Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) & Sanctions Policy

CALLISTO
CAPITAL

Callisto Capital B.V. is the registered Alternative Investment Fund Manager (AIFM) of Callisto Capital

Version 2.2

September 15, 2025

Document details

Policy title	AML/CFT & Sanctions Policy
Fund name	Callisto Capital
Fund Manager	Callisto Capital B.V.
Legal Owner	Stichting Juridisch Eigenaar Callisto Capital
Administrator	AssetCare Fund Services B.V.
Fund Structure	Closed fund for the joint account ("BFGR") with an open-end character
License/Registration	AIFMD Registration
Risk area	Money laundering, terrorist financing and sanctions
Creation date	06-06-2023
Last Revision Date	15-09-25
Status	Version 2.2

Document Version

Date	Version	Author	Description
16 June 2023	1.0	Fund Manager and Administrator	First version
18 June 2024	2.0	Fund Manager and Administrator	Second version
24 June 2024	2.1	Fund Manager and Administrator	Second version
15 September 2025	2.2	Fund Manager and Administrator	Second version

Agreed by Fund Manager

Date	Version	Approval
21July 2023	1.0	Nicolaas Kaptein
21July 2023	1.0	Doeke Goedegebuure
	2.1	Nicolaas Kaptein
	2.1	Doeke Goedegebuure
15 September 2025	2.2	Niels Kaptein (via e-mail)

Content

Document rights

This AML/CFT & Sanctions Policy (hereinafter referred to as “Policy”) is confidential and must be accessed only by authorized persons. Unauthorized distribution of this document increases the risk of money laundering and terrorist financing. This document is considered dynamic and will be updated based on new insights and market developments. Any changes to the Policy must be approved by Fund Manager and are tracked using version numbers.

Access to the Policy is limited to the individuals listed below, as well as supervisory authorities and entities where Legal Owner holds, or is opening, a bank and/or investment account.

Name	Company	Role
Nicolaas Kaptein	Callisto Capital B.V.	Fund Manager
Doeke Goedegebuure	Callisto Capital B.V.	Fund Manager
Nicolaas Kaptein	Stichting Juridisch Eigenaar Callisto Capital	Legal Owner
Doeke Goedegebuure	Stichting Juridisch Eigenaar Callisto Capital	Legal Owner
Employees	AssetCare Fund Services B.V.	Administrator

1 General

1.1 Introduction and scope

Callisto Capital B.V. (hereinafter referred to as “Fund Manager”) is registered as a so-called “light” manager under the Alternative Investment Fund Manager Directive (hereinafter referred to as “AIFMD”), as outlined in Article 2:66a of the Dutch Financial Supervision Act (in Dutch: Wet op het financieel toezicht, hereinafter referred to as the “Wft”). This registration has been duly acknowledged by the Dutch Authority for the Financial Markets (hereinafter referred to as “AFM”). Consequently, Fund Manager is exempted from the AIFMD license requirement for managing assets as specified in Article 2:65 of the Wft.

Fund Manager has been appointed as the fund manager of Callisto Capital (hereinafter referred to as “Fund”), which is classified as an investment institution under the Wft and invests exclusively in Digital Assets. As a “light” manager under the AIFMD, Fund Manager is subject to the Anti-Money Laundering and Counter-Terrorist Financing Act (hereinafter referred to as "Wwft") and the Sanctions Act 1977 (hereinafter referred to as "Sanctions Act"). Fund Manager is responsible for complying with these laws and preventing any relationships with individuals or entities that may use the Fund for money laundering, terrorism financing, or sanctions violations.

This Policy outlines the procedures for mitigating the AML/CFT and sanction risks and is grounded on a risk-based approach. This involves implementing appropriate mitigating measures and procedures based on the assigned risk level for the following type of relationships:

- an (aspirant) Unit Holder ⇢ an individual or legal person who holds Units in the Fund.
- an (aspirant) Correspondent Relation ⇢ this refers to inter-institutional relationships that have been established by Fund Manager to e.g. manage the Fund’s assets; or
- any other (aspirant) relation ⇢ any other (natural or legal) person whom Fund Manager collaborates with on behalf of the Fund.

The risk level of each relationship is determined based on the following risk factors:

- Unit Holder risk;
- Geographical risk;
- Financial risk;
- Delivery channel risk;
- Product risk.

Obtaining accurate and objective information from a relation is considered essential for conducting an effective Customer Due Diligence (hereinafter referred to as “CDD”). To achieve this, the necessary information is requested prior to entering into a relationship. This information is then analyzed (I) to assess the associated risks and their potential impact, and (II) to mitigate these risks where possible. In order to ensure effective risk mitigation, relevant quantitative and qualitative information is kept up-to-date. As such, transaction monitoring and event-driven reviews are conducted in addition to initial CDDs.

To determine the suitable level of procedures and measures for each relationship, the risks are categorized as follows:

- Low;
- Medium;
- High;
- Unacceptable.

A higher risk rating requires more extensive and frequent measures to manage and mitigate the risks.

1.2 Objectives and principles

1.2.1 Objectives

The Policy considers the following objectives:

- To assess the Fund's risks related to money laundering, terrorist financing and sanctions violations;
- To determine Fund Manager's risk appetite regarding combating money laundering, terrorist financing and sanctions violations;
- To establish a framework for combating money laundering, terrorist financing, and sanctions violations based on the identified risks, Fund Manager's risk appetite, and applicable legal requirements applicable for a "light" manager. This includes the following:
  - To determine the responsibilities of Fund Manager and other parties in the fund structure;
  - To establish mitigating measures, including conducting intitial CDDs, transaction monitoring, event-driven reviews, periodic reviews and reporting;
  - To identify the required documentation and information to conduct the procedures effectively.

1.2.1 Principles

The Policy is governed by the following principles:

- The Policy applies to all parties who want to collaborate with and/or invest in the Fund;
- CDD must be completed before establishing a relationship;
- Fund Manager provides collective asset management only through the Fund;
- Fund Manager does not accept cash, (direct deposits of) virtual money or currency, and prepaid cards from Unit Holders;
- Fund Manager has outsourced various AML/CFT and sanctions related activities to Administrator;
- Despite the outsourcing, Fund Manager (periodically) monitors whether Administrator performs the AML/CFT and sanctions related activities on all parties in line with this Policy, as Fund Manager is fully responsible for complying with the Wwft and Sanctions Act;
- Both Fund Manager and Administrator should have a good understanding of applicable legal requirements, the AML/CFT & Sanctions Policy and procedures, and be aware of their responsibilities;
- Information that follows from the AML/CFT and sanctions related activities are documented such that historical information can be included in reviews, and it can be easily and quickly assessed by supervisory authorities in the event of a request;
- Fund Manager ensures adequate follow-up on information related to the AML/CFT and sanctions activities of the parties;
- Information is retained for five years after a relationship is terminated or after an aspirant Unit Holder is rejected;

- Records are held on a durable medium in accordance with applicable Privacy Laws;
- Fund Manager reassess or outsources the reassessment of the AML/CFT & Sanctions Policy at least once a year to ensure that the Policy remains up to date with market developments.

1.3 Legal framework

1.3.1 Legislation

This Policy complies with the relevant legislations, including the following:

Title	Description c
Anti-Money Laundering Directive (hereinafter referred to as "AMLD")	The European AMLD provides a framework to prevent and combat money laundering, terrorist financing and the misappropriation of assets in the financial system. The European Parliament adopted the sixth version of the AMLD on July 20, 2021.
Wwft	This Dutch law imposes obligations on the prevention of money laundering, terrorist financing and the reporting of unusual transactions to the Financial Intelligence Unit (hereinafter referred to as "FIU").
Sanctions Act	Under the Sanctions Act 1977, investment institutions must screen their relationships on sanctions prior to establishing a business relationship and periodically thereafter. If a relation is listed on a sanction list, it must be reported to the supervisor and assets must be frozen.
Wft	The Wft regulates the supervision of financial institutions in the Netherlands, effective since January 1, 2007. "Light" managers under the AIFMD are exempted from requirements imposed on fund managers under the Wft.
General Data Protection Regulation (hereafter referred to as the "GDPR").	The GDPR came into force on May 25, 2018, and governs data privacy for (potential) Unit Holders and other relations of the Fund.

Besides, this Policy considers others legislations, including the Uitvoeringsregeling Wwft, Uitvoeringsbesluit Wwft 2018, AFM Leidraad Wwft, Wwft BES en Sanctiewet of 25 juli 2018, Risk Factor Guidelines van de Joint Committee of the European Supervisory Authorities (JC 2017 37) and article 21 and 22 Besluit Gedragstoezicht financiële ondernemingen ("BGfo").

Moreover, Fund Manager completes an annual Wwft & Sanctions Act questionnaire for investment institutions and this questionnaire is also used to determine whether the Policy still meets the expectations. At last, the AFM Applicability of Wwft to (managers of) investment institutions in crypto and the DNB Crypto Recommendations for a Regulatory Framework are consulted.

1.3.2 Other

In addition to the legal framework, multiple guidelines from leading global bodies have been used for this policy.

1.3.2.1 FATF

The Financial Action Task Force (hereinafter referred to the "FATF") is an independent inter-governmental body that establishes international standards and promotes policies to safeguard the global financial system from money laundering, terrorist financing, and the proliferation of weapons of mass destruction. With over two hundred countries and jurisdictions that are committed to implement the FATF standards and policies, the FATF recommendations are recognized as the global standard against money laundering and terrorist financing.

The primary objectives of the FATF are to establish standards and promote the effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing and other threats to the integrity of the international financial system.

This policy adheres to the following FATF documents at a minimum:

Number	Title
1	FATF Report – Money Laundering and Terrorist Financing in the Securities Sector
2	FATF Guidance – Risk-Based Approach Guidance for the Securities Sector
3	FATF Guidance – Transparency and Beneficial Ownership
4	FATF Guidance – Politically Exposed Persons
5	FATF Guidance – Guidance for a risk-based approach: Virtual assets and virtuals asset service providers

1.3.2.2 Wolfsberg Group

The Wolfsberg Group is a consortium of thirteen major banks worldwide, dedicating to creating frameworks and guidance for managing risks related to financial crime risks, especially in the areas of know your customer (KYC) and AML/CFT policies.

The Policy has taken into consideration the following guidelines of The Wolfsberg Group:

Number	Title
1	Wolfsberg Statement – Anti-Money Laundering Guidance for Mutual Funds and Other Pooled Investment Vehicles
2	Wolfsberg Group Frequently Asked Questions (FAQs) Source of Wealth and Source of Funds (Private Banking/Wealth Management)
3	Wolfsberg Guidance on Politically Exposed Persons (hereinafter referred to as “PEP”)
4	Wolfsberg Guidance on Sanctions Screening
5	The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption
6	Wolfsberg Group Country Risk Frequently Asked Questions (FAQs)

1.4 Integrity risk

1.4.1 Assessment

Annually, Fund Manager conducts a risk assessment to evaluate the Fund's risk exposure to money laundering, terrorist financing and sanctions violations. This risk assessment analyzes the inherent risks that may arise from various risk factors (Unit Holder, Geographical, Financial, Delivery channel and Product risk).

Section 2 presents the current assessment.

1.4.2 Risk appetite

The level of risk appetite that Fund Manager is willing to take on regarding the Fund's involvement in activities related to money laundering, terrorist financing and sanctions violations (or other integrity risks) by Unit Holders or other relations is know as the risk appetite.

Further information on the risk appetite can be found in Section 2.4.

1.5 Outsourcing

The activities outlined in this Policy, including CDD, have been outsourced to AssetCare Fund Services B.V. (hereinafter referred to as "Administrator") by Fund Manager. This implies that Administrator carries out most of the operational activities that follow from this Policy.

Despite outsourcing activities, Fund Manager remains ultimately responsible for complying with the Wwft and Sanction Act as stipulated by law. As a result, Fund Manager (periodically) monitors Administrator for the correctness and completeness of activities and compliance with related laws and regulations.

The role of Administrator and the monitoring process are further explained in Section 3.3.

1.6 Document structure

The remainder of this policy is structured as follows:

- Section 2 outlines the risk assessment related to the Fund's exposure to money laundering, terrorist financing and sanctions violations, as well as Fund Manager's risk appetite concerning the identified risk;
- Section 3 outlines the Fund structure and the roles and responsibilities of the involved parties regarding AML/CFT and sanctions;
- Section 4 outlines the theoretical framework necessary for performing the AML/CFT and sanctions related activities;
- Section 5 outlines the practical procedures for conducting the AML/CFT and sanctions related activities;
- Section 6 outlines the reporting obligations that arise from the AML/CFT and sanctions related responsibilities;
- Section 7 outlines the storage and privacy measures for the AML/CFT and sanctions related activities.

Additionally, Appendix 1 contains the definitions, Appendix 2 contains the risk classification per country, and Appendix 3 contains the sanctions lists used.

2 Risk assessment

2.1 Introduction

This section includes an assessment of the Fund's risks related to money laundering, terrorist financing, and sanctions.

2.2 Risk areas

Given the Fund's role in the financial system, the following risk areas have been identified:

Risk Area	Keyword	Description
Sanctions violations	Prevention	Prevention of entering into relationships with individuals or entities by identifying (potentially) unusual transactions or financial services – as per the Sanctions Act.
Money Laundering	Origin	Prevention of receiving funds from criminal activities by Legal Owner.
Terrorist Financing	Destination	Prevention of the Fund being used for terrorist financing and/or exposing the networks and plans of terrorist organizations.

2.3 Risk identification and weighting

2.3.1 Per risk factor

To assess the risk associated with each risk area (money laundering, terrorist financing and sanctions violations), the risk factors from the Wwft and Sanctions Act are used. These risk factors include the Client (Unit Holder), Geographic, Delivery channel and Product risk. Financial risk is also included to emphasize the source of funds.

Risk factor	Description	Assessment	Risk Weighting
Unit Holder risk	The risk at the Unit Holder's level is assessed by monitoring several factors, including sanction lists, PEP lists, adverse media, the complexity of the structure, and the risks associated with the Unit Holder's profession and work sector.	It is expected that the majority of the Fund's Unit Holder base will continue to be comprised of individuals or entities with a straightforward structure. Identifying the structure and profession/sector of the Unit Holder is an essential step in assessing this risk factor.	▪ The risk assessment considers a low Unit Holders risk due to the clear structure of the individuals and the relatively simple entities involved. ▪ The risk weighting is higher if Unit Holders have a more complex structure or are involved in cash-intensive sectors. In these cases, a more thorough investigation is carried out with respect to their source of funds. ▪ Sanctions: Unit Holders and other relations are initially and continuously monitored for sanctions to avoid any links with relations on a sanctions list. ▪ Money laundering: A profile of the Unit Holder is created to monitor the background and source of funds, including PEP status, negative media, profession, and underlying companies in the structure, to prevent money laundering. ▪ Terrorist financing: To prevent terrorist financing, funds can only be refunded to the specified IBAN within the EU/EFTA used to fund the initial subscription of the Unit Holder. In case this IBAN is no longer active, funds can only be refunded to an IBAN within the EU/EFTA in the name of the Unit Holder, verified by reviewing a bank statement prior to refunding.
Geographical risk	The geographical risk is evaluated by monitoring the residency/residencies, nationality/nationalities and the country where the Unit Holder and/or bank account is located.	The Fund anticipates primarily attracting Unit Holders with Dutch nationality in the future, although it is possible to attract Unit Holders of other nationalities. The Fund may potentially deal with various countries outside the Netherlands (see Appendix 2). The investigation is enhanced if a related country poses a higher risk.	▪ The risk weighting is considered low as most Unit Holders have Dutch nationality. ▪ Enhanced CDD is conducted if there is a link between a Unit Holder and a country with a higher level of risk. Prospective Unit Holders from high-risk countries without prior relation to the Fund / Fund Manager will be refused. ▪ Sanctions: See sanctions under Unit Holders' risk. ▪ Money laundering: Information about the Unit Holder's address, nationality, and IBAN is collected. If this information suggests a heightened risk, an enhanced investigation will be conducted. ▪ Terrorist financing: See terrorist financing under Unit Holder's risk. Further action will be triggered if suspicious or unusual requests are made by a Unit Holder, such as a request to transfer funds to a third party.

Risk factor	Description	Assessment	Risk Weighting
Financial risk	The financial risk includes an evaluation of the Unit Holder's (expected) subscription amount, as well as the (expected) frequency of subscriptions and redemptions.	The Fund is primarily intended as a long-term investment, resulting in minimal (expected) subscriptions and redemptions. In cases where a subscription amount exceeds a certain threshold or the source of funds is not adequately explained, the Fund will request additional documentation to verify the transfer to Legal Owner.	▪ The risk weighting is considered low as the turnover of subscriptions and redemptions is minimal. ▪ A minimum deposit of EUR 100,000 is required to subscribe to the Fund. For subscriptions exceeding EUR 100,000 with an unexplained source of funds, additional documentation will be requested. ▪ Sanctions: See sanctions under Unit Holder's risk. ▪ Money laundering: Each Unit Holder is required to declare the source of their funds used to invest in the Fund. This information, along with other data such as profession and expected deposit frequency, is included in the Unit Holder's profile. If the source of funds is not satisfactory or a relatively high deposit is made, a more thorough investigation will be conducted. If the frequency of subscriptions or redemptions raises suspicion, an intensive investigation is also carried out. ▪ Terrorist financing: See terrorist financing under Unit Holder's risk. The expected frequency of redemptions is requested, and if the frequency raises concerns initially or during the investment term, an enhanced investigation is conducted.

Risk factor	Description	Assessment	Risk Weighting
Delivery channel risk	To assess the delivery channel risk, an evaluation will be performed to determine whether any intermediaries (domestic or foreign) were involved and whether the contact occurred through physical or digital means.	Each Unit Holder can subscribe digitally. The Fund accepts only subscriptions from Unit Holders who are known to the Fund Manager or have been met in person or via Teams. The Fund does not allow subscriptions through intermediaries. Besides, if a prospective Unit Holder is unknown, a digital or physical meeting will be arranged before the Unit Holder can subscribe to the Fund.	▪ The risk weighting is low as the Fund Manager has a selected group of investors whom Fund Manager knows well (at least the most of them), identified through physical or virtual meetings. ▪ Each Unit Holder must provide valid proof of identity to the Fund, and subscriptions via intermediaries are not accepted. ▪ Sanctions: See sanctions under Unit Holder's risk. ▪ Money laundering: See money laundering under Unit Holder's risk. An independent Administrator monitors all relations, strengthening the integrity of the Fund Manager and reducing the risk of money laundering. ▪ Terrorist financing: See terrorist financing under Unit Holder's risk. An independent Administrator monitors all relations, strengthening the integrity of the Fund Manager and reducing the risk of money laundering.
Product risk	This concerns the risks that arise from Fund Manager's investment policy, which may include investing in higher risk products such as real estate, and the product offered (in this case the Fund).	The Fund invests in Digital Assets. This asset class has an increased risk on AML perspective. In the case of other investments, the associated Product Risk is reassessed.	▪ The risk weighting is considered high due to asset class of Digital Assets. ▪ The Fund invests only in Digital Assets and derivatives. This means that the Fund conducts extensive due diligence on all Unit Holders. This check is particularly focused on the origin of the subscription amount and may also be intensified in other areas based on the outcome of the other risk factors. ▪ Sanctions: See sanctions under Unit Holder's risk. ▪ Money laundering: See money laundering under Unit Holder's risk. The Fund only invests in Digital Assets and derivatives with sufficient liquidity which enables realistic valuation. Moreover, Fund Manager determines the investment policy on which a Unit Holder has no influence. ▪ Terrorist financing: See terrorist financing under Unit Holder's risk. The Fund only invests in Digital Assets and derivatives with sufficient liquidity which enables realistic valuation. Moreover, Fund Manager determines the policy on which a Unit Holder has no influence. This situation is not ideal for terrorist financing.

2.3.2 Overall Risk

After assessing the risks, it is expected that the likelihood of money laundering, terrorist financing and sanctions violations is High due to the following aspect:

- Product risk is classified as High since the Fund invests in Digital Assets.

This means that the Fund performs enhanced CDD on each Unit Holder. The process is further explained in the coming sections. In case a relation does not want to cooperate with an enhanced CDD, a relationship they are refused to participate in the Fund and/or collaboration.

2.4 Risk Appetite

2.4.1 Introduction

Fund Manager aims to conduct business operations with integrity and comply with the laws and regulations arising from the Wwft and Sanctions Act.

An unambiguous policy is implemented to ensure that Fund Manager adheres to ethical business practices and complies with the AML/CFT and sanctions laws and regulations. To achieve this, many activities are delegated to an independent Administrator.

The Fund will have high risk relationships due to the Product Risk. It therefore requires the same initial information from every part and enhanced CDD is conducted. Additional increasing risk circumstances may include a Unit Holder:

- having an unnecessarily complex and/or unexplainable structure;
- being a resident in or national of a grey listed country as listed in Appendix 2.
- having no connection with Fund Manager or the country where the Fund is based;
- making a deposit without a clear explanation of the source of funds; and
- having unusual subscription or redemption patterns that do not match the Unit Holder's profile.

If a relation refuses to cooperate with the enhanced CDD process, access to the Fund will be denied access and/or no collaboration will be initiated.

2.4.2 Money Laundering and Terrorist Financing

When requesting the information, a unified process applies. The information and background of underlying individuals or entities are also verified. Money laundering and terrorist financing often involve the use of all kinds of constructions to conceal the true source or destination of the funds (or other values). The investment institution intends to identify the ultimate beneficial owner (hereinafter referred to as "UBO") at all times to draw a correct picture and a good understanding of a transaction.

After conducting the investigation, a risk profile is determined. In this case, that is high or unacceptable (because of product risk). The Fund then continuously assesses whether the situation and the risk profile of the relationship have changed since acceptance. This is also done through transaction monitoring, which detects any unusual transaction patterns based on an analysis of Unit Holder's data. The Fund considers a comprehensive understanding of the Unit Holder's situations necessary to detect any potential anomalies in their (transactional) behavior.

2.4.3 Sanctions

The Fund is commited to avoiding any relationships with individuals or entities on sanction lists. The initial CDD process, which includes identifying relevant (natural) persons and sanctions screening, is designed to to prevent such relationships being established. However, it is possible for an individual or entity to end up on a sanction list at a later date. The sanctions screening is updated daily, so immediate action can be taken if necessary to terminate any relationships with sanctioned individuals or entities.

2.4.4 Delegation

Fund Manager has a relatively small size and has therefore opted to delegate the AML/CFT and Sanctions activities, including continuous sanctions screening and transaction monitoring. In order to achieve the desired level of CDD, Fund Manager has assigned an independent Administrator to perform these operational activities.

Despite the delegation, Fund Manager remtains responsible for complying with the Wwft and the Sanctions Act, and therefore, will periodically review the performed activities on a Unit Holder level, and due diligence processes.

2.5 Evaluation

Fund Manager and Administrator hold annual meetings to discuss the Policy, procedures, Unit Holders' files, fund characteristics and risk appetite. The risk assessment is also updated annually. If there are changes in the Fund's characteristics, the Unit Holders, or investments, this may affect the AML/CFT and sanctions procedures.

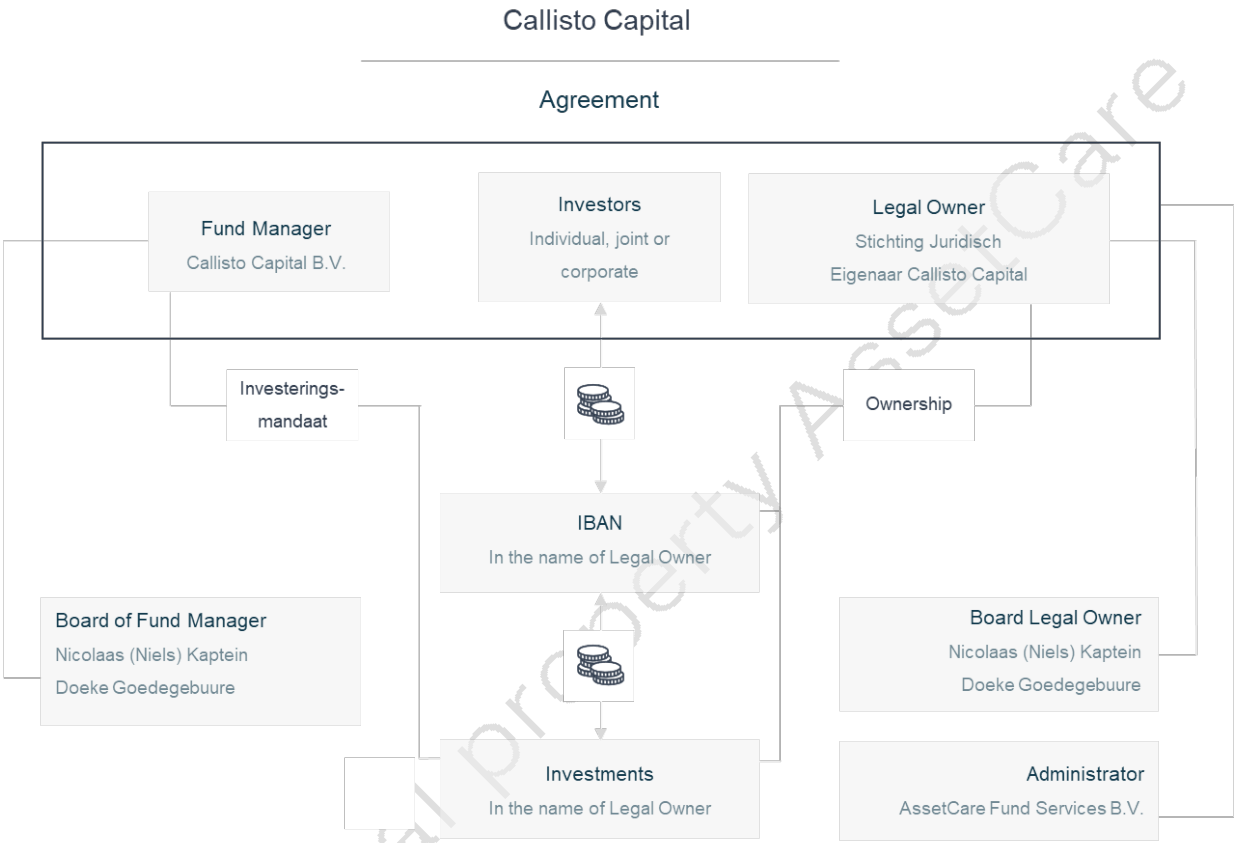
In addition, Fund Manager monitors Administrator performance of delegated activities to ensure they are carried out completely and correctly.

3 Roles and responsibilities

3.1 Structure of the Fund

The structure of the Fund is shown graphically in Figure 1. The following paragraphs provide an explanation of the roles and responsibilities of each party involved, as well al the Fund's relationship with the Unit Holders.

Figure 1: Structure overview of the Fund



3.2 Fund Manager

Callisto Capital B.V., a private limited liability company, is the initiator and sole manager of the Fund. Fund Manager is established at Franklinstraat 7, 5807 GJ, Venray, the Netherlands and is registered with the Chamber of Commerce under number 89924169. The board of Fund Manager is formed by D. (Doeke) Goedegebuure and N. (Nicolaas) Kaptein.

The board of Fund Manager is responsible for this Wwft and Sanctions Act policy, which includes the following responsibilities and activities:

- Approving the initial policy during establishement and regularly evaluating its effectiveness, correctness and completeness;
- Iimplementing relevant laws, regulations and administrative provisions in the Policy;
- Ensuring timely and adequate performance of all activities described in this Policy;
- Guaranteeing the further training and awareness of relevant persons;
- Strictly enforcing this Policy, with any exceptions requiring approval from the board; and
- Ensuring confidentiality and preventing the unlawful sharing and/or use of this Policy by third parties.

Stability, transparency, reliability and integrity are at the core of Fund Manager's activities.

3.3 Administrator

AssetCare Fund Services B.V. (hereinafter referred to as "Administrator") is responsible for conducting the administration of the Fund based on a Cooperation Agreement with Fund Manager as of the 6 July 2023. Administrator periodically calculates the Fund's value and communicates it to both the Unit Holders and Fund Manager. Additionally, Administrator maintains a Unit Holder Register and monitors both existing and future investors in compliance with this Wwft and Sanctions Act policy. Finally, Administrator submits the relevant reports to the supervisory authorities.

The Administrator carries out the following list of AML/CFT and sanctions-related activities::

- Conducting a risk-based CDD and collecting the relevant documentation and information to establish a risk classification for each Unit Holder;
- Recording and keeping information and documentation resulting from the CDD up to date;
- Taking appropriate actions upon identification of a risk increase;
- Processing the subscriptions, redemptions and any other changes (such as address changes) of Unit Holders;
- Preparing reports on unusual and suspicious transactions to the FIU in consultation with Fund Manager, who is responsible for submitting the report;
- Reporting any breach of this Policy to Fund Manager and taking appropriate measures in consultation with Fund Manager;
- Reporting to the supervisors for the Fund. In case this is not possible, filling reports based on known data and sharing them with Fund Manager.

When performing its activities, Administrator adheres to the following principles:

- Administrator is committed to full compliance with all applicable laws and regulations and conducts its business in accordance with the highest ethical standards. This means that Administrator does not enter into business relationships with entities and individuals that may adversely affect its reputation;
- Administrator does not rely on the CDD of third parties;
- The employees of Administrator carefully assess the intentions and circumstances of all Unit Holders and the associated natural and legal persons;
- Administrator ensures that all provisions contained in the Policy are known by each employee;
- Administrator expects that Fund Manager periodically reviews the activities performed by Administrator;
- Administrator requires an approval of Fund Manager before a high risk Unit Holder can be accepted;
- Administrator expects Fund Manager to be aware of the Policy.

3.4 Unit Holders

The Fund accepts subscriptions from individuals, private companies and other type of entities. The are two types of relationships that can be established with a Unit Holder:

- Direct relationship: a Unit Holder subscribes directly to the Fund, and the funds are transferred directly from the Unit Holder to the legal entity.
- Indirect relationship: a Unit Holder subscribes to the Fund trough an intermediary (e.g. through an asset manager).

To maintain control over which Unit Holders subscribe to the Fund and increase transparency, Fund Manager only accepts Unit Holders who enter through a direct relationship. This eliminates the need for additional procedures for indirect relationships.

3.5 Legal owner

The legal owner of the Fund is Stichting Juridisch Eigenaar Callisto Capital. This entity holds and acquires all assets owned by the Fund, but the risks and benefits of these assets accrue to the Unit Holders. Legal Owner is registered as a foundation with the Chamber of Commerce under number 89930436 and its board determines the daily policy.

Legal Owner serves to separate the Unit Holder's funds from Fund Manager's funds. Unit Holders transfer their funds to Legal Owner's bank account. These funds can only be transferred to the bank and/or exchange where the assets are managed, or refunded to the Unit Holder's bank account.

The board of Legal Owner, in this case D. (Doeke) Goedegebuure and N. (Nicolaas) Kaptein, preserves the Unit Holders' interests and monitors Fund Manager compliance with the investment policy, as well as the proper transfer of funds.

3.6 Bank/exchanges

To safegaurd and manage cash and Digital Assets and execute transactions, Legal Owner maintain accounts with one or more banks and exchanges:

Type	Name
Bank	Neo Payment factory SL
Exchange	Bybit
Exchange	Amdax
Exchange	Crypto.com
Exchange	Deribit

Banks and exchanges are also bound by the Wwft and must comply with CDD obligations. To obain a better understanding of the Fund's Unit Holders, banks and/or exchanges may request one of the following:

- AML Comfort Letter: A formal document that aims to provide assurance to the receiving party that the Fund is in compliance with their AML obligations.

- Sharing CDD: If a bank or exchange cannot rely on an AML Comfort Letter, they may require separate analysis of each Unit Holder. Sharing the Unit Holder Register and information/documentation per Unit Holder may be necessary.
- Audits: Banks or exchanges can conduct audits (spot-checks on site) to verify the completeness of the CDD activities.

3.7 Training

To ensure the correct implementation of this Policy and raise awareness among employees and parties involved, Fund Manager and Administrator have implemented the following measures:

- All involved parties are required to sign a confirmation form, confirming that they have read, understood and will comply with the Policy;
- An annual session is organized to discuss the Policy, highlight cases, identify risks, discuss how to recognize unusual or suspicious activity, and answer questions. Fund Manager is responsible for initiating this session;
- All involved parties are kept informed of significant changes in applicable laws, regulations and policies;
- Persons involved in CDD are subscribed to the AFM & De Nederlandsche Bank's (hereinafter referred to "DNB") sanctions warning to stay informed of changes in existing sanctions rules;
- The prevention of money laundering and terrorist financing is on the agenda of Fund Manager and Administrator's annual board meetings.

Creating a compliance culture is crucial for successful implementation and operation of the Policy. This is achieved by clear communication that emphasizes the need to control risks before establishing or maintaining relationships.

The staff of Administrator is required to undergo training courses as prescribed by the Wwft at least once a year to ensure sufficient knowledge and understanding of the regulations. This training also enables them to recognize unusual transactions and integrity risks, and perform their first-line tasks related to the Wwft.

3.8 Audit

To ensure that the Wwft and Sanctions Act policy comply with the regulations, the Policy is periodically reviewed and adjusted if necessary. Fund Manager seeks external advice on the latest developments concerning the Policy to ensure that it continues to meet the requirements of the laws and regulations.

4 CDD

4.1 Instruction

The purpose of CDD is to evaluate the risks of money laundering, terrorist financing, and sanctions violations. Fund Manager will perform CDD under the following circumstances, as stated in Article 3 of the Wwft:

- When a business relationship is established.
- When a business relationship has already been established and the information needs to be updated based on policy or due to unusual or suspicious transactions;
- When there are indications that the relevant party (and/or related party) is involved in money laundering or terrorist financing;
- When there are doubts about the accuracy or completeness of previously obtained data of the relevant party (and/or related party);
- When there is an increased risk of money laundering or terrorist financing due to the relevant party's (and/or related party's) country of residency, establishment or registered office.

The CDD process consists of three phases:

Phase 1	Phase 2	Phase 3
Determining the inherent risk	Assessing the internal control environment	Deriving the residual risk

If the required information cannot be obtained to complete the CDD process, it may be decided not to establish or continue a business relationship. Furthermore, any suspicious transactions will be reported to the FIU.

4.1.1 Inherent risks

The Fund assesses inherent risks using risk factors derived from legal guidelines that incorporate both qualitative and quantitative criteria. These risk factors represent the underlying causes or circumstances in which the Fund may be used for financial crime purposes. Inherent risk is the exposure to money laundering, terorrist financing or sanctions violations without any control environment.

A risk-based approach is used to determine the inherent risk. The Fund assigns each risk factor a classification indicating the risk level and prevalence compared to other risk factors. The classifications include 'low', 'medium', 'high' or 'unacceptable'. Failure to manage the risk factors can lead to reputational risks, regulatory or legal sanctions and financial sanctions.

4.1.2 Control environment

The Fund creates an overall risk profile based on the various risk factors examined during the CDD. This profile determines the level and frequency of monitoring and is the basis for entering into, continuing or terminating a business relationship.

4.1.3 Residual risks

The assessment of residual risk is based on inherent risks and helps to determine the appropriate risk mitigation measures. The residual risk must align with the Fund Manager's risk appetite.

A (potential) Unit Holder with an 'unacceptable' risk classification will not be accepted. For Unit Holders with a 'high' risk rating, Fund Manager will evaluate on a case-by-case basis whether or not to accept them. Finally, there is always the right to refuse Unit Holders, or to terminate the relationship.

4.2 Risk factors

The Unit Holder's risk profile is based on various risk factors:

Risk factor	Description
Unit Holder's risk	To assess the risk at the Unit Holder's level, factors such as their legal and organizational structure, sanction and PEP lists, negative media coverage, and their profession and work sector are taken into consideration.
Geographical risk	The countries relevant to the Unit Holder, such as their nationality or country of residence, are analyzed as certain countries may lead to increased risk.
Financial risk	The financial risk is evaluated to determine the risk of the Unit Holder's source of funds and to define a transaction profile.
Delivery channel risk	The way in which the Unit Holder came into contact with Fund Manager and/or the Fund is analyzed to determine any potential risks.
Product risk	This factor considers the risk associated with the Fund, such as risks arising from the Fund Manager's investment policy.

Each risk factors is initially classified as 'low', 'medium', 'high' or 'unacceptable', which is then used to assign an overall risk classification.

Risk classification	Unit Holder's risk	Geographical risk	Financial risk	Delivery channel risk	Product risk

4.2.1 Unit Holder's risk

4.2.1.1 Definition

A Unit Holder can be an individual, private company, or other entity. When assessing individuals, their background, profession, negative media mentions, and inclusion of PEP and sanction lists are considered. For entities, the individual and other legal persons involved, UBO(s), and transparency of the structure are evaluated.

The following categories are used to identify aspects of Unit Holder risk:

- Individuals (e.g. UBO(s)):
  - Profession and sector;
  - Possible decision-making role of the individual;
  - Negative media attention;
  - Listed on a PEP or sanction list.
- Legal entities (e.g. private limited company):
  - Type;
  - Organizational structure;
  - Number of layers in the organizational structure;
  - Involvement of a 'Corporate Service Provider';
  - Negative media attention in the name of entity;
  - Negative media attention in the name of the shareholder(s) and/or director(s);
  - Inclusion of any shareholders and/or director(s) on a PEP or sanctions list;
  - Sector in which the entity performs its activities;
  - Statutory seat of the entity in relation to the country of residence of the UBO(s);
  - Frequency of change in the management, shareholders and statutory seat of the entity;
  - Unreasonable or unexplained relationships with other entities.

4.2.1.2 Type of Unit Holder

The assessment considers if a particular type of Unit Holder poses a higher risk and how the mitigating measures could impact the evaluation. This categorization can be based on the Unit Holder's profession, behavior, or activities.

The following factors contribute to a higher risk:

Activity	Risk weighting		
	Medium	High	Unacceptable
The inclusion of the Unit Holder or any other relevant (natural or legal) person on a sanction list			✓
Status of a PEP of the Unit Holder or any other relevant (natural or legal) person		✓	
The Unit Holder or any other relevant (natural or legal) person have received negative media attention	✓ (not related to money laundering or terrorism)		✓ (related to money laundering or terrorism)
Possible involvement in criminal activities of the Unit Holder or any other relevant (natural or legal) person and/or their transactions			✓
Involvement in or receipt of income from a cash-intensive sector that is considered high-risk of the Unit Holder or any other relevant (natural or legal) person	✓ (no decision-making role)	✓ (decision-making role)	
Non-cooperation or incomplete cooperation with the completion of CDD by the Unit Holder or any other relevant (natural or legal) person			✓

Enhanced CDD is typically carried out for Unit Holders with a medium or high risk level, based on their risk assessment. The CDD Manual of Administrator outlines the procedures for conducting enhanced investigations.

4.2.1.3 UBO and Pseudo-UBO

4.2.1.3.1 Definition

UBO refers to the ultimate beneficial owner of a legal entity or company, who is always a natural person and holds a direct or indirect 25% or more interest in (the assets of) the organization. The following are examples of how this interest can be obtained:

- A direct interest in shares or depositary receipts.
- Indirect stakeholders who own or control 25% or more of the:
  - voting rights in the general meeting;
  - interest as a beneficiary of the assets;
  - special control over the assets;
  - right to a share in the community;
  - right to a share in the profits;
  - voting rights in the decision-making on amending the partnership agreement;
  - voting rights in the decision-making on important decisions implementing the partnership agreement;
  - actual control.

In the absence of a UBO, one or more pseudo-UBOs can be designated, who belong to senior management and have effective control.

Failure to obtain adequate, accurate, and timely data about UBO(s) can increase the risk of money laundering and terrorist financing as it makes it difficult to identify:

- the true purpose of the subscription;
- the ownership of an entity;
- the source of the funds related to the entity;
- the identity of known or suspected criminals.

Non-cooperation or incomplete cooperation of a Unit Holder to identify its UBO(s) can lead to non-acceptance of the Unit Holder or termination in case of an existing Unit Holder.

4.2.1.3.2 Application by entity

The application of UBO and Pseudo-UBO per entity is described in Article 3 of the Wwft Implementation Decree 2018. The most common structures are outlined below:

Private limited company (B.V.) or public limited company (N.V.)	
UBO	Any natural person: ▪ with a direct or indirect interest of more than 25% of the shares, voting rights or ownership interest, including the holding of bearer shares; or ▪ who can exercise actual control in another way (is the ultimate policymaker).
Pseudo-UBO	Any statutory director. If a statutory director is a legal person, this concerns any natural person who is a direct or indirect director under the articles of association.

Foundation, association, mutual insurance institution and cooperative	
UBO	Any natural person: ▪ with a direct or indirect interest of more than 25% of the ownership; ▪ with directly or indirectly more than 25% of the votes in the event of an amendment to the articles of association; or ▪ who can exercise actual control in another way (is the ultimate policymaker).
Pseudo-UBO	Any statutory director. If a statutory director is a legal person, this concerns any natural person who is a direct or indirect director under the articles of association.

General partnership, partnership, limited partnership and shipping company

UBO	Any natural person: ▪ with a direct or indirect interest of more than 25% of the ownership interest; ▪ with directly or indirectly more than 25% of the voting rights in the event of an amendment to the cooperation agreement; ▪ with directly or indirectly more than 25% of the voting rights in the implementation of the cooperation agreement (other than through acts of management); or ▪ who can exercise actual control in another way (is the ultimate policymaker).
Pseudo-UBO	Any partner, with the exception of limited partners (also known as silent partners) in a limited partnership. If a partner is a legal entity, this concerns any natural person who is a direct or indirect director under the articles of association.

4.2.1.4 Organizational structure

To gain a comprehensive understanding of all pertinent stakeholders, the complete organizational structure of a Unit Holder is charted. If the structure and/or UBO(s) are not evident, it can pose a higher risk of money laundering and/or terrorist financing.

The following factors lead to increased risk:	Risk weighting		
Activity	Medium	High	Unacceptable
Non-transparent ownership structure, which includes at least three layers.		✓	
Legal entities primarily incorporated in the form of 'bearer shares'., which is prohibited in most European countries.			✓
Shell companies (which can be established with different forms of ownership structure and especially in cases where there is ownership and/or activity in different jurisdictions);			✓
Frequent changes in governance;		✓	
Informally appointed shareholders and directors, such as family and close associates, who lack the necessary knowledge to perform their function;	✓		
Trusts and other legal arrangements that enable the separation of legal and beneficial ownership of assets;		✓	
Use of intermediaries, including professional intermediaries, in the formation of legal entities.	✓		

When a Unit Holder is deemed to have medium or high risk, Administrator usually conducts additional investigations tailored to the level of risk. The enhanced CDD procedures are outlined in the CDD Manual of Administrator.

4.2.1.5 Industry and sector

The sector/industry in which a Unit Holder operates is only one of the factors that should be considered in determining the Unit Holder risk. The risk classification is tailored to individual Unit Holders, taking into account their specific roles, responsibilities, and decision-making authority. As such, it is not a one-size-fits-all approach and may vary depending on the nature of the job performed within the relevant sector.

The table below shows those industries that carry a higher risk. The risks of each industry are briefly explained. For each case, a consideration should be made whether the Unit Holder operates in a risk-increasing sector and how this manifests itself.

Industry/Sector	Explanation
Art dealers, auctioneers and trade in luxury/valuable products	The art trade and trade in luxury/valuable items is attractive to money laundering in a number of ways. The identity of the buyer or seller is rarely recorded. The price of goods depends on many factors and is therefore difficult to control. This makes it attractive to convert illegally obtained money into art or luxury/valuable products. Products like gold, precious stones, leather/fur, antiques and art fall under this category.
Cash-intensive retail business (hospitality, pawn shops, personal care, car dealers, etc.)	Industries where a lot of cash is used are more susceptible to money laundering. In these industries, illegally obtained money can be easily converted to legal money. The sectors below may fall under the cash intensive sector. This list is not exhaustive: ▪ Hospitality (restaurants, cafes, bars are often cash-intensive due to frequent transactions with customers) ▪ Retail (Smaller shops, such as convenience stores. Market stalls and craft shops, can handle a lot of cash transactions) ▪ Personal services (Service providers such as hairdressers, beauticians, masseurs and personal trainers can receive cash payments) ▪ Tourism (Small tourism businesses, such as local guides, souvenir shops and small eateries, may prefer cash payments. ▪ Car dealers and metal/scrap trade (both scrap dealers and car dealers often deal with local transactions and direct interaction with customers. In such cases, customers may prefer cash payments. These traders are often involved in the buying and selling of used goods, such as scrap metal or used cars. In these sectors, the tendency towards cash transactions is sometimes stronger, especially for private sales.
Charities, non-profit organizations, religious institutions and crowdfunding	These types of organizations often handle cash flows from (anonymous) donations, grants and other sources. This can pose a risk if it is not clear where the money comes from and where it goes. In addition, some organizations operate internationally, especially in regions with increased risks of money laundering and terrorist financing (high risk countries) and may lack transparency about the source of funding or the purpose of the campaign.
Coffee shops, grow shops	Coffee and grow shops may include risks such as cash transaction processing, customer anonymity, international customer base and the potential for money laundering given the nature of the goods sold (such as cannabis-related products and growing material).
Commodities, minerals, mining	The combination of factors such as the complexity of transactions, global nature of operations, cash-intensive activities, use of shell companies, corruption risks, and environmental and social issues contribute to the perception of the commodities, minerals, and mining industry as higher risk.

Industry/Sector	Explanation
Construction	The construction industry is known for often having large amounts of cash in circulation. There may also be dirty money or possible bribes to secure large projects, which is especially applicable to smaller job companies (such as painters, plasterers, garden contractors) that can take on jobs they do not declare.
Digital Assets	The combination of pseudonymity, cross-border transactions, lack of centralized regulation, privacy features, rapid innovation, and association with illicit activities contributes to the higher risk of the digital assets industry.
Gambling and gaming (casino, arcades, poker, etc.)	Casinos and gambling establishments often handle large amounts of cash, which can be used to 'launder' illegally obtained money. The nature of activities in this sector, such as exchanging chips for cash and placing large bets, makes it difficult to trace the source of the money. With the rise of online gambling, new challenges have emerged, including the fact that customers can conduct transactions from different locations and with different currencies, making it more difficult to identify and track suspicious activity.
Military goods/defense	Due to the nature of military goods and defense activities, there is a risk that criminals could use this sector to finance or support illegal activities, such as arms trafficking, terrorist financing or circumventing international sanctions. Trade in military goods and defense activities often involves cross-border transactions and cooperation with international partners. This can increase the risk that transactions are used to launder or move money between different countries and jurisdictions.
Oil, gas, energy, offshore & dredging	These sectors are often involved in large investments, projects and transactions involving significant financial resources. This can lead to complex financial structures and transactions that make it difficult to trace the origin and destination of money flows, increasing the risk of money laundering. As these sectors often deal with environmental and regulatory issues, they may also be exposed to risks related to money laundering of money obtained from environmental crimes, such as illegal waste dumping or violations of environmental regulations.
Pharmaceutical industry	The pharmaceutical industry includes the production, distribution and sale of drugs and other medical products, involving large financial interests. This can attract criminals who try to commit illegal activities, such as falsifying drugs, illegally selling prescription drugs or trafficking stolen drugs.
Professional sports	Corruption and match-fixing can have serious consequences for the integrity of professional sports. Gambling on sports matches can be used as a means of laundering illicit funds. In addition, players can gamble on their own matches for financial gain. Besides, sports brokers, agents and intermediaries can be used to carry out transactions or manage money flows in the professional sports world. This can make it more difficult to identify the ultimate beneficiaries of financial transactions and increase the risk of money laundering.
Real estate exploitation and development (domestic and/or foreign)	Business real estate activities, by their nature, have a higher risk of fraud and money laundering, due to the relatively high value of real estate properties, the often non-transparent pricing and the complexity of transactions
Relaxation businesses, prostitution, adult industry (incl. internet)	These industries often have a significant amount of cash transactions, which increases the risk of hiding illicit income. Individuals working in the prostitution or adult industry, including online, may

Industry/Sector	Explanation
	use fake identities to disguise their activities. Many businesses in these industries may operate under the radar, without full disclosure of their activities.
Target companies managed/administered by trust companies or trust offices	Trust companies and firms are often used to set up complex legal structures that can disguise ownership mixes and transaction flows. This can make it difficult to identify the ultimate beneficiaries of a business or transaction, increasing the risk of money laundering.

The table below provides insights into various events as regards to the client risk factor that require mitigating measures and outlines the probable measures that will likely be implemented. However, the specific measures depend on the information already available and the complete profile of the Unit Holder.

Note: it is also likely that further measures will be implemented regarding the source of funds (alongside the follow-up questions for the various sources outlined under "Financial risk") as it is optional to request documentation when the risk is classified as medium (risk-based) and mandatory when the risk is classified as high. Moreover, the assessment may involve considering a combination of events.

Event	Potential mitigating measures
Natural persons	
Unit Holder is active in a higher risk sector (e.g. cash intensive sector), but doesn't have a decision-making role	▪ Conduct additional due diligence to clarify the company, nature of the company, sector, and business activities. ▪ Review and verify the legitimacy of the Unit Holder's source of funds. – If a Unit Holder operates in a cash-intensive sector without a decision-making role, documentation is optional as the risk is considered medium. Only when there is insufficient information to plausibly determine the Unit Holder's source of wealth should they provide documentation to support their statements. ▪ If risks associated with the sector are deemed significant, consider escalating the risk level to high or imposing restrictions on the relationship.
Unit Holder is active in a higher risk sector (e.g. cash intensive sector) and has a decision-making role (someone who has influence on the decision-making within a company, such as board members, directors and shareholders).	▪ Conduct additional due diligence to clarify the company, nature of the company, sector, activities, and Unit Holder's specific decision-making responsibilities within the organization. ▪ Review and verify the legitimacy of the Unit Holder's source of funds. – If a Unit Holder operates in a cash-intensive sector and has a decision-making role, there is always a high risk. Therefore, the Unit Holder should provide documentation to support their statements regarding the source of their wealth. ▪ If risks associated with the sector are deemed significant, consider restricting the relationship.
Unit Holder (or relevant subject) is a sanctioned	▪ Sanctioned (natural or legal) persons pose an unacceptable risk
Legal entity	
Unit Holder has a non-transparent ownership structure or consists of more than three layers (excluding the UBO)	▪ If the organizational structure of the Unit Holder is non-transparent (e.g., a foundation or association) or comprises more than three layers (excluding the UBO), the risk is deemed high. The determination of the number of layers starts with the Unit Holder. ▪ Assess the rationale for the using such an ownership structure, such as obtaining a more detailed breakdown of the ownership structure, identifying any intermediary entities and understanding the complexity of the ownership structure should be provided.

Event	Potential mitigating measures
	▪ If risks associated with the sector are deemed significant, consider restricting the relationship.
Unit Holder is active in a higher risk sector (e.g. cash intensive sector)	▪ Conduct additional due diligence to clarify the company, nature of the company, sector, and activities within the organization. ▪ Review and verify the legitimacy of the Unit Holder's source of funds. – The legal entity has per definition a decision-making role, and so there is a high risk. Therefore, the Unit Holder should provide documentation to support their statements regarding the source of their wealth. ▪ If risks associated with the sector are deemed significant, consider restricting the relationship.
Unit Holder has 'bearer shares' or is a shell company	▪ This poses an unacceptable risk.
Frequent change in the management, shareholders and statutory seat	▪ Assess the reasons for frequent changes and investigate any potential risks. Besides, it is important to monitor and review changes in management, shareholders, and statutory seat. ▪ If risks associated with the frequent changes are deemed significant, consider restricting the relationship.
Unit Holder has informally appointed shareholders and directors (such as family) that don't have the required knowledge	▪ Assess the rationale for the appointment of the shareholders and/or directors, such as the reason that the shareholders and/or directors are appointed, the specific roles the informally appointed shareholders and directors play in the Unit Holder's operations and how the lack of required knowledge is addressed within the organization. ▪ If risks associated with the informally appointed shareholders are deemed significant, consider increasing the risk level or restricting the relationship.
Unit Holder uses trusts other legal arrangements that allow separation of legal ownership and beneficial ownership of assets	▪ Assess the rationale for the using such arrangements in the organizational structure, such as the purpose of using trusts or similar arrangements and how the Unit Holder ensures transparency within the structure. ▪ If risks associated with the usage of trusts and other legal arrangements are deemed significant, consider restricting the relationship.
Unit Holder uses intermediaries in the formation of legal entities, including professional intermediaries.	▪ Assess the rationale for the using such intermediaries in the organizational structure, such as the purpose of using intermediaries, the details on the role and selection criteria for intermediaries should be provided. ▪ If risks associated with the intermediaries are deemed significant, consider restricting the relationship.
Stationary seat deviates from UBO(s) residence	▪ Assess the rationale for the deviation in the stationary seat from the UBO(s) residence as this is seen as high risk. This contains collecting the factors that contribute to the deviation between the stationary seat and UBO(s) residence are considered. ▪ If risks associated with the deviation are deemed significant, consider increasing the risk level or restricting the relationship.
Unreasonable or unexplained relationships with other entities	▪ Assess relationships with other entities that are deemed unreasonable or unexplained. ▪ Request additional information or documentation to clarify the nature of relationships with entities that are considered unreasonable or unexplained. ▪ If risks associated with adverse media or any other hits are deemed significant, consider increasing the risk level or restricting the relationship.

4.2.1.6 Sanctions

Sanctions are political instruments in foreign and security policy by institutions like the United Nations and the European Union. With regard to financial transactions, the AFM and DNB are responsible for ensuring compliance with the Sanctions Act 1977, which requires institutions to have measures in place to monitor if any of their relations are listed on sanction lists. Sanctions are implemented in response to violations of international law, human rights, or when legal or democratic principles are not respected. Sanctions are also critical in the fight against terrorism.

Common types of sanctions include:

- trade restrictions;
- arms embargoes:
- travel restrictions; and
- visa restrictions.

Sanctions screening is used to detect, prevent, and disrupt financial crime, especially the risk of sanctions. The Fund Manager's data, including the Unit Holder's data, is compared with lists of names and other indicators of sanctioned parties or locations to detect potential risks.

If a Unit Holder or any other relevant natural or legal person involved is found to correspond to a "Hit" on the sanctions lists, Administrator reviews the situation and takes necessary action (see Section 6.2). This may include terminating the business relationship or not accepting the Unit Holder.

More information regarding the screening process is available in Section 5.9.7.

4.2.1.7 Media

Unit Holders and related parties are screened for negative media publicity using tools such as “Handelzeker” and Google searches. In case a potential risk is identified, a higher risk classification may be assigned and stricter measures in the context of CDD may be applied.

Examples of such measures include:

- Gathering additional information for CDD, such as statements on negative publicity, information on past and current business activities, and sources of income of the Unit Holder or UBO(s)
- Increasing the frequency of periodic reviews and conducting more thorough transaction monitoring.

4.2.1.8 PEP

4.2.1.8.1 Description

A PEP is an individuals who holds a public office or position of political influence. Such individuals may present higher risks due to their potential to abuse their power and influence for personal gain or the gain of their close relatives and close associates. If a Unit Holder or a related (legal) person is identified as a PEP, Administrator typically assigns a higher risk classification to the Unit Holder.

4.2.1.8.2 Increase in risk classification

When determining the risk classification of a Unit Holder who is identified as a PEP, the following factors are taken into consideration:

- The political and legal system of the country concerned;
- Vulnerability to corruption based on publicly available independent sources;
- The official responsibilities of the individual's function;
- The nature of the title, where honorary or remunerated;
- The level of authority the individual holds over government activities and other officials;
- Whether the individual has access to significant government assets, funds or the ability to direct the award of public contracts or other contracts;
- Whether the individual has links to an industry that is particularly susceptible to corruption.

After conducting a risk assessment on the PEP, Administrator applies a risk-based CDD procedure that includes the following components:

- Explaining the duration, title or position and country in which the PEP has political exposure. If the individual is a close family member or associate of the PEP, their relationship must be documented as well.
- Explaining the nature and intended purpose of the relationship, the source of the funds, and the expected levels of activity.
- Explaining the sources of funds and wealth (e.g. salary, compensation from official duties, and assets from other sources). If the risks associated with financial crime are high or if there is uncertainty regarding the accuracy of the information provided, Administrator will verify this information using independent and reliable sources. To establish or verify this information, Administrator may use internet and media searches, taking into account the potential limitations of such sources.

4.2.1.8.3 Characteristics of PEP status

Characteristics of specific higher public functions, as listed below, may be useful as indicators of seniority, prominence or importance and are used to determine whether a person should be considered a PEP. However, even within these categories, it must be ensured that only those positions that are truly prominent are considered.

Some examples of specific features that are likely to lead to PEP status include:

- Heads of State, Government Leaders and Ministers;
- Senior judicial officers that have seats on bodies whose decisions are not subject to appeal;
- Heads and other senior officials holding senior positions in the armed forces;
- Members of ruling royal families with governmental responsibilities;
- Senior executives of state-owned companies, where the state-owned company has a real economic or political interest;
- Senior officials of major political parties.

4.2.1.8.4 Relationships of PEPs

Relationships of PEPs can pose greater risks due to the potential for these individuals to use their power and influence for personal gain or to benefit their close family members and associates. They may also attempt to conceal misappropriated funds or assets through these relationships, which could be a result of corruption or bribery. Additionally, PEPs may leverage their positions of power to gain access or control over legal bodies for similar purposes. As a result, Administrator may classify relationships of PEPs as high risk and apply more rigorous control measures to better detect and prevent money laundering practices.

Individuals who are considered "close family members" or "close associates" of a PEP should be classified as such. This includes:

- Close family members: This refers to the PEP's spouse, children and their spouses, parents and siblings.
- Close associate: This refers to individuals who are well-known business colleagues or personal advisors of the PEP, especially those who act in a financial fiduciary capacity.

4.2.2 Geographical risk

4.2.2.1 Definition

Determining whether a jurisdiction presents a higher risk of money laundering or terrorist financing is challenging as there is no agreed definition or methodology. However, several factors can be considered as indicators of higher risk, including:

- Countries identified by Administrator's sources (Appendix 2) that provide funding or support for terrorist activities or that have designated terrorist organizations active within their borders;
- Countries identified by Administrator's sources (Appendix 2) as having significant levels of organized crime, corruption, or other criminal activity, including countries that are sources or transit points for illegal drugs, human trafficking, smuggling and illegal gambling;
- Countries identified by Administrator's sources (Appendix 2) that are subject to sanctions, embargoes or similar measures issued by international organizations such as the United Nations;
- Countries identified by Administrator's sources (Appendix 2) that have weak governance, law enforcement and regulatory regimes, including those with weak AML/CFT regimes according to the FATF standards.

These indicators can help financial institutions to identify and manage the risks associated with operating in certain jurisdictions.The Fund must pay special attention to business relationships and transactions with these countries.

4.2.2.2 Types

The following categories are used to classify the geographical risk associated with a Unit Holder:

Category	Description	Result
Black	According to independent sources, these countries pose high risks of money laundering and terrorist financing	Unit Holder may not be accepted.
Grey	According to independent sources, these countries pose average risks in terms of money laundering and terrorist financing	For each case, it is determined whether the Unit Holder is accepted.
White	According to independent sources, these countries pose low risks in terms of money laundering and terrorist financing	Unit Holder is generally accepted.

The following guidelines must be followed regarding geographical risk:

	Risk weighting		
Scenario	Medium	High	Unacceptable
Unit Holders who (I) have the nationality of a black listed country and/or (II) have a bank account in a black listed country			✓
Unit Holders who (I) are residents of a black listed country, but (II) have the nationality of a grey listed or white listed country, and (III) have a bank account in a grey listed or white listed country		✓	
Unit Holders who meet at least two of the following requirements: ▪ have the nationality of a grey listed country; ▪ have a bank account in a grey listed country; ▪ reside in a grey listed country.		✓	
Unit Holders who meet one of the following requirements: ▪ have the nationality of a grey listed country; ▪ have a bank account in a grey listed country; ▪ reside in a grey listed country.	✓		

Unit Holders, who (I) have the nationality of a white listed country, (II) have a bank account in a white listed country and (III) reside in a white listed country are categorized as low geographical risk;

As the Fund is based in the Netherlands, any Unit Holder with (I) nationality and/or (II) bank account and/or (III) residence outside the Netherlands is subject to additional investigation. This includes:

- the reasons for the Unit Holder connections to countries outside the Netherlands;
- their engagement with the Fund / Fund Manager; and
- their intentions for subscribing to the Fund.

Failure to provide sufficient explanations may result in an increase in the geographical risk or denial of acceptance. Section 4.2.2 also acknowledges that a Unit Holder may have links with countries outside the Netherlands due to other factors, in which case additional investigation may be necessary to determine the level of risk.

For Unit Holders with medium or high risk, tailored enhanced due diligence procedures are conducted as outlined in the Administrator's CDD Manual.

4.2.2.3 List of countries

Appendix 2 contains the current list of countries. This list categorizes countries as black listed, grey listed or white listed, and specifies the sources used to determine their classification. This is then used to classify a Unit Holder's geographical risk.

4.2.3 Financial Risk

4.2.3.1 Definition

Determining the Unit Holder's source of funds is critical in assessing whether they are derived from criminal or corrupt practices. This not only applies to the subscrpiption amount, but also to the overall wealth of the investor.

4.2.3.2 Origin of assets and resources

This risk factor is among the most significant aspects of the investigation as it can have a direct link to criminal activity. The investigation will provide insight into the following:

- The Unit Holder's background and financial history;
- How the assets were obtained by Unit Holder;
- The resources used to invest in the Fund;
- The consistency of the Unit Holder's transaction activity with the expected transaction activity;
- Suspicious or unusual activities or transactions;
- Unexplained or incoherent information obtained;
- Adequate documentation to verify the information obtained (if necessary);
- Negative media or facts related to the information;
- The Unit Holder's reputation and integrity;
- The extent to which the source of funds is from a high-risk country.

The following quantitative thresholds are used:

Risk classification	Subscription amount	Documentation
Low	< € 250.000	Unlikely
Medium	€ 250.000 – € 750.000	Likely
High	> € 750.000	Yes

Assessment of this risk follows a risk-based approach that considers factors such as the type of Unit Holder, specific circumstances, and risk classification. The level of information and documentation required to verify the source of funds is based on this evaluation. In some cases, such as when deemed necessary, a proof of the source (such as a salary specification) may be requested.

The enhanced CDD procedures are outlined in the CDD Manual of Administrator.

4.2.3.3 Transfers

The Fund solely accepts SEPA or WIRE transfers through a bank or payment institution. The funds are deposited into Legal Owner's bank account and subsequently transferred to the bank or exchange where the assets are managed, or returned to the Unit Holder's bank account.

Funds can only be refunded to the specified IBAN within the EU/EFTA used to fund the initial subscription of the Unit Holder. In case this IBAN is no longer active, funds can only be refunded to an IBAN within the EU/EFTA in the name of the Unit Holder, verified by reviewing a bank statement prior to refunding. Besides, the name of the bank account must correspond with that of the Unit Holder. Funds cannot be (I) received for the Unit Holder's benefit from an account that is not in their name, or (II) paid out to an account that does not belong to the Unit Holder.

If an employee is presented with a Unit Holder who insists on making cash or cash equivalent payments, or if funds are received without any information from the Unit Holder or their associate, the situation is reviewed, and appropriate action is taken.

4.2.4 Delivery channel risk

4.2.4.1 Definition

Delivery channels refer to the method by which the Unit Holder engages with the Fund. These channels can pose a higher risk of money laundering because of the possibility that the Unit Holder's identity and activities cannot be clearly identified during the CDD phase.

4.2.4.2 Direct or indirect participation

The involvement of third parties, such as intermediaries, can increase the inherent risk of money laundering. A distinction can be made between direct and indirect participation:

- Indirect pariticipation: investors acquiring units in the Fund through e.g. investment firms or banks.
- Direct participation: investors acquire units in the Fund directly, without the intervention of e.g. investment firms or banks. In this case, the units are held in name of the investor.

Since it is only possible to subscribe directly to the Fund, there is a lower risk of money laundering due to intermediary involvement, and additional mitigating measures are not necessary.

4.2.4.3 Intermediary

If a Unit Holder subscribes directly, but after being introduced to the Fund through an intermediary, the following factors lead to a higher risk:

	Risk weighting		
Scenario	Medium	High	Unacceptable
Intermediary is located in a country that is classified as grey or black listed	✓ (grey)	✓ (black)	
Intermediary provides services to clients without appropriate risk mitigation measures	✓		
Intermediary has received negative media attention		✓	
Intermediary appears on a sanctions list		✓	
There is an unexplainable relationship between the intermediary and Fund Manager / the Fund		✓	
Intermediary is suspected of criminal activities, particularly financial crimes or having links to criminal partners		✓	
Intermediary acts on behalf of the Unit Holder, but is unwilling or unable to provide consistent information or complete the required documentation;			✓

When a Unit Holder has a medium or high risk, additional CDD procedures are typically conducted, which are tailored to the relevant risks. The enhanced CDD procedures are outlined in the CDD Manual of Administrator.

4.2.4.4 Digital versus physical

Digital submission of the Subscription Form is mandatory for all Unit Holders.

The CDD process remains unchanged in situations where the Fund Manager has not conducted a face-to-face meeting with the prospective Unit Holder. The initial CDD procedures are standardized and performed by an independent Administrator, and the result of the risk assessment determines whether enhanced CDD is required.

Physical encounters do not necessarily affect the risk assessment, but if any doubts are raised during such meetings, the risk may increase.

4.2.4.5 Cash

The Fund does not accept cash, payment cards, or cryptocurrencies from its business relations and investors.

4.2.5 Product risk

4.2.5.1 Definition

Product risk refers to the degree to which the products in which Fund Manager invests may pose an increased risk. Fund Manager must evaluate to what extent the offered product (the Fund) and the underlying investments may pose potential vulnerabilities for placement, layering or integration of criminal proceeds into the financial system.

A higher product risk impacts the overall risk of Unit Holders. Therefore, if this risk factor is categorized as medium, an enhanced CDD process will be carried out.

4.2.5.2 Factors

The Policy identifies the following aspects as potentially increasing risk:

	Risk weighting		
Scenario	Medium	High	Unacceptable
Products traded on unregulated exchanges	✓ (grey)	✓ (black)	
Products or services that promote anonymity or lack clear information about underlying transactions (e.g., bearer shares or omnibus account services)	✓		
Products with an unusual complexity or structure and no clear economic purpose		✓	
Products or services that enable the anonymous transfer of value (through payment or change of ownership of assets) to an unrelated third party, in particular, those residing in a higher-risk jurisdiction		✓	
Products particularly sensitive to fraud and market abuse, such as low-priced securities (penny stocks/micro-cap stocks)	✓		
The purchase of securities using cash			✓
The purchase of virtual currencies		✓	
The purchase of investment objects (horses, teak, whisky, gold, wine, etc.), art and/or antiques, real estate, microfinance, CO2 emission rights, oil, gas, or minerals.	✓		
The purchase of virtual currencies		✓	
The purchase of investment objects (horses, teak, whisky, gold, wine, etc.), art and/or antiques, real estate, microfinance, CO2 emission rights, oil, gas, or minerals.	✓		

For the Fund, there is an increased risk as Digital Assets are part of the strategy. Digital Assets pose a high risk of money laundering and terrorist financing, among other things due to the anonymity of transactions. This means that this risk factor is classified as "high" for each Unit Holder. Due to the high risk associated with Digital Assets, Fund Manager conducts enhanced customer due diligence on:

- Unit Holders in the Fund;
- relationships that are professional counterparties, such as other funds (fund to funds) and Virtual Asset Service Providers (VASPs) that facilitate Crypto trading, among others;
- Service Provider.

In its sector letter, the AFM stated the following:

'*The AFM notes that given the nature of cryptos and the unfamiliarity with origins and intermediaries in transactions involving cryptos, in many cases it will not be possible to comply with the requirements of the Wwft. It is the responsibility of the institutions to put the necessary safeguards in place for this purpose*.'

Administrator implements the following safeguards to keep the risk manageable:

Category	Description	Measures
Unit Holders	The Product Risk is “high”	Unit Holders are subject to enhanced CDD
Initial Coin Offering (ICO) / decentralized exchange (DEX)	The checks for potentially fraudulent trading in an ICO and on a DEX are too complex.	Fund Manager is not permitted to participate in an ICO or trade on a DEX.
Transfers	The origin of funds in crypto transfers is too complex and opaque to trace. With fiat deposits, however, the funds are monitored by a regulated banking institution.	The Fund only accepts transfers in fiat.
Service Provider / VASPs	For Service Providers and/or VASPs, it is important that the party has similar level of Wwft and Sanctions Act procedures as the Fund.	The Fund does business only with Service Providers Relations and/or VASPs that have been analyzed and approved by Fund Manager. For this process, see the sectie 4.2.5.3.
Transactions	It is important to keep non-financial and financial transactions for at least 5 years.	Fund Manager retains transactions, such as trades in Cryptos on a Crypto exchange or the outcome of a client inquiry, for at least 5 years.

4.2.5.3 Due diligence Service Providers

Fund Manager requires that Services Providers (I) conduct due diligence on clients, (II) take the necessary measures regarding security and (III) the Service Providers have a good reputation. Administrator also classifies a VASP as a Service Provider.

To assess Service Providers, they are evaluated according to the following risk factors:

- Service Provider Risk;
- underlying risk;
- geographical risk;

Fund Manager performs the assessment at the start of new relationships, on an annual basis and/or as Manager deems necessary based on objective or subjective observation.

Several questions are central to the assessment. These are listed below for each risk factor. The answers are then reviewed by Fund Manager to determine whether Fund Manager does business with a Service Provider.

Service Provider risk

- What are the licenses and/or registrations held by the Service Provider and from which regulators were they obtained?

- What are the legislations related to the prevention of money laundering, terrorist financing and/or sanctions that the Service Provider is subject to?
- What documents are available that describe anti-money laundering, sanctions and/or terrorist financing activities?
- What are the Service Provider's convictions related to money laundering, sanctions and/or terrorist financing?
- What is the transparency score of Nomics and CryptoCompare (in the case of a Crypto exchange)?
- What are the past hacks known from the Service Provider or what are the properties of relationships/clients that have been lost?
- What are the protective measures taken by the Service Provider to prevent loss of investment institution property?

Underlying risk

- What kind of due diligence does the Service Provider conduct on its clients?
- How does the Service Provider verify the identity of relationships/clients?
- How does the Service Provider conduct research on the source of funds/assets (including origin of Cryptos) of its relations/clients?
- What kind of controls does the Service Provider perform on the parties it works with?
- What checks does the Service Provider perform on coins (and parties involved) before they are purchased in the investment vehicle (in the case of fund to funds)?
- What investments does the Correspondent make in ICOs (in the case of fund to funds)?
- How does the Service Providers prevent transactions that are fraudulent?

Geographical risk

- What are the countries where Service Provider is located?
- What are the countries where Service Provider does or does not accept clients?
- What is a further explanation of the above questions?

The analysis on all Service Providers (i.e. VASPs) can be found in a separate document.

On an annual basis, Service Providers are subject to reassessment. This reassessment is carried out by Fund Manager. In addition, it is possible that Fund Manager occasionally stops trading through a crypto platform when Fund Manager is aware that a crypto platform has appeared negatively in the media or another Hit has been found.

4.2.5.4 Due diligence VASPs

To implement its investment policy, the Fund wishes to invest on various crypto platforms. These platforms are also considered as Service Providers (i.e. VASPs). Fund Manager has examined the different platforms according to the assessment described in section 4.2.5.3. The VASPs which were examined for the implementation of the investment policy are as follows:

- Bybit
- Amdax
- Crypto.com
- Deribit

The results are described in a separate document and can be requested from the Fund Manager.

4.2.5.5 DEX

An investment institution that makes use of a DEX on the basis of its investment policy is under circumstances obliged with respect to this DEX to perform customer due diligence within the meaning of the Wwft and to verify the identity within the meaning of the Sanctions Act. This requires a "business relationship" within the meaning of Section 1(1)(b) of the Wwft and a "relationship" within the meaning of Section 1(b) in the Sanctions Act.

Business relationship

What matters for the terms "business relationship" and "relationship" is whether an owner/operator is attached to the DEX. There is no (business) relationship if a DEX is run solely by protocol. Indeed, FATF provides that the underlying software or technology does not qualify as a VASP (paragraph 67 in this web link). In that case, an investment institution is not required to conduct client due diligence or identity verification.

The "Analyze Service Providers" document identifies whether there is a (business) relationship for each DEX by examining whether the DEX has (I) an open source protocol, (II) general terms and conditions, (III) privacy statements, (IV) customer service and/or (V) contact information. These are considered features that may be indications that a DEX is run by a protocol or owner/operator. Based on the observations, it is concluded whether a DEX can be considered a (business) relationship.

In this case there may well be a (business) relationship and it is required to conduct a customer due diligence on the owner/operator and verify the identity. Should there be a (business) relationship, the investigation will be completed as described in section 4.2.5.3.

Other side of the order book

Furthermore, an investment institution is in principle not obliged to verify the identity with respect to the other side of the order book (the person who submits the buy or sell order to the DEX). Nonetheless, the risk remains that with a DEX, the party "on the other side of the order book" is a sanctioned person or entity since no client due diligence is performed by a DEX. This goes against the objectives of the Sanctions Act.

To mitigate the "sanctions risk," the "Analyze Service Providers" document identifies (I) what measures the DEX itself takes or are built into the protocol (e.g., Proofi or Tgrade), (II) what the transaction volume is on the DEX (lower volume reduces the risk of sanctions evasion) and (III) what - if possible - are the activities of the owners/operators associated with the DEX and screen them using Trade Sure.

The above determinations are a standard part of the analysis on a Service Provider.

Risk appetite.

In the "Analyze Service Providers" document - as with any Service Provider - the identified risk of the DEX in question is ultimately measured against the risk appetite of the investment institution in question.

4.3 Risk classification

The table below outlines the different risk classifications along with their descriptions, outcomes and the frequency of periodic monitoring:

Category	Description	Results	Frequency of periodic monitoring
Low	Note: Due to product risk, the customer due diligence cannot conclude that the participant has low risk in terms of money laundering and terrorist financing.		
Medium	Note: Due to product risk, the customer due diligence cannot conclude that the participant has medium risk in terms of money laundering and terrorist financing.		
High	The CDD has shown that the Unit Holder has a high risk with regard to money laundering and terrorist financing.	An enhanced CDD is performed, which indicates that additional information or documentation is requested.	CDD is updated once (1) per year or due to an event-driven review.
Unacceptable	The CDD has shown that the Unit Holder has a crucial unacceptable risk with regard to money laundering and terrorist financing.	The participant will not be accepted.	-

4.3.1 Establishment of risk classification

The table below shows how the overall risk is classified:

Category	Possibilities
Low	▪ Due to product risk, the risk profile cannot be low risk in terms of money laundering and terrorist financing.
Medium	▪ Due to product risk, the risk profile cannot be medium risk in terms of money laundering and terrorist financing.
High	▪ One or more of the risk factors display a “high” risk and in the subjective approach, there is no reason to increase the risk to “unacceptable”.
Unacceptable	▪ One or more of the risk factors display an “unacceptable” risk; ▪ None of the risk factors displays an “unacceptable” risk, however, in the subjective approach, there is reason to increase the risk to 'unacceptable'.

4.4 Continuous monitoring

4.4.1 Periodic monitoring

The frequency and intensity of periodic monitoring for a Unit Holder depends on their risk profile. The higher the risk profile, the more frequent and thorough the reviews will be conducted in order to mitigate risks to an acceptable level:

Risk classification	Frequency of periodic monitoring
Low	Due to product risk, the risk profile cannot be low risk in terms of money laundering and terrorist financing.
Medium	Due to product risk, the risk profile cannot be medium risk in terms of money laundering and terrorist financing.
High	The CDD is updated once (1) per year or when an unusual transaction is observed.
Unacceptable	-

4.4.2 Transaction monitoring

Objective or subjective indicators of unusual or suspicious transactions may result in a report being submitted to the FIU.

4.4.2.1 Objective indicators

The objective indicator for unusual or suspicious transactions is as follows:

- Transactions that raise concerns about being linked to money laundering or terrorist financing;

In this case, a report to the FIU is considered necessary.

4.4.2.2 Subjective indicators

The following subjective indicators may indicate suspicious activity by a Unit Holder:

a. Transactions lacking a clear economic basis;
b. A Unit Holder’s request to transfer the subscripion amount shortly after the initial subscription;

c. The Unit Holder that is regularly represented by different trustees or characterized by frequent changes in UBO;
d. Doubts about the reliability of previously obtained identification data of the Unit Holder;
e. The Unit Holder is a trust, a shell company or a private investment company that is reluctant to provide information about related (legal) persons and/or UBO(s);
f. Publicly knowledge of of ongoing criminal, civil or regulatory proceedings against the Unit Holder for corruption, misuse of public funds, other financial crimes, or non-compliance with regulations, or a relationship with such (legal) persons;
g. The Unit Holder's background is questionable or deviates from expectations;
h. The Unit Holder has been rejected by other financial service providers or had a terminated business relationship with them;
i. The Unit Holder is reluctant to provide information regarding identity and/or transactions;
j. The Unit Holder raises concern about compliance with the Wwft and Sanctions Act policy, reporting requirements or other controls.
k. The Unit Holder tries to persuade an employee not to submit required reports or to keep track of necessary data.
l. Receipt of money transfers from third parties or sources with no clear relationship to the Unit Holder.
m. The Unit Holder requests payments be made through other accounts instead of his or her account.
n. Suspicious or unusual patterns are revealed in transfer activity over a period of time.
o. Unusual transfers or a high volume/frequency of transactions without reasonable or obvious reason;
p. The Unit Holder regularly changes known and verified bank account.
q. Transactions by or for a (legal or natural) person residing or established in a country indicated as high-risk without reasonable or obvious reason;
r. Withdrawals/transfers to bank accounts in a blacklisted country without reasonable or obvious reason;
s. Other signals highlighted by Fund Manager or Administrator.

4.4.2.3 Event-driven review

The CDD is also updated in the following events:

a. Change in the composition of the Unit Holder (e.g. the board) or UBO(s);
b. Change in the profession or business activity of the Unit Holder or UBO(s);
c. Change in the address of the Unit Holder or UBO(s);
d. Change in country risk;
e. Net subscription amounts (redemptions considered) exceed limit values of € 100,000 or € 250,000;
f. Change of the PEP status of the Unit Holder, other relevant (legal) persons involved or UBO(s);
g. The Unit Holder, other relevant (legal) persons involved or UBO(s) are listed on a sanction list;
h. Adverse media attention for the Unit Holder, other relevant (legal) persons involved or UBO(s);

4.4.2.4 Expected transaction profile

Prospective Unit Holders are required to provide an expected transaction profile in the subscription form. If a Unit Holder exceeds the thresholds in their profile, they will be asked to provide an explanation. If the explanation is deemed unreasonable, the risk profile may be increased. The CDD Manual of the Administrator outlines the procedures for this purpose.

4.4.2.5 Fund Manager

Fund Manager is responsible for managing the assets of the Fund, which may provide Fund Manager with opportunities to engage in criminal activities through the Fund. The Board of Legal Owner is responsible for verifying that Fund Manager is following the investment policy as stated in the Information Memorandum.

Moreover, Administrator makes reasonable efforts to identify any deviation from the Fund's investment policy by regularly monitoring the Fund's trading activity. However, Administrator does not have continuous insight into the trading activity of Fund Manager. These information is obtained later by importing information from the bank and/or exchange.

5 Procedure

5.1 Purpose

The purpose of CDD is to:

- identify a Unit Holder and verify the identity;
- identify the UBO(s) and take reasonable measures to verify the identity. If the Unit Holder is a legal entity, reasonable measures must be taken to obtain insight into the ownership and control structure. If the UBO holds a senior management position, reasonable measures must be taken to verify the identity of this natural person. The measures taken and the difficulties encountered during the verification process taken must be documented;
- determine the purpose and intended nature of the business relationship;
- continuously monitor the business relationship and the transactions conducted to verify that they align with the Unit Holder's risk and transaction profile. This may involve investigating the origin of the resources used in the business relationship or transaction;
- verify if the natural person representing the Unit Holder is authorized to do so and, if necessary, identify and verify their identity;
- take reasonable measures to verify if the Unit Holder is acting on their own behalf or on behalf of a third party.

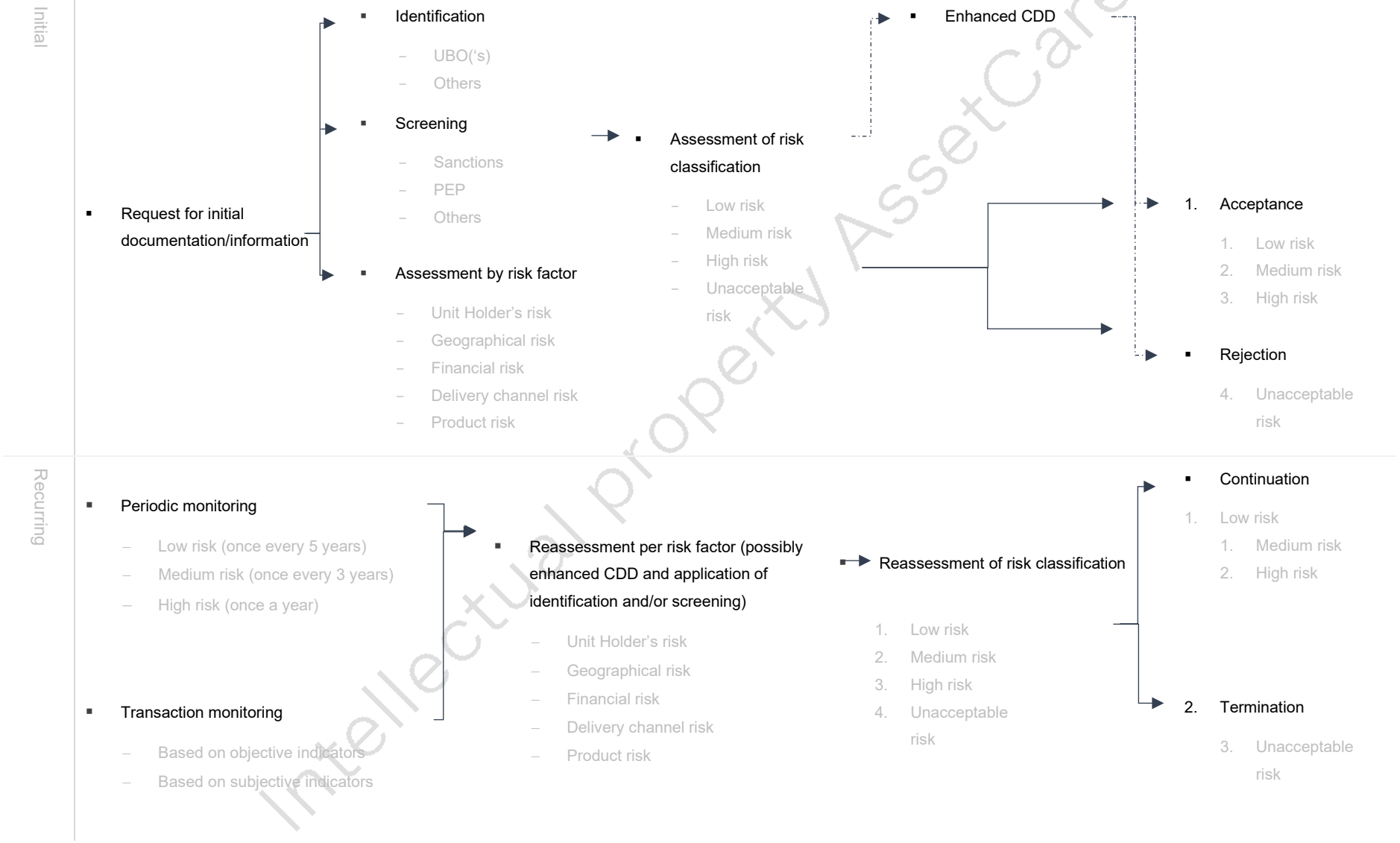
5.2 Process

The next page contains a visual representation of the essential actions required to carry out both the initial and recurring CDD.

CALLISTO CAPITAL

CDD

During CDD, an unusual transaction may need to be reported (see Section 6.1).



5.3 Initial CDD

The information required to assess the various risk factors is collected at the time a business relationship is initiated. The information corresponds to the necessary information from the various risk factors described in Section 4.2 and is integrated into the subscription form.

An initial risk classification is determined based on the various risk factors (identification and sanction screening are part of the risk factor “Unit Holder’s risk”). The substantiation, findings of the risk factors, risk classifications, and accompanying information and documentation are stored in the AssetCare Portal.

If the information or documentation is not promptly provided and remains incomplete, the Unit Holder cannot subscribe to the Fund. In such cases, it should be considered to report to the FIU (see Section 6.2).

5.4 Identification

5.4.1 Introduction

Verifying the identity of Unit Holders and other relevant individuals is a critical task that must be performed based on reliable and independent data or documentation. The level of identification procedures applied depends on the risk associated with the Unit Holder, the Fund and/or the transaction.

The following means of verifications are allowed for identification purposes:

- For natural persons:
  - a valid passport or identity card for individuals with Dutch nationality;
  - a valid passport for individuals with non-Dutch nationality.
- For Dutch and foreign legal entities established in the Netherlands:
  - an (electronic) commercial register extract (certified, if required); or
  - a deed or declaration by a Dutch notary or a similar official from another Member State.
- For foreign legal entities not established in the Netherlands:
  - reliable documents from independent sources, data or information in international trade; or
  - documents, data or information recognized by law as valid means of identification in the individual's state of origin
- For other clients:
  - documents, data or information from a reliable and independent source.

5.4.2 Verification of natural persons

When initiating a new relationship, the required information for identifying a natural person is collected. This includes their name, nationality, date and place of birth, and residency. To verify the accuracy of the provided information, the following verification methodologies are applied:

- Requesting a copy of the proof of identity
  - This document allows to compare and verify whether the information provided matches the details on the proof of identity. The proof of identity must be valid and the Citizen service number must be visible (if possible). This information is also used to screen the individual.
- Requesting a bank statement (including name, bank account and address)

- Unit Holders can only transfer their subscription amount from a bank account registered in their name. A bank statement allows to verify the correctness of the bank details, and the individual's name and residency.

At least the following natural persons shall be identified by type of Unit Holder, including the verification methodologies:

	Verification methodologies	
Natural person	a. Copy of proof of identity	b. Bank statement
Single Unit Holder		
Unit Holder 1	✓	✓
Joint Unit Holders		
Unit Holder 1	✓	✓
Unit Holder 2	✓	✓
Corporate Unit Holder		
Representative	✓	Unlikely
Director(s)	✓	Unlikely
(Pseudo) UBO('s)	✓	✓
Shareholders (>10%)	✓	Unlikely

5.4.3 Legal entity verification

The following information is required for legal entities:

- Name of the entity, the proof of incorporation, legal form and status, registered office address, articles of association and a list of directors;
- Register of shareholders (or members), including the number of shares held by each shareholder and the classes of shares (including the nature of the corresponding voting rights);
- UBO(s).

To verify the above-mentioned information, the following verification methodologies are applied:

- Requesting an extract from the Chamber of Commerce or equivalent document in another country:
  - A digital extract from the Trade Register serves official proof of registration in the Trade Register and also provides certainty about the signing authority of the relevant party.
  - A digitally certified extract is legally valid when it is received digitally. If the digitally certified extract is printed, it will not be considered legally valid. In such cases, the certification will not be visible and the signature cannot be verified.
- Requesting a bank statement (incl. name, fixed counter account and address)
  - Unit Holders are required to deposit funds from a bank account that is registered in their exact name. This can be verified by reviewing a bank statement, which also allows for additional monitoring of the Unit Holder's name and address.

- Requesting an organizational chart (shareholders' structure):
  - A visual representation of the shareholder structure, which provides insight into the relevant legal entities and natural persons involved.

- Requesting a shareholders' register:
  - The shareholders' register shows the shareholders of a company and is issued upon the formation of the company.
- Requesting the articles of association:
  - The articles of association are part of the deed and contains the rules and provisions of a legal entity, including its name, objective, place of establishment, capital, etc. The notary creates the articles of association when the legal entity is established and can later be amended through the notary.
- (Pseudo) UBO declaration (see Section 5.4.4)

At least the following legal entities are identified for a corporate Unit Holder, including the verification methodologies:

	Legal entities		
Verification methodologies	Account holder	Shareholders(>25%)	Directors
Corporate Unit Holder			
Chamber of Commerce registration	✓	✓	✓
Bank statement	✓	Unlikely	Unlikely
Structure chart	✓ (unless 1 layer)	Unlikely	Unlikely
Shareholders' register	✓ (unless 1 shareholder)	Unlikely	Unlikely
Statutes	✓	Unlikely	Unlikely
UBO statement	✓	Unlikely	Unlikely

5.4.4 UBO and Pseudo-UBO

Fund Manager is required to identify the UBO(s) of the corporate Unit Holders.

5.4.4.1 UBO declaration

A (Pseudo) UBO statement should be completed by the Unit Holder at the commencement of the business relationship. Unit Holders are also required to notify Fund Manager of any organizational changes.

5.4.4.2 UBO registration

UBO registration is necessary to comply with the AMLD and to prevent the financial system from being used for money laundering and terrorist financing.

During the CDD, it is mandatory to use information from the Chamber of Commerce extract UBO register to verify the information that is declared by the Unit Holder. Fund Manager must report to the Chamber of Commerce if there is a discrepancy between the information obtained during CDD and the information on the extract.

Note: as of 22 November 2022, the UBO register data has ceased to be publicly available and the option to request a Chamber of Commerce extract UBO register has been discontinued.

5.5 Screening

5.5.1 Sanctions

An external system, Handelzeker, is used to screen for sanctions when entering into a new relationship. The system is designed to monitor sanctions lists. During the initial monitoring, the necessary data is inserted into the system, such as:

- gender;
- name (in any case first name and surname as stated on the proof of identity and possibly other known names and aliases);
- date of birth;
- country of birth;
- nationality.

The system has been adjusted to detect slight differences in the data from various sources and systems, minimizing errors.

The persons and entities that have been added to Handelzeker are monitored on a daily basis, with Administrator receiving notifications from Handelzeker of any changes in screening outcomes. The sanctions lists that are included in Handelzeker are listed in Appendix 3.. If any information about a relationship changes, it is accordingly actualized in Handelzeker.

An additional monitoring is also conducted through the Database of the Offshore Leaks by the International Consortium of Investigative Journalists (ICIJ). This database provides a list of natural and legal persons with money in secret accounts in tax havens.

At a minimum, the following parties are screened for sanctions:

- Unit Holders (including relevant natural and legal persons);
- Fund Manager (including relevant natural and legal persons);
- Administrator (including relevant natural and legal persons);
- Any external service providers (including relevant natural and legal persons).

Besides, a bank/exchange that is used for the execution of the investments policy reviews if any sanctions have been imposed on the investment products that can be traded via the relevant bank/exchange, including investment products subject to the Cluster Munitions Treaty (Verdrag inzake Clustermunitie, the “CCM”). Fund Manager is also prohibited from trading in such products, as stated in the Information Memorandum.

In the event of a hit, Administrator reviews the outcome and the findings are shared with Fund Manager. Subsequently, action is taken if deemed necessary by Fund Manager.

5.5.2 PEP

PEP screening is performed in conjuction with sanctions screening, using Handelzeker to monitor whether the person is identified as PEP. This happens initially during the start of the relationship and then continuously through the system. It is determined whether the person is a PEP and what role and during what period these concerns. In addition, the PEP screening is performed at least at those parties that are subject to identification requirements to comply with the CDD. This may include, but is not limited to, the Unit Holders and UBO(s).

If a hit occurs, Administrator will first assess the associated risk and may contact the Unit Holder to obtain more insight. Subsequently, a thorough evaluation of the Unit Holder's risk will be undertaken in consulation with Fund Manager to determine the appropriate course of action.

5.5.3 Other

Negative media monitoring is also performed using Handelzeker, similar to the sanctions and PEP screening. Besides, a Google check is conducted at the beginning of the business relationship using a specific string in Dutch or English, searching for relevant natural or legal persons via www.google.com:

Language	String
Dutch	"voornaam en achternaam of naam van entiteit" AND (witwassen OR fraude OR terrorisme OR criminaliteit OR "insider trading" OR schending OR sanctie OR kartel OR inbreuk OR wangedrag OR wapen)
English	"first name and last name or name of the entity" AND (launder OR fraud OR terrorism OR crime OR "insider trading" OR violate OR sanction OR cartel OR breach OR traffic OR misconduct OR weapon)

Additionally, the person/entity in question is searched via LinkedIn as an additional verification to ensure that the information in the subscription form matches the background of thwork experience whether it corresponds to the information in the Subscription Form and what the work history and education of the subject is (or has been).

5.6 Enhanced CDD

Enhanced customer due diligence applies to all relationships due to product risk. This involves identifying additional measures based on the type of participant and available information and documentation.

Examples of stricter measures that may be implemented include:

- obtaining additional information/documentation and identification data from the Unit Holder and/or other data subjects (such as the UBO(s));
- obtaining additional information on the intended nature of the business relationship;
- verifying the additional information obtained with independent and reliable sources;
- verificying the origin of the assets and funds involved.

The information/documents that may be requested are outlined in Section 4 per risk factor. Communication regarding these measures is typically conducted via email, though telephone contact may also be made.

5.7 Assessment

Upon obtaining the necessary information, the relationship is assessed based on various risk factors and a decision is made to either accept or reject the business relationship.

If the relationship is with an existing Unit Holder, a determination is made whether to continue or terminate the relationship after actualizingthe information resulting from an event.

5.7.1 Acceptance

The overall risk classification is determined based on various risk factors. Fund Manager or Administrator may deviate from this classification if there are sufficient reasons to do so. The final risk classification determines what measures are taken to mitigate the risk. For this fund, only participants classified as `high' are accepted (due to product risk).

If a Unit Holder is classified as high risk, Fund Manager and Administrator will consult before accepting or continuing the relationship.

5.7.2 Rejection

If the Unit Holder's profile appears unusual, cannot be explained or indicates a demonstrable risk of money laundering, terrorist financing or sanctions violations, the Unit Holder in question may be considered to be rejected.

This determination is made in consultation between Fund Manager and Administrator. Fund Manager is responsible for rejecting a Unit Holder, while Administrator has the right to refuse a relationship if the Unit Holder is not in line with the AML/CFT and Sanctions Act policy.

When a relationship with a Unit Holder ends, all documents related to the Unit Holder's file will be kept for five (5) years in accordance with the legal retention period. If a potential Unit Holder is rejected, the data will be kept for two (2) years.

5.8 Monitors

Continuing CDD is essential and requires implementing procedures that can detect significant changes in the Unit Holder's information. The risk-based approach involves both periodic reviews and transaction monitoring.

5.8.1 Periodic monitoring

The Unit Holder's register monitors when CDD needs to be updated. This should be done before the final date stated for this and involves once (1) per year for the Unit Holders as they are all considered high risk due to product risk.

5.8.2 Amendments

Unit Holders must report any changes using the amendment form, which are then updated in the CDD scanner. Changes may also be obtained from Handelzeker if a Unit Holder, a concerned (legal) person or UBO(s) appears on a PEP or sanction list or has negative media coverage.

If the changes require updating CDD (see Section 4.4), the update will be performed upon the changes are received. If the changes seems unusual based on the subjective indicators (see Section 4.4.2.2), an additional CDD will be carried out, which may eventually lead to a report to the FIU.

5.8.3 Subscriptions or redemptions

The amendment form is used by Unit Holders to subscribe to new Units in the Fund or redeem their existing Units.

For subscriptions and redemptions, the bank account provided by the Unit Holder is checked to ensure that:

- The account is located in a country that is a member of the European Union or EFTA.
- The account name corresponds to the Unit Holder's name at the time of the initial subscription (or a bank account that is verified at a later stage).

If a different bank account is used, the account information is verified to ensure that:

- The bank statement is in the name of the Unit Holder.
- The account is located in a country that is a member of the European Union or EFTA.

Note: if an individual Unit Holder transfers funds from a joint bank account, the joint account holder must also be identified and their written and signed approval must be obtained. Similarly, if a joint Unit Holder transfers funds from an individual bank account, written and signed approval must be received from both account holders indicating that only that bank account is to be used (otherwise, it may result in a transfer of ownership).

The monitoring is carried out before the transaction is conducted. If any changes occur that require an update to the CDD (see Section 4.4.2.3), this will be performed once the changes are received. If a change appears unusual based on subjective indicators (see Section 4.4.2.2) and does not fit the expected transaction profile (see Section 4.4.2.4), an additional CDD will be performed, which may ultimately lead to a report to the FIU.

5.8.4 Fund Manager

The fund administration system imports the transactions of Fund Manager in the Fund (transfers and trades) on an ongoing basis. Both the system and the personnel of Administrator monitor these transactions as described in Section 4.4.2.5.

In the event that Administrator observes unusual transactions of Fund Manager, Administrator must report this to the FIU.

5.9 Systems

5.9.1 Introduction

Multiple systems and databases are used for conducting CDD, determining risk classifications and monitoring transactions:

System/Database	Purpose
Subscription form	Requests necessary information from Unit Holder to initiate the CDD.
Amendment form	Allows Unit Holders to report changes.
CDD Scanner (AssetCare Portal)	Monitors Unit Holders based on various risk factors and generates a general risk profile. The CDD scanner is integrated into the AssetCare Portal.
Register (AssetCare Portal)	Records Unit Holders and other relevant individuals and entities. The register is integrated into the AssetCare Portal.
SS&C	Reviews transactions, such as subscriptions and trades.
Handelzeker	Screens Unit Holders on sanctions, PEP-status and adverse media.
Offshore Leaks Database	Searches for relations involved in the Panama Papers or other scandals.
Google Checks	Conducts additional screening on adverse media.
LinkedIn Check	LinkedIn (or other sources) is used to gain insight into the profession and the background of a relationship.

5.9.2 Subscription form

The subscription form, available in a digitally fillable PDF, is used to inform Unit Holders about the subscription procedure for participating in the Fund and to gather the information and documentation to perform the initial (and subsequently, period) CDD.

Should any additional information or documentation be required, the Unit Holder will be notified via email.

5.9.3 Amendment form

The amendment form enables a Unit Holder to report any relevant changes, such as address changes, additional subscriptions or redemptions.

5.9.4 CDD Scanner

The information obtained from the Unit Holder is analyzed by the CDD Scanner based on various risk factors and assigns a calculated risk classification. The calculated risk classification is enhanced by the findings of a CDD analyst, who has the authority to overwrite the initial classification. The information in the CDD scanner is periodically monitored and updated.

5.9.5 Register

The AssetCare Portal stores information about the Unit Holders and other relevant individuals or entities. This portal has all the necessary functions to maintain the Unit Holder's Register and to process subscriptions, redemptions, conversions and other changes. Transaction monitoring is also performed in this portal.

5.9.6 Fund administration

The fund administration is performed using the systems of SS&C, including Pacer (investment accounting), Genvest (investment ledger) and Persys (performance measurement). As part of the administration, it is also verified if subscription amounts are received from the Unit Holder's known bank account.

5.9.7 Screening

5.9.7.1 Handelzeker

Handelzeker is used to screen Unit Holders against PEP and sanction lists, and adverse media. This is a stand-alone software that allows individuals and entities to be screened. The content of Handelzeker is derived from 100,000 different sources and contains all relevant sanction lists. All relationships are screened daily, regardless of their assigned risk classification.

5.9.7.2 Other public sources

The ICIJ's Offshore Leaks database exposes financial secrets of individuals and entities in offshore havens. This database is screened for Unit Holders, relevant individuals (such as UBOs) and entities. In addition, Google is used to search for adverse media, which can lead to other public sources. At last, LinkedIn is used to verify the obtained background information of an individual.

6 Reporting

6.1 Unusual transactions

6.1.1 Introduction

Fund Manager is responsible for reporting potentially unusual or suspicious transactions to Administrator. Administrator then conducts an independent assessment to determine whether the transaction is deemed unusual, based on the indicators listed in Section 4.4.2.2. Besides, Administrator may request clarification or additional information/documentation from the relevant party to determine whether a transaction is classified as unusual.

Any reports of unusual transactions will be treated confidentially and will not be shared with any other employees (unless necessary), the relevant party and/or third parties.

6.1.2 FIU

Under the Wwft, Fund Manager is obligated to report unusual transactions to the FIU in the Netherlands. As per Article 16 of the Wwft, any unusual transaction must be reported to the FIU without delay, as soon as the unusual nature of the related transaction has been discovered. To ensure timely reporting, Fund Manager has registered with the FIU.

Any suspicious transactions, even in cases where no business relationship is established, must be reported to the FIU.

6.1.3 Procedure

The following manual provides instructions for submitting a report to the FIU through the reporting portal.

Manual goAML

When submitting a report, the following information must be provided:

- The identities of the Unit Holder, UBO(s), natural persons, and, where applicable under Article 3/4 of Wwft, the person on whose behalf the transaction is performed;
- The type and number of the Unit Holder's identity document, and, where possible, those of other persons referred to in the prior bullet point;
- The nature, time and location of the transaction;
- The amount, origin, and destination the funds, securities, or other assets involved in the transaction;
- The circumstances that make transaction unusual;
- A description of any valuable items involved in transactions above € 15,000;

For internal administration purposes, the following information must be documented at a minimum:

- Information about the specific suspicious or unusual transaction, as reported in the reporting portal, along with the information described above;
- Confirmation from the reporting portal that the suspicious or unusual transaction has been reported;
- Confirmation message from the FIU to ensure that they have received the notification.

All information related to suspicious or unusual transactions must be stored for a period of five years from the date and time of the report. Furthermore, the FIU may request additional information about a suspicious or unusual transaction, which must be provided directly in writing.

6.2 Sanctions

6.2.1 Introduction

Fund Manager must adhere to the Sanctions Act, which serves as the basis for implementing (inter)national sanction rules. As such, Fund Manager must report without delay if a Unit Holder corresponds to a (legal) person listed on a sanction list, or if there is a (potentially) unauthorized transaction or financial service.

6.2.2 Process

If a relation appears on a sanction list, Administrator will contact Fund Manager directly. On behalf of Fund Manager, Administrator informs the AFM by completing the following form in full.

- Notification form for the implementation of Article 3 of the Sanctions Act Supervision Regulation

The form will be send to meldingsanctiewet@afm.nl: Besides, the relationship in question is ended as soon as possible and/or the transaction will be reversed. Administrator has the right to end the relationship with Fund Manager when this party or a relevant (legal) person is listed on a sanction list.

6.3 Taxation

6.3.1 Common Reporting Standard

The Common Reporting Standard (hereinafter referred to as “CRS”) has been agreed upon by more than hundred countries for the automatic exchange of the financial data for individuals and organisations. Under this standard, Fund Manager must provide (financial) data of Unit Holders who are not residents or established in the Netherlands for tax purposes to the Dutch tax authorities. The Dutch authorities will then share this information with the relevant tax authorities of the country where the Unit Holder resides or is established, subject to the country’s adoption of the CRS. The following data of a Unit Holder is shared with the Dutch authorities:

- First name;
- Last name;
- Initials;
- Prefixes;
- Date of birth;
- Citizen service number (in Dutch: “burgerservicenummer”) / Tax identification number;
- Address information;
- Market value of the Units at year-end;
- Realized gains on redemptions of Units during the year.

6.3.2 Foreign Account Tax Compliance Act

The Foreign Account Tax Compliance Act ("FATCA") became effective on July 1, 2014 as enacted by the United States. To comply with this regulation, Fund Manager and Legal Owner must complete the W-8BEN-E and the W-8IMY forms. Both W-8 forms are valid for the year in which they are signed and for the following three calendar years.

It is also mandatory to identify U.S. Persons and report specific data related to them. However, U.S. Persons are not accepted as investors.

6.4 UBO register

6.4.1 CDD

The UBO register of the Chamber of Commerce keeps records of the UBOs of a legal entity. Fund Manager must notify the Chamber of Commerce if they find a discrepancy between the information on a UBO from the trade register and the information available on other grounds.

Note: as of 22 November 2022, the UBO register data has ceased to be publicly available and the option to request a Chamber of Commerce extract UBO register has been discontinued.

6.4.2 UBO-register trusts

The Fund is required to register its UBOs with the Chamber of Commerce's UBO-register trusts. The following natural persons are classified as UBOs:

- Founder(s);
- Fund Manager;
- Legal Owner; and
- Unit Holders.

The UBO registration must include the UBO's name, month and year of birth, nationality and residence, and the nature and extent of their economic interest. The Unit Holder's interest in the Fund is expressed in percentage classes of 0% - 25%, 25% - 50%, 50% - 75% and 75% - 100%. Additionally, a copy of the UBO's proof of identity must be provided.

7 Administration and Privacy

7.1 Administration

The AssetCare Portal is used to document each initial CDD and to update it during event-driven or scheduled periodic reviews. The relevant documents, data and information are verified immediately.

The aim is to provide regulatory bodies with insight into the relation's information and activity so that the information and documentation can be used as evidence in legal proceedings or investigations related to money laundering or terrorist financing.

A Unit Holder's file includes at least:

- the proof of identity of the Unit Holder and relevant persons (such as (Pseudo) UBO(s), representatives and board members);
- the nature and purpose of the business relationship;
- the organization's authorization(s) and registration number (if applicable);
- the source of funds;
- the organization and ownership structure;
- sanction, PEP and adverse media screenings;
- the AML/CFT risk profile (per risk factor and the overall risk classification);
- evidence of minutes of meetings or phone calls with the relationship, email conversations that is relevant for the AML/CFT risk profile;
- the expected transaction profile;
- the intended and executed (unusual) transactions;
- other information used in the Unit Holder's CDD or other documentation that must be documented.

7.2 Privacy

Since 25 May 2018, Europe has implemented uniform legislation to protect privacy.

Fund Manager and Administrator process personal data in accordance with applicable (inter)national laws and regulations, such as the GDPR, to ensure the protection of personal data. Administrator is not authorized to use any confidential information for any other purpose other than the one for which it was obtained. However, this provision may be exempted with the written consent of Fund Manager and/or for disciplinary, civil or criminal proceedings in which such information may be essential.

Personal data will be utilized for CDD purposes to prevent money laundering and terrorist financing, and it will not be processed in a manner that conflicts with this objective. The personal data stored in the customer files must not be retained beyond the legally mandated period. The documentation and information of the CDD related to the AML/CFT and Sanctions activities involved are stored for five years following:

- the termination of the established or plannedrelationship; or
- the notification to FIU, AFM, local supervisory authority, or another applicable regulatory body in the event of an unusual transaction.

Administrator is using a cloud-based portal (AssetCare Portal) to manage the personal data of Unit Holders and perform the CDDs. This system enabled Fund Manager and Administrator to respond efficiently and promply to any inquiries from regulatory bodies such as the FIU, AFM and the Dutch Data Protection Authoriy (AP).

Appendix 1 Definitions

Definition	Description
Administrator	AssetCare Fund Services B.V., the entity that performs the Unit Holder's and Fund administration for the benefit of the Fund.
AFM	Dutch Authority for the Financial Markets, the supervisory authority for financial institutions.
Bearer shares	Negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate.
CRS	Common Reporting Standard (CRS). Over hundred countries have come to agreements on the automatic exchange of the financial data of persons and organizations under the CRS.
Corporate Service Provider	A company that provides services to another company with regard to – but not limited to – management services, direct debit services, legal services, (legal) secretarial services and/or administration services. A Corporate Service Provider is involved when the shareholder of a company locates in a country other than the country where the company provides its services. The tax position of the company is the most important reason to engage a Corporate Service Provider to meet the substantive requirements. Other reasons may be the protection of the assets and/or the anonymization of the company structure.
Country list	A list of countries that have been categorized as white, grey or black with regard to the risks of money laundering and terrorist financing.
Crypto (Digital Asset)	A digital representation of value that is not issued or guaranteed by a central bank or a government, that is not necessarily tied to a legally determined currency and that does not have the legal status of currency or money, but that is accepted by natural or legal persons as a medium of exchange and that can be carried, stored and traded electronically.
Currency	Banknotes and coins that are in circulation as a medium of exchange.
DNB	De Nederlandsche Bank N.V.
Enhanced CDD	Additional information collected as part of customer due diligence or heightened precautionary measures. The scope of the additional information requested and of the measures that are exercised with respect to a participant (or person(s) involved) depends on the risk of money laundering or terrorist financing may entail and its basis.
FATCA	Foreign Account Tax Compliance Act. This act aims at identifying U.S. Persons holding accounts or financial assets outside the United States.
Fund	Callistp Capital, closed fund for joint account.
Fund administration	The administration of the Fund.
Fund Manager	Callisto Capital B.V.
Hit	A "hit" demonstrates the trigger on a Unit Holder's transaction which can potentially be considered unusual concerning the risk of money laundering, terrorist financing, and sanctions.

Identification	The process by which the relation's data and information are collected to identify the relation. The data enables an adequate and robust risk assessment of the relation.
Information memorandum	The document that describes the main components of the Fund, such as the strategy, costs and risk.
Inherent risk	The risk of the Fund being exposed (directly or indirectly) to money laundering, terrorist financing, or sanctions in the absence of a control environment.
Investment institution	Provides the opportunity for collective investments in assets and liabilities, enabling Unit Holders to participate and share in the returns on those investments.
Legal Owner	Stichting Juridisch Eigenaar Callisto Capital
Money laundering	The act of disguising the illegal origin of criminal proceeds.
Residual risk	The risk that remains after mitigating measures have been applied to the inherent risk.
Risk assessment	Identification of the main risks to the Fund so mitigating measures can be identified.
Screening	The screening of a relation against sanctions lists, PEP lists and negative media.
Terrorist financing	Involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations.
Transaction monitoring	The process of monitoring both financial and non-financial transactions, such as subscriptions, redemptions, and address changes or unusual activities that don't fit into the (transaction) profile of a relation.
Ultimate beneficial owner	Refers to the natural persons who ultimately[1] own or control the Unit Holder[2] and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. [1]Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. [2]This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.
Unit Holder	A natural person or legal entity who is invested in the Fund.
Unit Holder Register	The administration (the register) where the details of the Unit Holders in the Fund are maintained by Administrator.
Virtual Asset Service Provider (VASP)	Service provider in the field of Crypto that, as a business for or on behalf of another natural or legal person, performs one or more of the following activities or operations: I. Conversion between virtual assets and fiat money; II. Conversion between one or more Cryptos. III. Transfer of Cryptos; IV. Custody and/or management of Cryptos or instruments enabling control over Cryptos; and Participation in and provision of financial services in connection with the offer and/or sale of a Crypto.

Appendix 2 List of countries

Each country is categorized as white-, grey- or black listed based on the following sources:

- Corruption Perceptions Index (2023)
  - Countries ranked on corruption, scoring on a scale of 0 (highly corrupt) to 100 (very clean).
- Basel AML Index (2023)
  - Countries ranked on the risk of money laundering and terrorist financing in jurisdictions on a scale of 0-10, where 10 indicated the highest risk level.
- Offshore Jurisdictions
  - The EU list of non-cooperative jurisdictions for tax purposes is part of the EU's work to fight tax evasion and avoidance. Countries listed are considered to have a high-risk ranking.
- EU & UN Sanctions (2024)
  - Sanctioned countries are black-listed.
- EU commission (2024)
  - The European Commission identified jurisdictions with strategic deficiencies in their AML/CFT regimes. These jurisdictions are black-listed countries.
- FATF (February 2024)
  - Jurisdictions under Increased Monitoring black-listed countries. High-Risk Jurisdictions subject to a Call for Action are listed as unacceptable.

Based on the sources, the countries have been classified as follows:

Country	Risk	Country	Risk
Afghanistan	Black	Lesotho	Black
Albania	Black	Liberia	Black
Algeria	Black	Libya	Black
American Samoa	Black	Liechtenstein	White
American Virgin Island	Black	Lithuania	Grey
Andorra	White	Luxembourg	White
Angola	Black	Macedonia	Grey
Anguilla	Black	Madagascar	Black
Antigua and Barbuda	Black	Malawi	Black
Argentina	Black	Malaysia	Black
Armenia	Black	Maldives	Black
Aruba	Grey	Mali	Black
Australia	White	Malta	Grey
Austria	White	Marshall Islands	Black
Azerbaijan	Black	Mauritania	Black

Country	Risk	Country	Risk
Bahamas	Grey	Mauritius	Grey
Bahrain	Black	Mexico	Black
Bangladesh	Black	Micronesia	Black
Barbados	Black	Moldova	Grey
Belarus	Black	Monaco	Black
Belgium	White	Mongolia	Black
Belize	Black	Montenegro	Black
Benin	Black	Morocco	Black
Bhutan	Grey	Mozambique	Black
Bolivia	Black	Myanmar	Unacceptable
Bosnia and Herzegovina	Black	Namibia	Black
Botswana	Grey	Nauru	Black
Brazil	Black	Nepal	Black
British Virgin Island	Black	Netherlands	White
Brunei	White	New Zealand	White
Bulgaria	Black	Nicaragua	Black
Burkina Faso	Black	Niger	Black
Burundi	Black	Nigeria	Black
Cambodia	Black	North Korea	Unacceptable
Cameroon	Black	Norway	White
Canada	White	Oman	Black
Cape Verde	Grey	Pakistan	Black
Cayman Islands	Black	Palau	Black
Central African Republic	Black	Palestine	Black
Chad	Black	Panama	Black
Chile	Grey	Papua New Guinea	Black
China	Black	Paraguay	Black
Colombia	Black	Peru	Black
Comoros	Black	Philippines	Black
Congo-Brazzaville	Black	Poland	Grey

Country	Risk	Country	Risk
Congo-Kinshasa	Black	Portugal	Grey
Costa Rica	Black	Puerto Rico	Black
Croatia	Black	Qatar	Grey
Cuba	Black	Romania	Black
Curacao	Black	Russia	Black
Cyprus	Grey	Rwanda	Grey
Czech Republic	Grey	Saint Kitts and Nevis	Grey
Denmark	White	Saint Lucia	Grey
Djibouti	Black	Saint Vincent and the Grenadines	Grey
Dominica	Grey	Samoa	Black
Dominican Republic	Black	San Marino	White
Ecuador	Black	Sao Tome and Principe	Black
Egypt	Black	Saudi Arabia	Grey
El Salvador	Black	Senegal	Black
Equatorial Guinea	Black	Serbia	Black
Eritrea	Black	Seychelles	Black
Estonia	White	Sierra Leone	Black
Eswatini	Black	Singapore	White
Ethiopia	Black	Slovakia	Grey
Fiji	Black	Slovenia	Grey
Finland	White	Solomon Islands	Black
France	White	Somalia	Black
Gabon	Black	South Africa	Black
Gambia	Black	South Korea	Grey
Georgia	Grey	South Sudan	Black
Germany	White	Spain	Grey
Ghana	Black	Sri Lanka	Black
Gibraltar	Black	Sudan	Black
Greece	Grey	Suriname	Black
Grenada	Grey	Swaziland	Black

Country	Risk	Country	Risk
Guam	Black	Sweden	White
Guatemala	Black	Switzerland	White
Guinea	Black	Syria	Black
Guinea-Bissau	Black	Taiwan	Grey
Guyana	Black	Tajikistan	Grey
Haiti	Black	Tanzania	Black
Honduras	Black	Timor-Leste	Black
Hong Kong	Grey	Thailand	Black
Hungary	Black	Togo	Black
Iceland	White	Tonga	Black
India	Black	Trinidad and Tobago	Black
Indonesia	Black	Tunisia	Black
Iran	Unacceptable	Turkey	Black
Iraq	Black	Turkmenistan	Black
Ireland	White	Tuvalu	Black
Israel	Grey	Uganda	Black
Italy	Grey	Ukraine	Black
Ivory Coast	Black	United Arab Emirates	Black
Jamaica	Black	United Kingdom	White
Japan	Grey	United States of America	Grey
Jordan	Black	Uruguay	White
Kazakhstan	Black	Uzbekistan	Black
Kenya	Black	Vanuatu	Black
Kiribati	Black	Vatican City	Black
Kosovo	Black	Venezuela	Black
Kuwait	Black	Vietnam	Black
Kyrgyzstan	Black	Yemen	Black
Laos	Black	Zambia	Black
Latvia	Grey	Zimbabwe	Black
Lebanon	Black		

Appendix 3 Sanctions lists

Handelzeker provides access to the following sanction lists:

- Office of Foreign Assets Control (OFAC)
- HMT (Her Majesty's Treasury)
- Austrac (AU)
- United Nations
- EU
- Japanese Ministry of Finance
- Malaysian Ministry of The Interior
- Russian Federal Financial Monitoring Service
- Swiss Secretariat of State for Economic Affairs
- Australian Government National Security
- Sanctions by the Canadian Government
- Monetary Authority of Singapore
- End-user list of the Federal Ministry of Economic Trade and Industry
- Chinese Ministry of Public Security
- Dutch National Terrorism Sanctions
- Ukraine National Security and Defense Council
- Australian Department of Foreign Affairs and Trade
- Belgian Federal Public Service Finance
- French Ministry of Economy and Finance, DG Treasury
- United States Department of State
- Asian Development Bank
- Pakistan National Counter Terrorism Authority – Proscribed Persons and Entities
- Ukraine State Financial Monitoring Service
- Australia Department of Foreign Affairs and Trade – Consolidated List
- Tunisian National Anti-Terrorist Commission
- Bahrain Ministry of Foreign Affairs
- Monaco Council of Ministers
- Israel Securities Authority
- Israel Ministry of Defense
- Turkey Ministry of Interior
- National Bank of Tajikistan
- New Zealand Police Designated Terrorists – Non-UN Listed Entities.

These lists contain names of individuals, entities, organizations, and countries subject to various types of sanctions, such as financial sanctions, trade sanctions, and travel bans, imposed by the relevant authorities.

The CDD Manual of Administrator outlines the internal screening control processes.