L-1352 Luxembourg; or
* By email to [sanctions@fi.etat.lu](mailto:sanctions@fi.etat.lu)

The IFM informs the Ministry of Finance in writing at one of the above-mentioned addresses of the execution of each prohibition or restrictive measure against a designated country, person, entity or group.

During the due diligence process, the IFM apply relevant controls and identifies therefore without delay:

* the States, persons, entities or groups involved in a transaction or business relationship subject to restrictive measures in financial matters in the context of the fight against terrorist financing, including, notably, those implemented in Luxembourg via EU regulations directly applicable in national law or through the adoption, among others, of ministerial regulations; and
* the States, persons, entities or groups involved in a transaction or business relationship subject to restrictive measures in financial matters, including, notably, those implemented in Luxembourg via EU regulations directly applicable in national law or, where appropriate, through the adoption of regulatory texts implementing them at national level.

In case of true hit identified, the asset(s) are frozen and the RC/RR inform, without delay, the Ministry of Finance with copy of this communication to the CSSF at the same time.

In case of detection of persons, groups or entities responding to the characteristics above, the IFM performs the following duties:

* Implementation of the restrictive measures,
* Information communicated immediately to the competent authorities, the FIU and when relevant to the CSSF,
* Information communicated immediately to the RC/RR.

**No tipping off**

It is not authorized to disclose to the investor or to other third persons the fact that information or transaction is being or has been reported to the authorities without the express prior consent of authorities.

When an employee has reported a suspicious transaction or activity to the IFM’s RC/RR, she/he may not inform anyone. Such employee shall continue to deal with the Customer in accordance with instructions received from IFM’s RC/RR and the head of the Compliance Department.

To avoid any risk of tipping off, whether accidental or intentional, the number of persons aware of the steps taken is limited to a need-to-know basis. The IFM will not execute a transaction it suspects to be linked to ML/TF. If it is not possible to wait with the execution of the transaction or the fact to not execute a transaction may prevent the "pursuit" of the beneficiaries of the transaction, the transaction will be executed, and the authorities will be informed immediately after.

Any transaction linked to terrorist financing will not be executed and the assets are immediately blocked internally until further instruction. In this instance, the authorities are informed immediately after the assets have been blocked.

# Annex 1. Definitions and acronyms

Where applicable, definitions listed below stem from the Luxembourg AML/CTF legislation

|  |  |
| --- | --- |
| Term | Definition |
| 1st LOD | First Line of Defence – perform due diligence on investors, distributors as well on assets. |
| AML/CTF | Anti-money laundering / Counter-Terrorism Financing (Combating the Financing of Terrorism) |
| AML/CTF Law | The Law of 12 November 2004 on the fight against money laundering and terrorist financing as amended |
| AML/CTF GDR | Grand-ducal regulation of 1 February 2010 as amended providing details on certain provisions of the AML/CTF Law of 12 November 2004 on the fight against money laundering and terrorist financing as amended |
| Beneficial Owner | Any natural person(s) who ultimately owns or controls the customer or any natural person(s) on whose behalf a transaction or activity is being conducted. The concept of beneficial owner shall include at least:  (a) in the case of corporate entities:  (i) any natural person who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a IFMlisted on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.  A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership;  (ii) if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), any natural person who holds the position of senior managing official.  “Control through other means may be determined in accordance with Articles 1711-1 to 1711-3 of the Law of 10 August 1915 on commercial companies, as amended, as well as in accordance with the following criteria:  (aa) the direct or indirect right to exercise a dominant influence over a customer, on the basis of a contract entered into with that customer or of a clause of the articles of association of that customer, where the law governing that customer allows being subject to such contracts or such statutory clauses;  (bb) the fact that a majority of the members of the administrative, management or supervisory bodies of the customer, in office during the financial year as well as the preceding financial year and until the preparation of the consolidated financial statements, were appointed through direct or indirect exercise of the voting rights of one natural person;  (cc) the direct or indirect power to exercise or the actual direct or indirect exercise of a dominant influence or control over the customer, including the fact that the customer is placed under a single management with another undertaking;  (dd) an obligation, under the national law to which the parent undertaking of the customer is subject, to prepare consolidated financial statements and a consolidated management report;”  (b) in the case of fiducies and trusts “, all following persons”:  (i) the “settlor(s)”;  (ii) “the fiduciaire(s) or trustee(s)”;  (iii) the “protector(s)”, if any;  (iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;  (v) any other natural person exercising ultimate control over the fiducie or trust by means of direct or indirect ownership or by other means;  (c) in the case of legal entities such as foundations, and legal arrangements similar to trusts, any natural person holding equivalent or similar positions to those referred to in point (b). |
| Board | The Board of Directors of the IFM |
| Business relationship | Professional or commercial relationship which is connected with the professional activities of the IFM and which is expected, at the time when the contact is established, to have an element of duration |
| CDD | Customer Due Diligence |
| CRF | ‘Cellule de Renseignement Financier’ – The Luxembourg ‘FIU’ of the State Prosecutor of the Luxembourg District Court |
| Company | the IFM |
| Correspondent relationship | The provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services; or any relationship between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent customer, and including any relationship established for securities transactions or funds transfers |
| CSSF | Commission de Surveillance du Secteur Financier (<https://www.cssf.lu/en/about-the-cssf>) |
| CSSF Regulation 12-02 | CSSF Regulation No. 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing, as amended |
| CTF | Combating the financing of terrorism, counter-terrorism financing |
| CRS | The Common Reporting Standard (CRS), developed in response to the G20 request and approved by the OECD Council on 15 July 2014, calls on jurisdictions to obtain information from their financial institutions and automatically exchange that information with other jurisdictions on an annual basis. It sets out the financial account information to be exchanged, the financial institutions required to report, the different types of accounts and taxpayers covered, as well as common due diligence procedures to be followed by financial institutions |
| Customer / Client | Natural or legal person with whom a business relationship exists or for whom an occasional transaction is carried out within the meaning of point (b) of Article 3(1) of the AML/CTF Law, including persons purporting to act on behalf of the customer.  In this policy, the term ‘investor’ may be used when referring specifically to the customer (investor of the Fund). The term customer or client also includes in this AML/CTF manual the other business relationships (distributors, parties to the assets, etc.) |
| DD | Due Diligence |
| Directive (EU)  2015/849 | Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, as amended, and its implementing acts |
| Distributor | Legal or natural person who markets the shares of UCIs and with whom the Fund or the IFM has an agreement This notion might include the ‘Global Distributor’ which appoints sub-distributors. |
| EDD | Enhanced Due Diligence |
| Equivalent country | Country imposing AML/CTF rules which are deemed equivalent to the ones applicable in Luxembourg |
| EEA | European Economic Area |
| EU | European Union |
| FATCA | The “Foreign Account Tax Compliance Act” is a US tax regulation which was passed as part of the HIRE Act, generally requires that foreign financial Institutions and certain other non-financial foreign entities report on the foreign assets held by their U.S. account holders or be subject to withholding on withhold able payments. Its objective is to reduce tax evasion by US individuals with respect to income from financial assets held directly (on an account) or indirectly (through a foreign entity) outside the United States.  The Final Regulations, as amended and completed, form the basis for the implementation of FATCA by Foreign Financial Institutions worldwide, save for the application of an intergovernmental agreement (IGA) on FATCA entered into between the United States and a given partner jurisdiction, as this is the case for Luxembourg. |
| FATF | Financial Action Task Force |
| FIU | Financial Intelligence Unit “under the administrative supervision of the Chief Public Prosecutor” |
| GoAML | The online portal which is to be used to make declarations of suspicious activities or transactions in Luxembourg. This system allows the reporting in a standardised format to the FIU. Professionals (including the IFM, the Funds and the regulated service providers) must report without delay to the FIU when they are aware, suspect or have reasonable grounds to suspect that money laundering, an associated predicate offence or terrorist financing is happening or has been committed or attempted, regardless of the amount involved |
| High risk country | Country included in the list of high-risk third countries pursuant to Article 9(2) of Directive (EU) 2015/849 or designated by the Financial Action Task Force (FATF) as presenting a higher risk as well as any other country that the supervisory authorities and the professionals consider, in the framework of their money laundering and terrorist financing risk assessment, as a high-risk country based on geographical “risk” factors listed in Annex IV of the AML/CTF Law. |
| IFM | Investment Fund Manager/Management Company |
| Initiator | Also ‘sponsor’ - The legal or physical person(s) at the inception /origin of the Fund project. |
| Investor | Please refer to ‘customer’ |
| KYC | Know Your Client – refers to the client due diligence obligations on customers |
| Law implementing restrictive measures in financial matters | Law of 19 December 2020 regarding implementation of restrictive measures in financial matters implementing by the Grand Duchy of Luxembourg of the restrictive measures in financial matters adopted against certain States, natural and legal persons, entities and groups |
| Management | the persons having a real influence on the overall management of the professional's business |
| ML/TF | Money laundering and terrorist financing |
| PEP | Natural persons who are or have been entrusted with prominent public functions and family members or persons known to be close associates, of such persons.  Natural persons who are or have been entrusted with prominent public functions mean all natural persons, including:  (a) heads of State, heads of government, ministers and deputy or assistant ministers;  (b) members of parliament “or of similar legislative bodies”;  (c) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;  (d) members of courts of auditors or of the boards “or directorates”25 of central banks;  (e) ambassadors, chargés d’affaires and high-ranking officers in the armed forces;  (f) members of the administrative, management or supervisory bodies of State-owned enterprises;  (g) important officials “and members of the governing bodies” of political parties;”  (h) directors, deputy directors and members of the board or equivalent function of an international organisation”;  (i) the natural persons exercising the functions included in the list published by the European Commission based on Article 20a(3) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, hereinafter referred to as “Directive (EU) 2015/849.  None of the categories set out in (a) to (h) above shall be understood as covering middle ranking or more junior officials.  ”Family members” mean all physical persons, including in particular:  (a) the spouse;  (b) any partner considered by national law as equivalent to the spouse;  (c) the children and their spouses, or partners “considered by national law as equivalent to a spouse”;  (d) the parents;  (e) the brothers and sisters.”  “Persons known to be close associates” mean all natural persons, including:  (a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to above;  (b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to above |
| Professional  obligations | Obligations for professionals as regards AML/CTF |
| Proliferation | Proliferation is defined by the Financial Action Task Force (FATF) as the illegal manufacture, acquisition development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials |
| Proliferation Financing (“PF”) | Proliferation financing is defined by the FATF as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations |
| RBA | Risk Based Approach |
| RC | As required under article 4(1) fourth paragraph and second paragraph, sub-paragraph a) of the AML/CTF Law and as further described by the FAQ issued on 25 November 2019 by the CSSF professionals must appoint a compliance officer at appropriate hierarchical level (the original French version of the law refers to a “responsable du contrôle du respect des obligations” and thus, the acronym “RC” will be used hereafter). The English version of the CSSF 12/02 Regulation as amended uses the term ‘compliance officer in charge of AML/CTF matters |
| RBE Law | The law of 13 January 2019 establishing a Register of Beneficial Owners |
| Red flag | A warning signal that should bring attention to a potentially suspicious situation, transaction or activity |
| Regulated market | A market which is regulated, operates regularly and is recognised and open to the public. |
| RR | As required under article 4(1) fourth paragraph and second paragraph, sub-paragraph a) of the AML/CTF Law and as further described by the FAQ issued on 25 November 2019 by the CSSF, professionals must appoint a person among the members of their management bodies, responsible for compliance with the professional obligations as regards the fight against money laundering and terrorist financing (the original French version of the law refers to a “responsable du respect des obligations” and thus, the acronym “RR” will be used hereafter).  Further according to the FAQ, ‘the RR can be the board of managers (or other governing body depending on the legal structure of the IFM) acting as a collegial body . Alternatively, the board may appoint one of its members as RR. The RR must be reachable for any contact by the Luxembourg AML/CTF competent authorities’ |
| SDD | Simplified due diligence |
| SAR | Suspicious Activity Report |
| Senior  Management | Any director (dirigeant, member of the authorised management) or employee with sufficient knowledge of the professional's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of managers  CSSF Regulation 12/02 as amended further defines: for the purposes of point (c) of Article 3-2(3) of the AML/CTF Law [with regards to the approval by the senior management in the context of enhanced due diligence], that Senior Management shall mean at least the person responsible for compliance |
| Shell bank | Credit institution or a financial institution or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management and which is unaffiliated with a regulated financial group |
| Source of funds | Origin of the funds involved in a business relationship or occasional transaction. It includes both the activity that generated the funds used in the business relationship, for example the investor salary, as well as the means through the investor’s funds were transferred |
| Source of wealth | Origin of the investor’s estimated total wealth, for example inheritance or savings |
| STR | Suspicious Transaction Report |
| TFS | Targeted financial sanctions – covering both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated states, persons, entities and groups |
| UBO | Ultimate Beneficial Owner |

# Annexe 2– Key AML/CTF legal and regulatory framework (non-exhaustive list)

This AML /CTF Manual has been prepared considering the international, European and national legal and regulatory applicable framework. It purports to fulfil the requirements of the Luxembourg AML/CTF legal and regulatory framework.

Compliance of the IFM with the professional obligations deriving from the applicable Luxembourg AML/CFT legal and regulatory framework is subject to the supervision of the Luxembourg Commission de Surveillance Financier (the "CSSF").

The key legal and regulatory texts are mentioned thereafter for ease of reference.

All the laws, regulations and circulars in force are available on the CSSF website:

* <https://www.cssf.lu/en/search/Financial%20crime>

**European Directives and Regulations**

* Commission Delegated Regulation (EU) 2020/855 of 7 May 2020 amending Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council, as regards adding the Bahamas, Barbados, Bostwana, Cambodia, Ghana, Jamaica, Mauritius, Mongolia, Myanmar/Burma, Nicaragua, Panama and Zimbbabwe to the table in point I of the Annex and deleting Bosnia-Herzegovina, Ethiopia, Guyana, Lao People’s Democratic Republic, Sri Lanka and Tunisia from this table;
* Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000.642/JHA;
* Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries;
* Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union;
* Council Implementing Regulation (EU) 2019/84 of 21 January 2019 implementing Regulation (EU) 2018/1542 concerning restrictive measures against the proliferation and use of chemical weapons;
* Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combatting money laundering by criminal law;
* Council Regulation (EU) 2018/1542 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons;
* Commission Delegated Regulation (EU) 2018/1467 of 27 July 2018 amending Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council, as regards adding Pakistan to the table in point I of the Annex;
* Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (the “**5th AML Directive**”);
* Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA;
* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
* Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, as amended (the “**Directive (EU) 2015/849**”);
* Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006

**Other European texts**

* EBA Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (“The ML/TF Risk Factors Guidelines”), repealing and replacing Guidelines JC/2017/37

Supranational risk assessment of the money laundering and terrorist financing risks affecting the Union, issued by the European Commission on 27 October 2022 (COM(2022) 554 final)

**Luxembourg legal and regulatory framework**

Luxembourg regulations are made of Laws, Grand Ducal Regulations (“GDR”), Ministerial Regulations, CSSF Regulations, CSSF Circulars, CRF circulars, LBR circulars and joint CSSF/CRF circulars.

The RC will notify the employees and explain the changes whenever a new legal or regulatory document is published.

**AML/CTF Laws**

* Law of 19 December 2020 on the implementation of restrictive measures in financial matters, and related acts adopted by the European Union or the United nations imposing targeted financing sanctions;
* Law of 25 March 2020 amending the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended;
* Law of 13 January 2019 establishing a Register of beneficial owners;
* Ministerial Regulation of 16 November 2018 amending Ministerial Regulation of 9 July 2009 creating a committee on the prevention of money laundering and terrorist financing;
* Law of 10 August 2018 amending: 1° the Code of Criminal Procedure, 2° the Law of 7 March 1980 on the organisation of the judicial system, as amended, 3° the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended, 4° the Law of 25 March 2015 determining the salaries and the advancement conditions and rules for civil servants for the purpose of organising the Financial Intelligence Unit (FIU),
* Law of 10 August 2018 on information to obtain and hold by trustees and transposing Article 31 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC,
* The Law of 23 December 2016 implementing the 2017 tax reform,
* Ministerial regulations amending Annex I C of Grand-ducal Regulation of 29 October 2010 implementing the law of 27 October 2010 relating to the implementation of United Nations Security Council resolutions as well as acts adopted by the European Union concerning prohibitions and restrictive measures in financial matters in respect of certain persons, entities and groups in the context of the combat against terrorist financing;
* Law of 12 November 2004 on the prevention of money laundering and terrorist financing, as amended;
* Law of February 19th, 1973 concerning the sale of medical substances and the fight against drug addiction;
* Luxembourg Penal Code.

**Ministerial Regulations**

The Ministry of Finance publishes Ministerial Regulations regarding sanctioned entities or make directly reference to European Union decisions. They are available on the Ministry of Finance website and aim to update the list of persons, entities and groups concerned by interdictions and restrictive financial measures in the context of the fight against financing of terrorism.

Therefore, assets and economical resources, directly, indirectly or jointly owned or controlled, with or by these persons are frozen.

The Ministry of Finance is competent regarding questions and interrogations on interdictions and restrictive financial measures which can be raised by professionals, who are obliged to apply them. Any question or interrogation (for example, in case of homonyms) from the persons, groups or entities subject to these interdictions and restrictive financial measures should be addressed to:

Ministry of Finance, L-2931 Luxembourg, or

by e-mail: [sanctions@fi.etat.lu](mailto:sanctions@fi.etat.lu).

According to Article 6 of the Law of 19 December 2020, the IFM must inform the Ministry of Finance of the enforcement of each restrictive measure taken in respect of a State, natural or legal person, entity or group designated and the implementing regulations, including attempted transactions.

Please see: <https://mfin.gouvernement.lu/fr/dossiers/2018/sanctions-financiaires-internationales.html>

* Ministerial regulations amending Grand-ducal Regulation of 29 October 2010 implementing the law of 27 October 2010 relating to the implementation of United Nations Security Council resolutions as well as acts adopted by the European Union concerning prohibitions and restrictive measures in financial matters in respect of certain persons, entities and groups in the context of the combat against terrorist financing

**Grand Ducal Regulations**

* Grand-Ducal Regulation of 14 November 2022 providing details on the Law of 19 December 2020 on the implementation of restrictive measures in financial matters.
* Grand-ducal regulation of 15 February 2019 relating to the terms of registration, payment of administrative fees as well as access to information entered in the Register of beneficial owners.
* Grand-ducal Regulation of 1 February 2010 as amended (coordinated version) providing details on certain provisions of the amended law of 12 November 2004 on the fight against money laundering and terrorist financing.

**CSSF Regulations**

* CSSF Regulation N°12/02 of 14 December 2012 on the fight against money laundering and the financing of terrorism, as amended (the “CSSF Regulation”).

**CSSF and CRF Circulars**

* The amended CSSF Circular concerning: 1) high-risk jurisdictions on which enhanced due diligence and, where appropriate, counter-measures are imposed; and 2) jurisdictions under increased monitoring of the FATF as amended.
* Circular CSSF 21/782 of 24 September 2021 : Adoption of the revised guidelines, by EBA, on money laundering and terrorist financing risk factors
* The CSSF Circular 21/767 implementing FATF statements concerning 1) high-risk jurisdictions on which enhanced due diligence and, where appropriate, counter-measures are imposed 2) jurisdictions under increased monitoring of the FATF;
* The CSSF Circular 20/744 complement to circular CSSF 17/650 “application of the law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended and Grand Ducal Regulation of 1 February 2010 providing details on certain provisions of the AML/CTF law to predicate tax offences”
* The CSSF Circular 20/742 relating to entry into force (1) of the Law of 25 March 2020 amending, inter alia, the Law of 12 November 2004 on the fight against money laundering and terrorist financing, and (2) of the Law of 25 March 2020 establishing a central electronic data retrieval system related to IBAN accounts and safe-deposit boxes;
* The CSSF Circular 20/740 of 10 April 2020 regarding Financial crime and AML/CTF implications during the COVID-19 pandemic;
* The CSSF Circular 19/732 of 20 December 2019 relating to the prevention of Money Laundering and Terrorist Financing: Clarifications on the Identification and Verification of the Identity of the Ultimate Beneficial Owner(s) (the “CSSF Circular 19/732”);
* The CSSF Circular 18/698 of 23 August 2018 relating to the authorization and organization of Investment Fund Managers incorporated under Luxembourg law. Specific provisions on the fight against money laundering and terrorist financing applicable to Investment Fund Managers and entities carrying out the activity of registrar agent;
* The CSSF Circular 18/684 of 13 March 2018 relating to entry into force of the Law of 13 February 2018 amending, inter alia, the Law of 12 November 2004 on the fight against money laundering and terrorist financing;
* The CSSF Circular 17/661 of 24 July 2017 relating to adoption of the joint guidelines issued by the three European Supervisory Authorities (ESMA/EBA/EIOPA) on money laundering and terrorist financing risk factors;
* The CSSF Circular 17/660 of 05 July 2017 relating to regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006;
* The CSSF Circular 17/650 of 17 February 2017 relating to the application of the AML/CTF Law and of the Grand-Ducal Regulation to predicate tax offences, as amended;
* The CSSF circular 15/631 of 28 December 2015 relating to dormant or inactive accounts;
* The CSSF Circular 15/609 of 27 March 2015 relating to the developments in automatic exchange of tax information and anti-money laundering in tax matters;
* The CSSF Circular 13/556 on 16 January 2013 relating to the entry into force of CSSF Regulation N° 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing - repeal of Circulars CSSF 08/387 and CSSF 10/476;
* The CSSF Circular 11/529 of 22 November 2011 on the risk analysis regarding the fight against money laundering and terrorist financing (AML/CTF);
* The CSSF Circular 11/528 of 15 December 2011 on abolition of the transmission to the CSSF of suspicious transaction reports regarding potential money laundering or terrorist financing (the “CSSF Circular 11/528”);
* The CSSF Circular 10/495 on 9 December 2010 relating to the entry into force of the Law of 27 October 2010 on the fight against money laundering and terrorist financing;
* The CSSF Circular 10/486 on 11 October 2010 relating to the fight against money laundering and terrorist financing: amendment of certain provisions of Circular CSSF 03/113;
* The CSSF Circular CSSF 10/458 dated 11 May 2010 on measures concerning the Democratic People’s Republic of Korea (DPRK);
* The CSSF Circular 06/247 dated 8 June 2006 on business relationships and transactions with natural or legal persons of North Korea;
* The CSSF Circular CSSF 07/327 dated 21 November 2007 on 1) FATF statement on Iran 2) FATF guidance regarding the implementation of certain UN resolutions;
* The CRF Guideline relating to suspicious operations report replacing the guideline of 1 January 2018 and applicable from November 1st ,2018;
* The CRF Guideline relating to freezing of suspicious transactions replacing the Guideline of 31 December 2016 and applicable from November 1st,2018.

**Other CSSF guidelines**

* FAQ regarding International Financial Sanctions updated on 21st March 2022
* FAQs regarding persons involved in AML/CTF for a Luxembourg Investment Fund or Investment Fund Manager supervised by the CSSF for AML/CTF purposes (dated 25 November 2019);
* CSSF sub-sectorial ML/TF risk analysis - collective investments dated 01 January 2020 as amended in 2022
* CSSF ML/TF sub-sector risk assessment – Specialised Professionals of the Financial Sector providing corporate services (Trust and IFMService Provider activities) dated July 2020

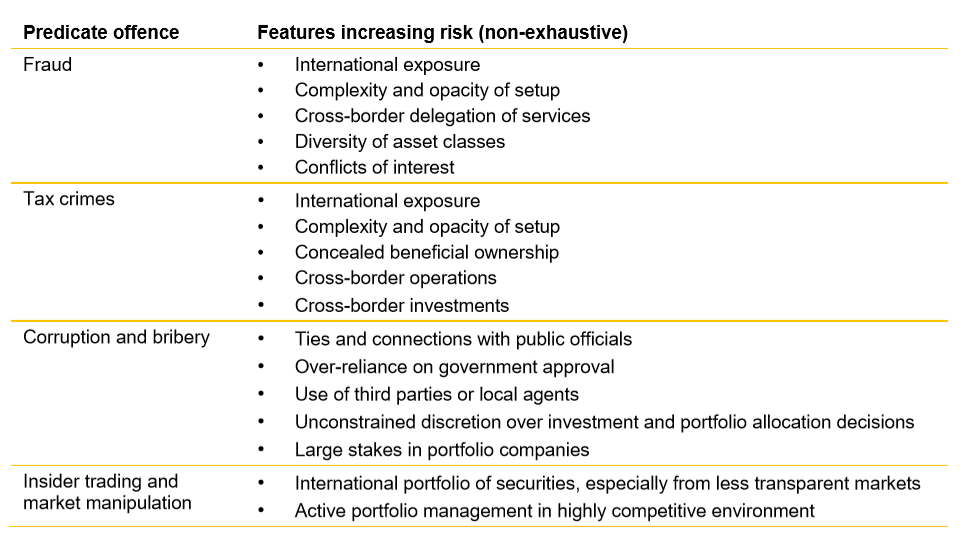
**Others**

* The FATF Recommendations relating to the International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation;
* The FATF risk based approach on securities and other FATF guidances and publications;
* ALCO WG50 – Sound Practices for Transfer Agent and Investment Fund Manager Compliance Officers.
* Guidelines by the Ministry of Finance relating to the implementation of financial restrictive measures (sanctions) against third countries, entities or individuals;
* Guidelines by the Ministry of Finance relating to the implementation of financial sanctions against certain persons, entities, bodies and groups within the framework of combating terrorism financing.
* Ministry of Finance, National risk assessment of money laundering and terrorist financing from 26.09.2018, updated on 15th September 2020 (“NRA”)
* CRF Déclaration d’opérations suspectes (applicable from 01/01/2017) – only in French
* CRF – Blocage de transactions suspectes (applicable à partir du 01/11/2018) – only in French
* CRF - Infractions primaires fiscales (applicable from 01/04/2017) – only in French

**LBR: legislation and circulars**

* <https://www.lbr.lu/mjrcs-rbe/jsp/webapp/static/mjrcs/en/mjrcs-rbe/legislation.html?FROM_MENU=true&time=1584002729232&pageTitle=menu.item.geninfolegislation&currentMenuLabel=menu.item.geninfolegislation>
* Circular LBR 19/01 : Register of Beneficial Owners
* Circular LBR 19/02 : The application of the provisions relating to the Register of Beneficial Owners to the non-profit associations (ASBL)
* Circular LBR 19/03 : The application of the provisions relating to the Register of Beneficial Owners to the foundations under the amended law of 21 April 1928 on non-profit associations and foundations
* Circular LBR 19/04: Application of the regulation concerning the register of beneficial owners to public-law institutions or companies which are partly or predominantly held by public institutions

# Annex 3 – Overview of key predicate offences perpetrated within collective investments[[5]](#footnote-6)



# Annex 4 – Annex II, III and IV of the AML/CTF Law as amended[[6]](#footnote-7)

**ANNEX II**

The following is a non-exhaustive list of risk variables that the professionals shall consider when determining to what extent to apply customer due diligence measures in accordance with Article 3(2a):

* + 1. the purpose of an account or relationship;
    2. the level of assets to be deposited by a customer or the size of transactions undertaken;
    3. the regularity or duration of the business relationship.

**ANNEX III**

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in the second subparagraph of Article 3-1(2):

1. Customer risk factors:

* 1. public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
  2. public administrations or enterprises from countries or territories having a low level of corruption;
  3. customers that are resident in geographical areas of lower risk as set out in point (3);

1. Product, service, transaction or delivery channel risk factors:
2. life insurance policies for which the premium is low;
3. insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
4. a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member’s interest under the scheme;
5. financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
6. products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (particularly, certain types of electronic money).
7. Geographical risk factors “- registration, establishment, residence in”:
8. Member States;
9. third countries having effective anti-money laundering and counter terrorist financing systems;
10. third countries identified by credible sources as having a low level of corruption or other criminal activity;
11. third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

**ANNEX IV**

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in the second subparagraph of Article 3-2(1):

* + 1. Customer risk factors:

1. the business relationship is conducted in unusual circumstances;
2. customers that are resident in geographical areas of higher risk as set out in point (3);
3. legal persons or arrangements that are personal asset-holding vehicles;
4. companies that have nominee shareholders or shares in bearer form;
5. businesses that are cash-intensive;
6. the ownership structure of the IFMappears unusual or excessively complex given the nature of the company's business;
7. customer is a third-country national who applies for residence rights or citizenship in exchange of capital transfers, purchase of property or government bonds, or investment in corporate entities.”
   * 1. Product, service, transaction or delivery channel risk factors:
8. private banking;
9. products or transactions that might favour anonymity;
10. non-face-to-face business relationships or transactions, without certain safeguards, such as “electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities”;
11. payment received from unknown or unassociated third parties;
12. new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products; (Law of 25 March 2020) “
13. transactions related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species.”
14. Geographical risk factors:
15. without prejudice to Article 3-2(2), countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective anti-money laundering and counter terrorist financing systems;
16. countries identified by credible sources as having significant levels of corruption or other criminal activity;
17. countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
    1. countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.”

1. Based on the definition of “Money Laundering” provided by ABBL, consulted on: https://www.abbl.lu/topic/money-laundering/ [↑](#footnote-ref-2)
2. *Source: CSSF, “ML/TF Sub-sector Risk Assessment, Collective Investments”, January 2020.* [↑](#footnote-ref-3)
3. Non exhaustive list [↑](#footnote-ref-4)
4. Non exhaustive list [↑](#footnote-ref-5)
5. *Source: CSSF, “ML/TF Sub-sector Risk Assessment, Collective Investments”, January 2020.* [↑](#footnote-ref-6)
6. https://www.cssf.lu/wp-content/uploads/L\_121104\_AML.pdf [↑](#footnote-ref-7)