Premier Invest

Anti–Money Laundering and Counter Financing of Terrorism

Document Review and Approval

Version Control

Version	Reviewed by	Endorsed by	Approved by	Implemented on
1.0	Compliance Officer	Senior Executive Officer	Board of Directors	23/05/2025

Table of Contents

Table of Contents (continued)

Premier Invest

1

PART ONE

ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

1 Introduction

Premier Investment Partners (herein referred to as the "**PIP**") is committed to assisting in the fight against money laundering, including bribery/corruption and terrorist financing and to comply with local and applicable international sanctions, by having in place effective measures and controls operated on a risk-based approach. In doing so, our aim is to manage legal, compliance, regulatory and reputational risks actively, within and across PIP, mitigate those risks and thereby seek to prevent, detect and report money laundering activities.

PIP seeks to comply with and adopt the highest standards of Anti Money Laundering ("**AML**") and Counter Financing of Terrorism ("**CFT**") compliance and require senior management and employees to adhere to these standards to prevent our products and services from being used for money laundering purposes.

This AML/CFT Manual (the "**Manual**") establishes and maintains systems and controls to prevent money laundering and to ensure that the Board and senior management remain aware of the effectiveness of our AML controls. This Manual also helps us in complying with applicable AML and CFT legislation and formalizes our arrangement for the annual risk assessment of our AML and CFT program.

The standards set out in this policy are requirements based on applicable legal and regulatory requirements, and these are intended to prevent PIP, our employees, and clients from being used as a conduit for money laundering, terrorist financing or other financial crime.

Responsibility for compliance with this policy lies with everyone in PIP and therefore everyone must always be vigilant and mindful in performing our duties in relation to this Manual.

PIP adopts and enforces rigorous policies, procedures, and controls to detect and deter the occurrence of money laundering, as set forth herein. The Manual consists of four parts:

(a) Policy;
(b) Procedures;
(c) Forms and Templates; and
(d) Definitions.

The Money Laundering Reporting Officer ("**MLRO**") is the owner of this Manual. Any amendments to this Manual must be endorsed by the Senior Executive Officer ("**SEO**") and approved by the **Board of Directors** ("**Board**"). The Manual is for internal use only and must not be distributed outside PIP without the prior written approval of the Compliance Department of Premier Investment Holdings Limited (herein referred to as "PIHL"), PIHL is the parent company of PIP. Violation of this Manual may result in disciplinary action.

2 Purpose

The Financial Services Regulatory Authority ("**FSRA**") of Abu Dhabi is PIP's home country regulator and supervisor which requires that a regulated firm to comply with not only its requirements in its AML and Sanctions Rules and Guidance but also with applicable rules and standards such as (but not limited to):

- Establishing and maintaining effective AML policies, procedures, systems and controls to prevent opportunities for money laundering, in relation to PIP and its activities;
- Taking reasonable steps to ensure that its employees comply with the relevant requirements of its AML policies, procedures, systems and controls;
- Reviewing the effectiveness of its AML policies, procedures, systems and controls;
- Applying a risk-based approach to AML;
- Assessing business AML risks, taking into consideration the nature, size and complexity of its activities;
- Applying risk-based assessment of clients to determine the level of risk it presents to PIP;
- Undertaking Client Due Diligence ("**CDD**").

3. Scope

This policy applies to PIP, its directors, officers and all its employees including, without limitation, every individual holding a licensed function as well as outsourced functions. Employees must ensure that they understand their individual roles and responsibilities as outlined in this Manual.

4. AML Manual Acknowledgement

Upon joining PIP and on an annual basis thereafter, employees are required to sign the Compliance and AML Manual Acknowledgement Form, **confirming** that they agree to be bound by the procedures set out in both Manuals and the FSRA AML Module to the extent that they apply.

Refer to Annex 1 of the Compliance Manual for the Compliance and AML Manual Acknowledgement Form.

5. AML and Client/Investor Identification Procedures

In addition to this Manual, PIP has developed AML Risk Assessment and Client Identification Procedures to assist PIP's personnel and the MLRO in undertaking the enquiries and analysis required to properly assess the AML and CFT risks associated with a client.

The Procedures are outlined in Part Two of this Manual.

6. Review

This Manual will be reviewed on an annual basis with reviews done more frequently on an ad hoc basis in case of regulatory updates, operational and/or business activities by the MLRO. This review forms part of PIP's annual compliance monitoring program.

7. Overview of Applicable Laws and Regulations

This Manual is designed to include guidance on compliance with the laws of the United Arab Emirates ("**UAE**"), ADGM and regulations of the FSRA and other relevant international AML and CFT and sanctions laws, rules and regulations.

7.1. Applicable Laws & Regulations

There are several AML and CFT laws, rules and regulations that apply to PIP. The key laws and regulations are mentioned below:

- UAE Ministry of Finance ("MoF") Cabinet Decision No. (10) of 2019 Concerning the implementing regulation of decree law no. (20) of 2018 on anti-money laundering and combating the financing of terrorism and illegal organisations;
- UAE Ministry of Finance ("MoF") Cabinet Resolution No. 74 of 2020 concerning the UAE list of terrorists and implementation of UN Security Council decisions relating to preventing and countering financing terrorism and leveraging non-proliferation of weapons of Mass Destruction and Related Resolutions;
- UAE Ministry of Finance ("MoF") Cabinet Resolution No. 50 of 2020 concerning the control list annexed to Federal Law No. 13 for 2007 relating to commodities subjected to Import and Export Control.
- UAE Federal Decree by Law No. 20 of 2018 on Anti Money Laundering, Combating the Financing of Terrorism and Financing of Illegal Organizations;
- UAE Federal Decree Law No. 43 of 2021 on the Commodities Subject to Non-Proliferation;
- UAE Ministry of Economy ("MoE") Federal Decree No. 26 of 2021, Amending Certain Provisions of Law No. 20 for 2018 on Anti-Money Laundering and Countering the Financing of Terrorism;
- UAE Ministry of Finance ("MoF") Cabinet Decision No. (74) of 2020 concerning the UAE list of terrorists and implementation of the UN Security Council decisions relating to preventing and countering financing terrorism and leveraging non-proliferation of weapons of mass destruction;
- UAE Federal Law No. 7 of 2014 on Combating Terrorism Offences;
- UAE Federal Law No. 13 of 2007; concerning Commodities subject to Import and Export control and its amendments including Federal Law No. 12 of 2008.
- The FSRA Anti-Money Laundering and Sanctions Rules and Guidance (AML) Rulebook;
- All communications from the Executive Office for Control and Non-Proliferation and the Committee for Goods and Materials Subject to Import and Export Control (CGMSIEC).

- Other FSRA rules regarding Anti-Money Laundering, Counter-Terrorist Financing and Sanctions and;
- Any other UAE laws and Federal legislations relating to money laundering, terrorist financing, the financing of unlawful organizations or sanctions non-compliance.

Under these laws, PIP and its employees may be criminally liable for the offence of money laundering if such an activity is committed in its name or for its accounts. PIP and its employees may also be liable for breaches of FSRA rules and potentially breaking UAE laws, if PIP and its employees fail to abide by this Manual and other related procedures that are aimed at preventing money laundering and other types of financial crime. PIP and its employees must also keep in mind that failure to report suspicions of money laundering, "tipping off" or assisting in money laundering may each constitute a criminal offence that is punishable under the laws of the UAE.

8. Applying a Risk-Based Approach ("RBA")

To ensure that PIP appropriately address the AML and CFT risks originating from its business, it has adopted an RBA. This approach takes into consideration the business, type of clients, their domicile, and the way PIP engages with its clients. The senior management of PIP commits to:

- establishing clear standards for accepting clients which may involve Enhanced Due Diligence (EDD) as the risk of the client increases;
- establishing procedures relating to client identification and screening against databases to assess customer risk;
- procedures relating to client risk assessment that justify the establishment of a business relationship with PIP;
- providing clear guidance when and under what conditions reliance can be placed on the AML/Know Your Customer (KYC) profiling or screening performed by affiliated entities or external third parties;
- establishing procedures to determine whether to exit a client relationship as a result of AML and CFT risks; and
- appointing a MLRO who would be responsible for the oversight and reporting of AML/KYC activities within and on behalf of PIP.

The RBA consists of two elements which are highlighted below:

8.1. Business AML Risks

The first step in assessing the AML and CFT risks is for PIP to take a holistic view of the business by assessing the nature, size, and complexity of the business activities. PIP has created a risk-based model which covers the following parameters:

- types of clients and their activities;
- countries or geographic areas in which we do business;
- products, services and activity profiles;
- distribution channels and business partners;
- complexity and volume of transactions;
- new products, business practices, delivery mechanisms, channels and partners; and
- the use of new or developing technologies for both new and pre-existing products and services.

PIP also takes appropriate measures to ensure that any risks identified in the assessment are considered in day-to-day operations and mitigated when taking on new clients, developing new products, services, business practices and technologies, or when other changes occur in PIP's business profile. PIP also takes into consideration the UAE's National Risk Assessment (NRA) while identifying its risk factors.

In addition to the above risk model, the MLRO conducts a subjective review of the AML risks facing PIP and documents the result in the final risk assessment produced for the Board's review and approval.

Furthermore, the information obtained through the business risk assessment is used to develop and maintain this policy and all related procedures. The business risk assessment ensures that AML and CFT controls adequately mitigate the risks identified as part of the annual assessment. It also provides a framework to assess the effectiveness of the AML and CFT program and assists in the prioritization and allocation of resources.

8.2. Client and Business Partner Risk

PIP obtains verification documents and perform CDD for all new clients and partners.

The MLRO also performs annual reviews of the CDD process and the documentation on file. This annual assessment forms part of the larger review exercise conducted to produce the Annual AML Return and Semi Annual MLRO Report required by the FSRA.

To ensure that PIP takes on clients in line with its risk profile, a risk-based assessment ("RBA") is conducted on each client. The outcome of this process produces a risk rating for the client, which determines the level of CDD to be applied to that client.

PIP will not establish a business relationship with any client where the client's ownership or control arrangements prevent the identification one or more of the client's beneficial owners.

Procedures for the RBA and the different risk factors included in the risk scoring model can be found in Part Two of this Manual.

A copy of the KYC identification requirements form can be found in Part Three of this Manual.

9. Client Due Diligence

CDD is the process of:

- verifying the identity of a client and beneficial ownership (including any person purporting to act on behalf of the client);
- understanding the purpose and intended nature of the business relationship;
- understanding the client's source of funds and source of wealth;
- performing adequate checks against sanctions lists; and
- undertaking on-going due diligence of the client business relationship.

The level of CDD to be undertaken (both initially and for the duration of the business relationship) is determined by reference to the client's risk rating assigned under the Client Risk Assessment in Part 2 of the Manual.

There are two levels of CDD: Standard (for low and medium risk clients) and Enhanced (for high-risk clients).

9.1. Client Identification Procedures

The Manual establishes, and maintains reasonable procedures designed to verify clients' identities to the extent reasonable and practicable (such procedures are referred to generally as "**Client Identification Procedures**"). The Client Identification Procedures undertaken with respect to PIP's clients should consider the specific risks presented by each of them.

PIP is licensed to deal with professional clients ("Professional Clients") and market counterparties ("Market Counterparties") as defined in the FSRA Conduct of Business Rules and most of PIP's clients are financial institutions, governments and large corporates with operations in Africa.

9.2. Business Partner Identification

Prior to establishing the business relationship, PIP must establish and verify the identity of its business partners by obtaining sufficient and satisfactory evidence of the identity of any business partner it relies upon in carrying on some or part of its regulated activities. If the business partner is a financial institution, PIP must verify that the business partner is authorised to conduct the activity it has been mandated to carry out and regulated by a relevant financial services regulator.

Within the context of the Anti-Money Laundering and Sanctions Rules and Guidance (AML) Rulebook, a 'business partner' includes:

(a) a qualified professional;
(b) a member of PIP's related group entity
(c) a Correspondent Bank; or
(d) any other service provider

Similar documentations used to identify and verify clients should be obtained from the business partner prior to any engagement. This includes maintaining accurate and up-to-date information and conducting on-going due diligence on its business partners, throughout the course of the business relationship.

At any time, PIP lacks sufficient information or documentation concerning a business partner's identity or develops a concern about the accuracy of the information or documentation, it must promptly obtain appropriate material to verify such business partner's identity. PIP should also find out whether any secrecy or data protection laws exists in the country of incorporation of the business partner that would prevent access to relevant information.

Appropriate provisions will be included in PIP's due diligence questionnaires to help PIP achieve the objectives of its Client and Business Partner Identification Procedures.

9.3. Sanctions and Other International Obligations

PIP will ensure compliance with all applicable local and international sanctions requirements by reviewing each new client and any beneficial owners against sanctions lists issued by the United Nations Security Council, UAE government, government agencies, the UAE Central Bank, EU, UK (Sanctions and Anti-Money Laundering Act 2018), Singapore, U.S. OFAC and the FSRA. This process is repeated regularly as part of ongoing monitoring of the business relationship with clients.

The MLRO will monitor and review any relevant resolutions or sanctions applicable under the UAE or ADGM laws, or where applicable to any other jurisdiction. Relevant resolutions or sanctions may, among other things, relate to money laundering, terrorist financing or the proliferation financing of weapons of mass destruction.

In the event that PIP becomes aware that it has or is about to enter into a business relationship with a person or entity which may constitute a contravention of any relevant resolution or sanctions, the MLRO will assess the circumstances and escalate to the SEO to determine whether to continue with that business relationship. This assessment and any proposed action will be documented in writing by the MLRO.

The MLRO will also notify the FSRA in writing and provide the following information:

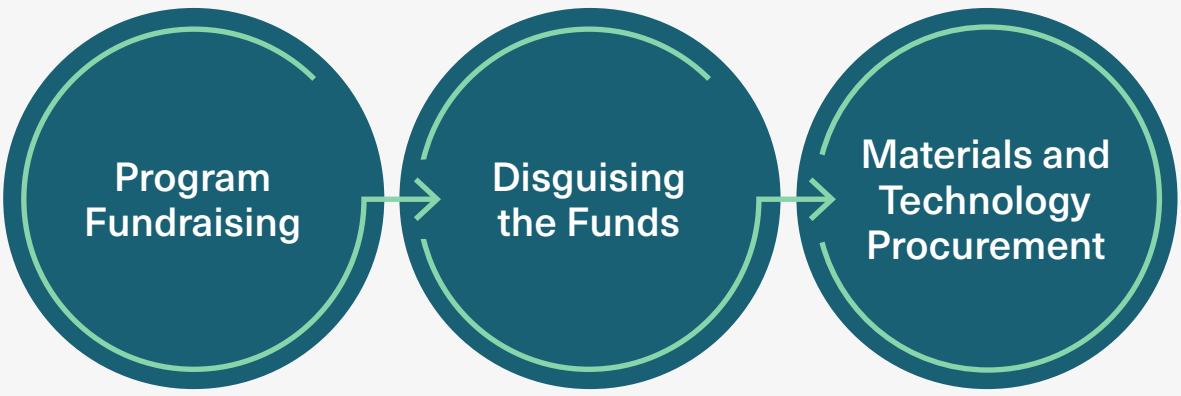
- a description of the relevant activity; and
- the action proposed to be taken, or that has been taken by PIP in regard to the matters specified in the notification.

9.3.1 Counter Proliferation Financing

Proliferation Financing ("**PF**") can be referred to as the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of weapons of mass destruction (WMD) proliferation, including the proliferation of their means of delivery or related materials (including both Dual-Use technologies and Dual-Use goods for non-legitimate purposes).

"**WMD Proliferation**" means the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both Dual-Use technologies and Dual-Use goods used for nonlegitimate purposes).

PF have 3 stages:



1. **Stage 1 - Program Fundraising** – Here, a proliferating country raises financial resources for in-country costs. The funding sources may derive from the proliferating country's budget, profits from an overseas commercial enterprise network, and/or proceeds from an overseas criminal activity network.

2. **Stage 2 - Disguising the Funds** – Here the proliferating state moves assets into the international financial system, often involving a foreign exchange transaction, for trade purposes. A proliferating country may use means that range from the simpler to the more complex, including using normal correspondent banking channels or an intricate network of procurement agents and front companies. During this stage, states that are subject to comprehensive sanctions will seek to circumvent such sanctions, often using sophisticated methods to disguise the funds.

3. **Stage 3 - Materials and Technology Procurement** - The proliferating state or its agents use the disguised resources for procurement of materials and technology within the international financial system. This stage also includes the payments for shipping and transport of materials and technology.

PF risks are assessed based on the following factors: threat, vulnerability, and consequence.

A. PF Threat - refers to designated persons and entities that have previously caused or have the potential to evade, breach, or exploit a failure to implement Targeted Financial Sanctions ("**TFS**") related to proliferation. Such threats may also be caused by those persons or entities acting for or on behalf of designated persons or entities.

   As part of its AML Business Risk Assessment, PIP collates a list of major known or suspected threats, key sectors, products, or services that have been exploited, types of activities that designated individuals/entities have engaged in, and the primary reasons why designated persons and entities have not been deprived of their assets or identified. The assessment also takes into consideration the extent and type of PF threats faced by PIP via its customer base, product and service offerings, and geographical region.

   PIP also takes into consideration its direct exposure to known PF threats and potential exposure to other legal activities that may be exploited by PF threat actors. As part of its PF identification, PIP uses the information collated as part of its due diligence process (initial and ongoing CDD).

B. PF Vulnerabilities - refers to matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation, or evasion of TFS related to proliferation. Vulnerabilities may include features of a particular sector, a financial product, or type of service that make them attractive for a person or entity engaged in the breach, non-implementation, or evasion of TFS related to proliferation.

   PIP, as part of its AML Business Risk Assessment also collates a list of key PF vulnerabilities which are based on its business structure, business sector, products and services, customers and transactions to identify its PF vulnerabilities.

C. PF Consequences - refers to the outcome where funds or assets are made available to designated persons and entities, which could ultimately allow them, for instance, to source the required materials, items, or systems for developing and maintaining illicit nuclear, chemical, or biological weapon systems (or their means of delivery), or where frozen assets of designated persons or entities would be used without authorisation for PF. A consequence may include reputational damage to PIP.

9.4. Timing of CDD

For all new clients, CDD must be gathered by or prior any business relationship is formalized, e.g. by the signing of a client agreement or formal acceptance by a fund's General Partner.

Exceptionally, subject to the MLRO and the Board's approval, CDD may be completed after this time if:

- deferral is necessary for a time-critical transaction that, if not executed immediately, would or may cause a financial loss to the client due to a price movement or loss of opportunity.
- there is little money laundering risk, or any identified risk is effectively managed; and
- the CDD is completed within 30 days from entering the business relationship.

Where the CDD is not completed within 30 days, PIP must, prior to the end of the 30-day period, document the reason for not meeting this timeframe and complete the CDD as soon as possible.

9.5. Failure to Conduct or Complete Client/Customer Due Diligence

It is PIP's policy not to deal with clients where the CDD process cannot be completed. Where such a situation arises and where a decision is made not to deal with the client due to suspicions of illicit activities, the MLRO will consider whether the situation necessitates filing a Suspicious Activity Report ("**SAR**").

9.6. Ongoing Client Due Diligence

PIP undertakes ongoing CDD for all clients. The frequency of this review depends upon the client risk rating. The ongoing CDD ensures that client information remains accurate, and that PIP can assess the client's transaction pattern against their business and current client risk rating. This ongoing process allows us to ensure that where required, changes to client risk ratings are made at reasonable intervals, particularly where the client is moving from low or medium risk to a high-risk rating.

9.7. Allocation of Responsibilities Between the Parties

Contractual agreements with third parties such as placement agents or administrators should clearly state the responsibilities for compliance with applicable AML laws and regulations including those in the home jurisdiction of the fund, the third-party and PIP.

Contractual agreements with third parties should also seek to establish effective lines of communication for addressing client due diligence issues and suspicious activities that may arise and provide a means by which PIP may periodically verify or audit the third-party's compliance with its AML policies, procedures and controls.

Procedures for Client Identification can be found in Part Two of this Manual.

10. Roles and Responsibilities

10.1. Money Laundering Reporting Officer

Role	Name	Email	Phone
MLRO			
Deputy MLRO			

Through this Manual, we have mandated the MLRO and in his absence the Deputy MLRO (DMLRO):

- to have direct access to the Board.
- to determine the level of resources required to perform his duties in an effective, objective and independent manner.
- to have status of Senior Manager to enable him to act on his own authority; and
- to have unrestricted access to information sufficient to enable him to carry out his responsibilities.

10.2. Responsibilities of the MLRO

The MLRO has the following responsibilities:

- Day-to-day operations for PIP's compliance with the relevant AML and CFT rules and regulations.
- Executes a thorough and appropriate AML Compliance Risk Assessment for PIP, its products, customer base, countries it has business with, its business third-party relations and delivery channels and assign a risk rating to each.
- Based on the results of the AML Compliance Risk Assessment, adopts appropriate risk management controls and procedures to adequately avoid exposing PIP to any material risks related to money laundering, terrorism financing, proliferation financing, and financing of illicit organizations and entities.
- Oversees appropriate CDD for all Politically Exposed Person's ("**PEP**"), or PEP-related individuals and obtain the approval of the SEO for client acceptance.
- Acts as the point of contact to receiving and acting upon any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices, or other conclusions regarding the prevention of money laundering.
- Receive suspicious transaction alerts from employees and analyse them to take appropriate actions and decisions to report all suspicious cases such as filing a SAR or Suspicious Transaction Report (STR).
- On-going monitoring of transactions to identify high-risk, unusual and suspicious customers/transactions.
- Provide necessary reports to the Board, SEO and Legal and Compliance on all AML/CFT issues, on a quarterly basis at a minimum.

- Acts as the point of contact in relation to AML and CFT queries originating from any UAE authorities and is responsible for promptly responding to such requests.
- Reviews the Manual on an annual basis to ensure that it remains up to date in relation to the laws and regulations but also takes into consideration the recommendations from international bodies such as the FATF and Wolfsberg forum.
- Conducting appropriate AML training.
- The general administration of this Manual.
- Review all reports submitted pursuant to this Manual, answer questions regarding procedures set forth in the Manual, update this Manual as required from time to time, and arrange for appropriate records to be maintained, including copies of all reports submitted under this Manual.
- Reviewing at least annually, the adequacy of the procedures of PIP and the effectiveness of implementation.
- Investigate any possible violations of the procedures in this Manual to determine whether disciplinary actions should be imposed, including, inter alia, a letter of censure or suspension or termination of employment of the violator, or such other course of action as may be appropriate.
- Ensure the filing and updating of all required forms and documents as applicable under the laws and regulations of the various jurisdictions under which PIP operates; and
- Reporting to the Board and FSRA on the status of PIP's compliance with relevant AML laws and rules, and for ensuring that all communication with the FSRA is done in an open and cooperative manner, disclosing any information the FSRA would reasonably expect to be notified.

Furthermore, the following circumstances must be brought to the attention of the MLRO immediately, in case of:

- Any complaint, whether written or oral, relating to AML and CFT. Any response to such complaints must be in writing and requires the approval of the MLRO.
- Any inquiry from any member of the press relating to AML and CTF matters; and
- In the event any federal, state, or self-regulatory organisation contacts PIP (either in writing or by telephone) or arrives for an inspection.

10.3. MLRO Reporting Requirements

The MLRO will report to the Board on a quarterly and semi-annually basis, regarding the status of AML and CFT compliance. The following reports are to be presented to the Board and the ARCC:

10.3.1. MLRO Semi-Annual AML Report

The MLRO is required to report semi-annually to Board of PIP on:

- The results of any reviews on the quality of PIP's AML Procedures (including the review referred to in section 8 of the Manual).
- PIP's compliance with applicable AML legislation and regulations.
- Any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices, or other conclusions and how PIP takes them into account.
- Any internal Suspicious Activity Reports and the action taken in respect of those reports, including the grounds for the actions taken.
- Any external Suspicious Activity Reports made by PIP and the action taken in respect of those reports, including the grounds of the actions taken; and
- Any other relevant matters related to money laundering relevant to PIP.

The Board must assess the report, take appropriate action on the findings of the report, and resolve any identified deficiencies, and then make a record of such assessment and actions taken.

10.3.2. Annual AML Return

The MLRO prepares an annual AML return which is submitted to the FSRA by 30th April each year. This return includes details regarding the status of the AML and CFT program, key issues, policy and procedural updates and the nature and type of clients PIP has taken on in the previous year.

11. Training and Awareness

To maintain an effective AML and CFT program, it is imperative that all employees understand this Manual and are trained to identify and report suspicious activity. To achieve these goals, PIP provides AML training to new employees as soon as reasonably practical upon joining PIP, and annually for current employees.

The AML training covers the following topics:

- UAE AML law and FSRA legislation relating to money laundering;
- PIP's AML Manual;
- Who are the MLRO and Deputy MLRO, and their duties and responsibilities;
- How to recognise and deal with transactions, risks, trends, techniques and other activities which may be related to money laundering;
- Understanding the types of activity that may constitute suspicious activity;
- How to make notifications to the MLRO;
- Prevailing techniques, methods, and trends in money laundering;
- Understanding each employee's role in combating money laundering.

12. Suspicious Activity Reports

This Manual requires all employees to monitor and report suspicious activity or transactions in relation to potential money laundering or terrorist financing.

Each employee is required to promptly notify and provide the MLRO with all relevant details of any incident in which the employee knows, suspects, or has reasonable grounds for knowing or suspecting that a person (whether a client or not) is engaged in, or attempting money laundering or terrorist financing. Reportable incidents also include when no business relationship was developed due to suspicious circumstances. An employee may consult with their line manager in deciding whether the circumstances merit notifying the MLRO about a suspicious transaction or activity. However, the employee ultimately decides whether the MLRO should be notified, and the employee should not be prevented or dissuaded from doing so if they know, suspect, or has reasonable grounds for knowing or suspecting that a person connected to PIP may be involved in money laundering.

Failure to report a suspicious transaction is a serious breach of duties and will result in disciplinary action. Procedures for Suspicious Activity Reporting can be found in Part Two of this Manual.

12.1. Filing Suspicious Activity/Transactions Reports ("SAR"/"STR")

The MLRO starts the investigation within 24 hours of receiving a suspicious transaction notification via the Internal Suspicious Activity Report. The investigation may involve reviewing CDD documents, transaction history, speaking to employees and any other action the MLRO deems relevant for the assessment. If the investigation results in a decision to file the Suspicious Activities Report/ Suspicious Transaction Report ("**SAR"/"STR**"), the MLRO will do so with the UAE Central Bank Financial Intelligence Unit (CBUAE FIU) via the GoAML portal. The MLRO will also notify the Board of the actions taken.

Where, after receipt of the Internal SAR/STR and based on the results of the investigations, the MLRO decides not to file an external SAR/STR, the MLRO will document the reasons for such determination and notify the Board.

PIP appoints the MLRO with the authority to decide if the SAR/STR is to be filed in consultation with Legal and Compliance.

All relevant details of any internal or external SAR/STRs must be kept for at least six years from the date the report was made.

12.2. Tipping-off

Tipping-off is defined as an unauthorized act of disclosing information that may result in PIP, client, or a third-party (other than the FIU or the Regulator), knowing or suspecting that PIP, client or third party is or may be the subject of a suspicious transaction report or an investigation relating to money laundering or terrorism financing, and may prejudice the prevention or detection of offences, the apprehension or prosecution of offenders, the recovery of proceeds of crime, or the prevention of money laundering or terrorism financing.

All employees are reminded that they must not tip-off any person. This means that they must not inform any person, whether a natural person or a legal entity, that they are being scrutinized for possible involvement in suspicious activity related to money laundering, or that any government agency is investigating their possible involvement in suspicious activity relating to money laundering.

If an employee reasonably believes that performing CDD will tip-off a client or potential client, the employee may choose not to proceed with the CDD in consultation with the MLRO. The MLRO, will also have to decide whether an SAR should be filed.

13. Targeted Financial Sanctions (TFS)

Targeted Financial Sanctions refers to both **asset freezing** and **prohibitions** to prevent funds or other assets from being made available, directly, or indirectly, for the benefit of sanctioned individuals, entities or groups. Its purpose is to is to deny certain individuals, entities, or groups the means to violate international peace and security, support terrorism or finance the proliferation of weapons of mass destruction. To achieve this, it seeks to ensure that no funds or other assets or services of any kind are made available to designated persons for so long as they remain subject to the targeted financial sanctions measures.

13.1. Asset Freezing

Asset Freezing is the prohibition to transfer, convert, dispose, or move any funds or other assets that are owned or controlled by designated individuals, entities, or groups in the Local Terrorist List or UN Consolidated List. It includes the freezing of funds, other financial assets and economic resources preventing their use, alteration, movement, transfer, or access. The freezing of economic resources also includes preventing their use to obtain funds or other assets or services in any way such as selling or mortgaging the economic resources.

13.2. Prohibition

This refers to the prohibition to provide funds or other assets to or render financial or other services to, any designated individual, entity, or group. The freezing measures, including the prohibition of making funds or other assets or services available, apply to:

A. Any individual, entity, or group designated in the Local Terrorist List issued by the UAE Federal Cabinet or designated by the UNSC in the UN Consolidated List.
B. Any entity directly or indirectly owned or controlled by an individual, entity, or group designated under point (A).
C. Any individual or entity acting on behalf of or at the direction of any individual, entity, or group designated under points (A) & (B).

In instances where an asset is owned or controlled in part or in full by a designated individual, entity, or group and such assets produce benefits in the form of income such as dividends or interest, the relevant portion of such benefit is also subject to freezing measures.

'Funds or other assets' here includes (but not limited to);

- financial assets;
- economic resources (including oil and other natural resources);
- property of every kind, whether tangible or intangible, movable or immovable, with legal documents or instruments in any form (including electronic or digital formats) evidencing title to, or interest in;
- funds or other assets, including, but not limited to, bank credits, traveller's cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets,
- any other assets which potentially may be used to obtain funds, goods or services.

NOTE: Asset freezing and prohibition measures have no time limit. The funds or other should remain frozen, and the prohibition from making funds or other assets or services available remains until the individual, entity, or group is removed from the Local Terrorist List or the UN Consolidated List or until there is a freezing cancellation decision made by a competent authority or the UNSC.

The information on designated individuals, entities, or groups can be found on the following (but not limited to) Lists:

- The Executive Office for Control & Non-Proliferation's (EOCN)'s Local Terrorist List (designated by the UAE Cabinet).
- The United Nations Sanctions Committees (UNSC) Consolidated List which includes all the sanctioned individuals, entities, or groups designated by the United Nations Sanctions Committee.

PIP has subscribed to the EOCN Notification System via the EOCN's website to receive automated email notifications on any updates to the Sanctions Lists.

13.3. Penalties

A firm found in violation with the obligations set out in the Cabinet Decision No. 74 of 2020 relating to TFS or failing to implement procedures to ensure compliance with TFS rules, laws and guidelines, will be subject to the following:

- Imprisonment of no less than one year and no more than seven years and/or a fine of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham). Other administrative penalties by the relevant supervisory authorities are as follows:

a. Letter of warning.
b. Administrative penalties of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) for each violation.
c. Banning the offender from working in the sector related to the violation for the period determined by the Supervisory Authority.
d. Constraining the powers of the board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointment of a temporary inspector.
e. Suspend managers, board members and supervisory and executive management members who are proven to be responsible for the violation for a period to be determined by the Supervisory Authority or request for their removal.
f. Suspend or restrict the activity or the profession for a period to be determined by the Supervisory Authority.
g. Cancel the financial license.

However, where a Firm applies all the freezing measures and executes the actions (post freezing of assets) as prescribed by the Cabinet Decision No. 74 of 2020, the TFS Guidance issued by the Executive Office for Control & Non-Proliferation (EOCN), shall be exempt from any damages or claims, resulting from such actions, including penal, civil, and/or administrative liability.

14. Review of AML/CFT Procedures

PIP will conduct regular reviews and assessments of the effectiveness and compliance with PIP's AML framework, and will specifically cover the following:

- Sample testing of compliance with PIP's CDD arrangements.
- An analysis of all notifications made to the MLRO to highlight any area where procedures or training may need to be enhanced; and
- a review of the nature and frequency of the dialogue between the Senior Management and the MLRO.

The reviews will be carried out at least annually and the results will be reported to the Board.

The MLRO, under the supervision of the Board, will conduct the appropriate follow-up to ensure that any deficiencies detected during the review are addressed and rectified.

15. Regulatory Requests

PIP and its employees shall be open and cooperative in their dealings with the FSRA. PIP will inform the FSRA in writing if, during its activities within the ADGM it:

- Receives a request for information from a regulator or agency responsible for AML, counter-terrorism, sanctions, or bribery regarding potential breaches by PIP.
- Becomes aware or suspects that money-laundering, terrorism financing, a sanctions breach, or an act of bribery has occurred or may occur in PIP's business.

- Becomes aware or suspects that another person outside of its business is engaged in money-laundering, terrorism financing, a sanctions breach, or an act of bribery unless these the information is legally privileged or in the public domain.
- Becomes aware of any money laundering or sanctions matters in relation to PIP which could result in adverse reputational consequences; or
- Becomes aware of any significant breach of the FSRA AML Module or UAE legislation.

16. Record Keeping

As part of the FSRA requirements, PIP should retain information for at least six (6) years from the date which a notification or report was made, when a business relationship ends, or a transaction is completed. The following information must be retained:

- A copy of all documents and information obtained in initial and ongoing CDD;
- Supporting records for CDD;
- Notifications made relating to potential money laundering activities;
- Suspicious Activity Reports and any relevant supporting documents and information.
- Any relevant communications with the UAE Central Bank Financial Intelligence Unit.
- The documents in relation to business AML risk assessments, client AML risk assessments and how these assessments were used to arrive at decisions;
- The relevant details of any transaction carried out for a client; and
- Complete, current and accurate log of all business partners PIP uses.

In respect of training records, PIP must retain the:

- The dates when the training was given;
- The nature of the training;
- The training material; and
- The names of employees who received the training.

PIP may keep such records in an electronic format provided such records are readily accessible and available in the event of FSRA's request for information.

Where such records are held outside of the ADGM, PIP must ensure that records are held consistent with this requirement and be readily accessible and available for inspection by the FSRA. Should access to such records be restricted due to secrecy or data protection legislation, PIP will obtain certified true copies.

17. No Retaliation Policy

It is PIP's policy to not prejudice in any way the standing of a staff member, who discloses information regarding money laundering to any relevant regulatory authority, government agency or to any other relevant body involved in the prevention of money laundering.

Premier Invest

2

PART TWO

ANTI-MONEY LAUNDERING RISK ASSESSMENT AND CLIENT IDENTIFICATION PROCEDURES

1 Introduction

The Anti-Money Laundering ("AML") Risk Assessment and Client Identification Procedures guides Premier Investment Partners (herein referred to as "PIP") in complying with the Anti-Money Laundering & Counter Terrorist Financing ("CTF") laws, rules and regulations of the United Arab Emirates ("UAE") and the Financial Services Regulatory Authority ("FSRA") the sole independent regulator of all financial and ancillary services conducted in or from the Abu Dhabi Global Market ("ADGM").

In addition to the AML & Client Identification Procedures, PIP has developed the AML Manual, which sets out the compliance framework based on applicable legal and regulatory requirements to prevent PIP, its employees and clients from being misused for money laundering, terrorist financing or other financial crime.

To counter the money-laundering risks to the business, PIP's senior management has adopted a risk-based methodology that entails the following components:

- AML Business Risk Assessment.
- AML Client Risk Assessment; and
- Client Due Diligence (CDD) standards.

PIP utilize these components to assess AML risks to its business and to take reasonable steps to manage these risks. The results of the Business and Client Risk assessments feed into the CDD requirements applied to each new and existing client relationship.

2. Business AML Risk Assessment

A key aspect of PIP's AML risk management is the Business AML Risk Assessment. The MLRO conducts the Business AML Risk Assessment annually (or earlier if there is a significant change in the business that warrants a review) and it is approved by the Board.

The Business AML Risk Assessment is conducted by assessing a range of factors and determining a risk score for each factor. A risk assessment spreadsheet is used to calculate an overall score for each factor to arrive at the overall Business AML risk of PIP.

Each element has been given a risk rating based on the inherent and money laundering risks associated with it.

- Risk scores of 0 – 3.99 are deemed Low Risk.
- Risk Scores of 4 – 6.99 are deemed Medium Risk.
- Risk Scores of 7 – 10 are deemed High Risk.

The following elements are used in the Business AML Risk Assessment:

- Types of clients and their activities i.e. Customer Risk.
- Counterparty Risk (i.e. foreign correspondent banks, financial institutions, agents, etc.)
- Countries or geographic areas in which we do business i.e. jurisdictional or country risk.
- Products and services offered i.e. product risk.
- Distribution channels and business partners i.e. delivery channel risk or interface risk.
- Complexity and volume of transactions.
- New products, business practices, delivery mechanisms, channels and partners; and
- New or developing technologies for both new and pre-existing products.

These factors are discussed in more detail below.

2.1. Types of Clients

Type of Client	Risk Rating
Legal Entities – Regulated – Non-equivalent Regulator	Medium Risk
Individuals	High Risk
Legal Entities – Unregulated	Medium Risk
Government Majority Owned (US, Western Europe, GCC)	Low Risk
Government Majority Owned (Other Countries)	Medium Risk
Legal Entities – Regulated – Equivalent Regulator	Low Risk
Legal Entities – Listed	Medium Risk

2.1.1. Natural Persons

To confirm the identity of a natural person, PIP will take reasonable steps to ascertain the client's name, address, and date of birth such as by requesting for official driver's license with photograph, passport or other government issued identification document.

In certain circumstances, additional information to verify a client's identity, address and background may be requested by the MLRO from the client, persons with close engagement with the client, or other information sources such as reports from credit bureaus.

PIP should also understand the client's business/occupation and their source of funds/wealth. If the client's income is from a business venture, PIP should understand the nature of that business.

2.1.2. Corporations, Partnerships and Comparable Legal Entities

The identity of a legal entity is verified based on the entity's name and address and its authority to make the contemplated investment. If the client is neither a publicly traded firm listed on a recognized exchange (or a subsidiary or a pension fund of such a firm) nor a regulated institution organized in a FATF-compliant jurisdiction (as defined in Part Four), PIP's MLRO may require additional information regarding the client's identity by obtaining any of the following, as deemed appropriate under the circumstances:

- evidence that the client has been duly incorporated in its jurisdiction.
- if the MLRO believes it would be reasonable to rely on a certification from the client, a certification from the client that it has implemented and comply with AML policies, procedures and controls that, for example, seek to ensure that none of its directors, officers or equity holders are Prohibited Clients, as set forth below, or, alternatively, a list of directors, senior officers and principal equity holders (in order for the MLRO to perform appropriate due diligence to determine that none of these persons is a Prohibited Client;
- description of the client's primary lines of business and how they derive their revenue.
- publicly available information from law enforcement agencies or regulatory authorities; or
- client's financial statements and/or bank references.

2.1.3. Prohibited Clients

PIP may not accept any form of financial assets from nor engage with the following:

- Any customer whose name appears on:
  - The List of Specially Designated Nationals and Blocked Persons maintained by the OFAC (as defined in Part Four).
  - Other Sanctions lists (see section 4.3).
  - Entities/Individuals within jurisdictions on the FATF's Blacklist.
  - Other lists of prohibited persons and entities may be mandated by applicable law or regulation.

Note: PIP must update the information that it maintains and relies upon for the purpose of checking the above lists in order to ensure that it does not engage with a Prohibited Client. PIP may consider using a third-party compliance service for assistance with monitoring prohibited lists.

- Foreign Shell Banks – Financial assets from or on behalf of a Foreign Shell Bank (as defined in Part Four) should not be accepted. With respect to clients that are Foreign Banks (as defined in Part Four), the MLRO should consider obtaining a representation that the bank either (i) has a Physical Presence (as defined in Part Four); or (ii) does not have a Physical Presence but is a Regulated Affiliate (as defined in Part Four).

2.1.4. Anonymous & Nominee Accounts

It is PIP's policy not to establish or maintain:

- an anonymous relationship/account or an account/relationship in a fictitious name.
- a nominee account which is held in the name of one person, but which is controlled by or held for the benefit of another person whose identity has not been disclosed: and
- an account with a Shell Bank.

2.1.5. Other Prohibitions

- Inadequate or incorrect KYC information.
- Not furnishing adequate information by the customer.
- Non-cooperation by the customer to provide KYC onboarding documents or other evidence.

2.2. Regions & Geographies

PIP may deal with clients originating from many different jurisdictions. Each jurisdiction is assigned a risk rating calculated using Transparency International's Corruption Perceptions Index.

Regions & Geographies	Risk Rating
GCC	Medium Risk
MENA (excluding GCC)	High Risk
EU & Western Europe	Medium Risk
Asia-Pacific	Medium Risk
Sub-Saharan Africa	High Risk
North America	Low Risk
Central & S America	High Risk
Eastern Europe & Central Asia	High Risk

2.3. Products, Services and Activity

The products or services offered are neither unusual complex, serving a clear economic purpose and are not particularly subject to fraud and market abuse. As a result, the services and product risk rating are therefore considered to be low/medium.

PIP will engage in advising clients and arranging deals in investments for and/or on behalf of its clients as an Investment Advisor and Arranger in the ADGM.

Products, Services and Activity	Risk Rating	
Advising on Investments or Credit	Low/	Medium
Arranging Deals in Investments	Low/	Medium
Arranging Credit	Medium	
Managing a Collective Investment Fund	Medium	

2.4. Distribution Channels and Business Partners

PIP does not expect to conduct business predominantly on a face-to-face basis with its clients. PIP will however ensure that CDD is performed prior to commencing any relationship with any client.

Distribution Channels	Risk Rating	
Face-to-Face	Low Risk	
Virtual	Low/	Medium

2.5. Complexity and Volume of Transactions

Complexity and Volume	Risk Rating
Not Complex	Low Risk
Complex	Medium Risk

2.6. New Products, Practices, Including New Delivery Mechanisms, Channels and Partners

New products, practices or technology	Risk Rating
No	Low Risk
Yes	Medium Risk

2.7. Overall Business Risk Assessment Score

The Business AML Risk Assessment calculator is available upon request from the MLRO with a template of the Business AML Risk Assessment available within the Annexes to this Manual.

3. Client Risk Assessment

This section describes the risk-based assessment that must be undertaken on a client and the process which PIP risk rates a client. This risk rating is used to determine the level of CDD that will apply to that client.

CDD in this context refers to the process of identifying a client, verifying its identity through documentation, and monitoring the client's business and money laundering risk on an on-going basis.

The risk assessment (and assignment of risk rating) is performed as part of the due diligence which must be done prior to establishing a business relationship with a client, on a periodic basis post establishment of the business relationship and where PIP becomes aware of any changes to the risk factors associated with the client that might contribute to the money laundering risk to increase materially.

To undertake a risk-based assessment of every client and to assign the client a risk rating, PIP is required to complete CDD prior to establishing a new client relationship and prior to a transaction being executed.

3.1. Requirements for Risk Based Assessment of Clients

To complete the risk-based assessment for each client, PIP must obtain, verify, and record certain client information.

In situations where the ownership or control arrangements of the client prevent PIP from identifying one or more of the client's beneficial owners, PIP will not establish a business relationship with that client unless regulatory exemptions are available.

The MLRO must be notified immediately (via email) where there are doubts to the accuracy and authenticity of documents provided by a client, where there is suspicion of money laundering or a change in circumstances of the client warrants a change in the risk-rating of that client, the MLRO must be notified as well.

A copy of the Client Risk Assessment Form and the Guide to completing the form are in the Annexes to this Manual.

4. Client Due Diligence Process

As mentioned in Part 1 of this Manual, CDD must be conducted prior to the establishment of a business relationship with a prospective client, the conduct of an occasional transaction equal to or more than USD$15,000, or where there are suspicions on the client or transaction being either involved in money laundering activities or for the purposes of money laundering. PIP perform CDD to identify the clients it is dealing with and verify their identity through legitimate documents and review them against the UN and other international sanctions lists.

CDD is conducted in the following manner, based on the risk ratings assigned to the client following the results of the risk assessment conducted:

- Standard ('Simplified') Due Diligence – for clients assigned with a low or medium risk rating.
- Enhanced Due Diligence – for clients assigned with a high-risk rating.

The process steps for the conduct of each type of due diligence is explained further below:

4.1. Standard Client Due Diligence Process

Standard CDD typically involves the following:

- Identifying and verifying the identity of the client, ownership and control structure;
- assessing and understanding the purpose and intended nature of the business;
- determine the level of activity;
- screening for any adverse information;
- conducting on going due diligence on the client/customer post onboarding
- understanding the source of funds and source of wealth.

The process below describes the steps required to complete the CDD process.

Step 1: Client reviews, completes and signs the Client Agreement.

Step 2: Client provides identification information set out in the Client Agreement and KYC form. The documents required must have information evidencing (but not limited to) the following:

For Natural Persons:

a. full name (including any alias).
b. date of birth.
c. nationality.
d. legal domicile; and
e. current residential address (other than a post office box);

For Corporates, Foundations, Trusts and other similar Legal Arrangements:

a. the full name of the Body Corporate and any trading name.
b. the address of its registered office and, if different, its principal place of business.
d. the date and place of incorporation or registration.

e. relevant corporate documents of the customer; and

f. the full names of the members of its governing body and persons in senior management positions.

g. For foundations, additional documentation will include: (i) a certified copy of its charter and by-laws of the foundation or any other documents constituting the foundation; and (ii) documentary evidence of the appointment of the guardian or any other person who may exercise powers in respect of the foundation.

h. For a trust or other similar Legal Arrangements, additional documentation will include: (i) a certified copy of the trust deed or other documents that set out the nature, purpose and terms of the trust or arrangement and (ii) documentary evidence of the appointment of the trustee or any other person exercising powers under the trust or arrangement.

Step 3: Verification

Ideally all documentation and information required in Step 2 should be obtained via a firsthand inspection of an original current, valid passport or, where a customer does not own a passport, an official identification document with a photograph. Where copies of the documentation are provided, such copies must be signed, dated and marked with 'original sighted'.

Where such documentation cannot be sighted nor obtained in its original form, they must be certified as a true copy of the original documents by ONE of the following:

a. a registered lawyer.

b. a registered notary.

c. a chartered accountant.

d. a government ministry.

e. a post office.

f. a police officer; or

g. an embassy or consulate

Their contact details must also be provided.

Step 3: If the information is not sufficient, MLRO will contact the client to request for further information/documents.

Step 3a: In cases where the client is unable to provide some of the requested documents, leading to incomplete CDD, PIP must either:

- not provide any services to the client.
- terminate or suspend any existing business relationship with the client.
- return any monies or assets received from the client/customer.

However, where such above actions may result in 'tipping off' or directives have been provided by the CBUAE FIU, PIP will seek advice on the course of action from the FSRA or an appropriate UAE government authority.

Step 3(b) Where PIP is unable to complete the verification of the identity of its client and beneficial owners before carrying out a transaction or an occasional transaction on its behalf, it may onboard the client or conduct and complete the CDD (including verification) within 30 days of effecting any transaction, provided that it has reasonable grounds to believe that non-fulfilment of the verification process:

a. bears little risk of money laundering,

b. that risk is effectively managed; and

c. doing so would interrupt or delay the normal course of business in respect of effecting the transaction.

Step 3(c) Where the Step 3(b) has been adopted, the MLRO will consider the issuance of a waiver and document the reasons and considerations a waiver can be granted.

Step 3(c)(i): In cases where the MLRO is unwilling to provide a waiver, the client will be informed that PIP is unable to proceed further without satisfying the CDD requirements.

Step 3(c)(ii): The MLRO may consider whether the inability or unwillingness of the client to provide any requisite information warrants filing an SAR.

Step 3(d): If the decision is made to file the SAR, the MLRO follows the SAR filing process.

Step 4: MLRO conducts a review on the client, directors and beneficial owners using a range of international databases.

Step 5: MLRO completes the Client Risk Assessment

Step 5(a): In the case of High-Risk clients, the MLRO forwards the Client Risk Assessment form and all supporting documents to the Board for review/comment and approval. In cases where the Client Risk Assessment identifies a client as High-Risk, but the MLRO is of the view that when all circumstances are considered, the client should not be rated as High-Risk, the MLRO will prepare a memo outlining the reasons for the decision to adjust the risk rating.

Step 6: All CDD documents are then recorded, saved and retained electronically as per the record keeping guidelines of PIP.

A copy of the KYC Identification Requirements Form can be found within the annexes to this Manual.

4.1.1. Beneficial Owners

Beneficial Owners are natural persons who meet any of the criteria below:

- own or control (whether directly or indirectly) more than 25% of the client's shares or voting rights;
- has the right to appoint or remove a majority of the board of directors of a Body Corporate; or
- has the right to exercise significant influence or control over the client.

A. Identification of Beneficial Owners

I. Trusts

Where the client is a Trust or a similar legal arrangement, PIP will need to identify: (a) the settlor of the Trust; (b) any other Trustee(s) aside from the client; (c) each beneficiary of the Trust; (d) where the persons (or some of the persons) benefiting from the Trust have not been determined, the class of persons whose main interest, in the opinion of PIP, the Trust has been established or operates; and (e) any natural person who has control over the Trust.

II. Foundations

Where the client is a Foundation or a legal arrangement similar to a Foundation, PIP will need to identify the: (a) the person who set up the Foundation; (b) the Foundation's council members (or otherwise members of the governing body of the Foundation); (c) the guardian, if any; (d) the beneficiaries (if named) or designee (if no beneficiaries are named) in whose main interest, in the opinion of PIP, the Foundation has been established or operates; and (e) any natural person who has control over the Foundation. 'Control' here means a person who holds, directly or indirectly, 25% or more of the voting rights in the management of the Foundation or the legal arrangement with the power to appoint or remove a majority of the officials of the Foundation.

4.2. Enhanced Client Due Diligence ("EDD")

EDD is undertaken for all clients identified as High-Risk based on the customer risk assessment (CRA) conducted as part of PIP's onboarding process prior to the establishment of the business relationship between the prospective client and where PIP, based on the information/documentation requested and the results of the CRA, has reason to believe that a client present high risk factors to money laundering.

- "High Risk factors" may include:
  - any client who is a Senior Foreign Political Figure (as defined in Part Four), a member of a Senior Foreign Political Figure's Immediate Family, or a Close Associate of a Senior Foreign Political Figure.
  - any client residing in or organized or chartered under the laws of a Non-Cooperative Jurisdiction.
  - any client who gives PIP reason to believe that its funds originate from, or are routed through, an account maintained at an Offshore Bank, or a bank organized or chartered under the laws of a Non-Cooperative Jurisdiction; and
  - any client who gives PIP reason to believe that the source of its funds may not be legitimate.
  - any client who has been identified as being 'high risk' for proliferation financing.

- transactions found to involve any proliferation-sensitive goods or services, regardless of whether the customer is itself in a high-risk category.
- Any client who has been identified on the FATF's list of jurisdictions subject to a Call for Action (the Blacklist) and depending on the risk that the client poses, the list of Jurisdictions under Increased Monitoring (the Grey List).

The extent of EDD required is determined on a case-by-case basis, depending on the risks posed by the client and the business relationship it intends to establish with PIP. However, it is likely to include the below information and requirements in addition to the ones listed in the Standard Due Diligence process:

- obtain and verify additional identification information on the client and all beneficial owners.
- obtain and verify information on the intended nature of the business relationship; and
- obtain and verify information on the reasons for a transaction.
- identify the expected end users of any strategic goods or Dual-Use goods and the customer's expected exposure to high-risk jurisdictions, including trans-shipment hubs.
- conduct more regular reviews and updating of the CDD information that PIP holds.
- identification and verification of the client's source of funds and source of wealth.
- increased monitoring of the business activities to determine whether there are any unusual or suspicious transactions.

The CDD information and transactions of all High-Risk clients are reviewed at least annually to ensure that PIP retain valid and up-to-date information of the client and assess the client's transaction patterns against the declared or expected behaviour. Where required, PIP will also update information with regards to a client's source of funds and wealth and increase the degree of monitoring of the business activities.

I. Politically Exposed Persons

Politically exposed persons ("PEPs"), refers to those individuals who have, or have had a high political profile, or hold, or have held public office. Members of their family and close associates can pose a higher money laundering risk as their position may make them vulnerable to corruption. Hence, this risk also extends to members of their families and to close associates. Consequently, PIP conducts EDD where PEPs are directors or beneficial owners of a client.

NOTE: The fact that an individual is a PEP does not automatically mean that the individual must be assessed to be a high-risk customer. However, ECDD still needs to be undertaken on those identified as PEPs.

4.2.1. Enhanced Due Diligence Process

The process for conducting EDD is as follows:

Step 1: After initial due diligence has been conducted and the client has been identified as a high risk client due to these checks, PIP, in addition to the standard information/documents request, will request for the following:

- Documentation evidencing source of wealth and funds of the client and its beneficial owners.
- Further documentation on the client and its beneficial owners
- Further details (with supporting documents) on the nature of business and its rationale and intention of establishing a relationship with PIP.

NOTE: This list is not exhaustive, and further information may be requested for.

Step 2: Once the client provides the above, all information and documentation including the client's risk profile via the CRA will be presented to the Board for review and determination if a business relationship is to be established with the client.

Step 2(a) Where the Board approves the establishment of the business relationship (i.e., to on board the client), confirmation of this approval is evidenced by the signature of the SEO. Where the Board does not approve for the establishment of the business relationship, the EDD process will not continue, and the client will be notified of this.

Step 3: In cases where the client is unable to provide and verify some of the requested documents, leading to the incompletion of the EDD, it must follow the steps highlighted under point 3(a) of the Standard Due Diligence process.

Step 4: The MLRO will also consider whether the inability or unwillingness of the client to provide information warrants filing an SAR.

Step 5: If the decision is made to file the SAR, the MLRO follows the SAR filing process.

NOTE: In cases where the CRA identifies a client as High-Risk, but the MLRO is of the view that when all circumstances are considered, the client should not be rated as High-Risk, the MLRO will prepare and present to the Board, a memo outlining the reasons for the decision to adjust the risk rating.

Step 6: All CDD documents are retained electronically.

All questions or concerns regarding a High-Risk Client should be directed to the MLRO.

4.2.2. Natural Persons

In addition to the EDD procedures mentioned above, EDD for natural persons identified by PIP as High-Risk may include:

- reviewing pronouncements of U.S. governmental agencies and multilateral organizations such as the FATF about the adequacy of anti-money laundering and counter-terrorism legislation in the client's home jurisdiction.
- assessing the client's personal and business reputation through review of generally available media reports or by other investigating means.
- assess the source of the client's wealth, including the economic activities that generated the client's wealth, and the source of the particular funds intended to be used to make the investment; and
- obtaining a letter of reference or certificate from a regulated financial institution that has performed meaningful due diligence procedures on such a client.

4.2.3. Legal Entities

The EDD procedures for legal entities identified by PIP as High-Risk Clients may include:

- same procedures as set forth for natural persons above.
- reviewing recent changes in the ownership or senior management of the client.
- if applicable, determining the relationship between the client, its directors, and material beneficial owners and the government of its home jurisdiction, including whether the client is a government-owned entity.
- reviewing the economic activities that generated the client's wealth, and the source of the funds intended to be used to make the investment; and
- obtaining a letter of reference or certificate from a regulated financial institution that has performed meaningful due diligence procedures on such clients.
-

The EDD template form can be found within the Annexes to this Manual.

5. Ongoing Client Due Diligence

All client information must be reviewed and updated in accordance with the following table. Any information that requires review/change in client's risk rating must be documented in the CDD form and should be escalated to the MLRO for sign-off.

Category	Review Frequency
Low Risk Clients	Within 36 months from the time the relationship commenced
Medium Risk Clients	Within 24 months from the time the relationship commenced
High Risk Clients	Within 12 months from the time the relationship commenced

The MLRO will also review the CDD documentation on file if there is a material change in the client's circumstances, the business relationship or where the client requests a transaction that is observed to be different from the existing pattern.

5.1. The Ongoing Review Process

PIP conducts on-going monitoring and review of its existing clients.

'On-going monitoring' here includes daily screening checks on its clients via Firm's AML screening tool against the current local and international sanctions lists including new updates to such lists.

The review includes the review/evaluation of all documentation and information provided during the onboarding stage (including AML, CFT, TFS screening). A formal reassessment of the risk rating (similar to the risk assessment conducted at the onboarding stage) will also be conducted via the Client Risk Assessment form. The reassessment will also involve identification, assessment, monitoring, management and mitigation of terrorist and proliferation financing risks, particularly sanctions-related risks.

For each ongoing review, the MLRO will prepare a new Client Risk Assessment form. If new supporting documents are required or existing supporting documents were amended, the MLRO will record the details and retain the documents on the file.

PIP must also ensure that its register of outsourced service providers is updated on at an annual basis, with all information on the agents PIP is currently engaged with to be current and accurate for presentation to the Regulator upon request.

5.2. Screening

PIP undertakes regular and ongoing screening on all its existing clients against the current Local Terrorist List(s) and UN Consolidated List(s) including any updates to such Lists and: (i) prior to the execution of any transaction (ii) prior to onboarding new client (iii) during ongoing CDD reviews or (iv) changes to a client's information.

PIP ensures that the screening measures applied are commensurate with the risks identified i.e. where there are higher risks, PIP will commensurately measure to manage and mitigate the risks, including applying enhanced screening measures. Correspondingly, where the risks are lower, they should ensure that the screening measures are commensurate with the lower level of risk.

The following are included in the screening process:

a. Existing client databases - All systems containing customer data and transactions need to be mapped to the screening system to ensure full compliance.
b. Potential clients before conducting any transactions or entering a business relationship.
c. Names of parties to any transactions.
d. Ultimate beneficial owners, both natural and legal.
e. Names of individuals, entities, or groups with direct or indirect relationships with the client.
f. Directors and/or agents acting on behalf of client (including individuals with power of attorney).

6. Suspicious Activity Reports

All suspicions of money laundering must be notified to the MLRO as soon as practical. A notification can be made verbally, via an email or in a formal memorandum.

The following are some of the circumstances that might give rise to reasonable grounds for suspicion:

- transactions which have no apparent purpose, which make no obvious economic sense, or which are designed or structured to avoid detection.
- transactions requested by a client without reasonable explanation, which are out of the ordinary range of services normally requested or are outside PIP's experience in relation to that client.
- where the size or pattern of transactions is out of line with any pattern that has previously emerged or are deliberately structured to avoid detection.
- where a client has refused to provide the requested information without reasonable explanation.
- where a client who has just entered a business relationship with PIP uses the relationship for a single transaction or for only a very short period.

- an extensive use of offshore accounts, companies or structures in circumstances where the client's economic needs do not support such requirements; and
- unnecessary routing of funds through third party accounts.

The MLRO must be notified of all suspicious situations, including situations when a business relationship has not been established.

A copy of the Internal SAR Form is in within the annexes to this Manual.

6.1. SAR Filing Process

Upon identification or notification of a suspicion, the MLRO (or in his absence, the deputy MLRO) starts the investigation as soon as practical upon receiving such notification. The investigation may include reviewing the CDD forms, interviewing the relevant employees and reviewing client transaction history or any other information the MLRO considers appropriate. Once the investigation is complete and where the MLRO decides to file an SAR with the UAE Central Bank Financial Intelligence Unit (FIU), the MLRO will complete the relevant automated report forms on the GoAML portal, including both or either of the following:

- Funds Freeze Report (FFR): To be used to report any freezing measure, prohibition to provide funds or services, and any attempted transactions related to confirmed matches.
- Partial Name Match Report (PNMR): To be used to report any 'potential match'.

Additionally, the correct and most applicable Reasons for Reporting (RFR) code(s) must also be selected when filing and submitting the above-mentioned forms within the portal.

All supporting documents used in the investigation must be attached to the report(s) and will be part of the filing and submissions unto the GoAML portal.

6.2. Proliferation Financing Reporting

PIP will file (via goAML) a suspicious transaction report (STR) and/or suspicious activity report to the UAE Financial Intelligence Unit (FIU) when it has reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute (in whole or in part, regardless of the amount) the proceeds of crime. The below instances are also red flags considered by PIP as suspicious transactions/activities which are reportable to the UAE Financial Intelligence Unit (FIU):

- Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.
- The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector.
- Dealings with sanctioned goods or Dual-Use goods.
- Identifying documents (e.g. bill of lading, sales purchase agreement, etc.) that seemed to be forged or counterfeited.
- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
- The activity developed or financed does not relate to the original or intended purpose of the company or entity. For example:
    - For companies, they are importing high-end technology devices which is not in accordance with their trade license.
    - For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide humanitarian aid.
- Complex commercial or business deals that seem to be aiming to hide the final destination of the transaction or the goods.
- Complex legal entities or arrangements that seem to be aiming to hide the beneficial owner.

6.3. Targeted Financial Sanctions (TFS) Reporting Process

Whilst conducting initial and ongoing due diligence of our customers, the following hits may be identified:

Partial Name Match	A partial name match is when there is a partial match between identifiers in the Sanctions Lists with any information in the databases, and PIP is unable to conclude a false positive or a confirmed match. Where this occurs, all transactions are suspended, and the match is reported to the Executive Office for Control & Non-Proliferation (EOCN) and the relevant Supervisory Authority.
Confirmed Match	A confirmed match is when an individual, entity, or group matches all key identifiers published on the Sanctions Lists. PIP will apply freezing measures in accordance with the AML Manual and report to the Executive Office for Control & Non-Proliferation (EOCN) and the relevant Supervisory Authority.
False Positive Result	A false positive is a partial name match to listed individuals, entities, or groups, either due to the common nature of the name or due to ambiguous identification data, which on further examination proves not to be a confirmed match.
Negative Result	A negative result is when no match is identified upon conducting screening.

Where PIP identifies any of the above 'hits' on the entity, the individuals and/or groups associated with the entity against PIP's sanction screening list, the following actions are taken:

A. Confirmed Match

1. Implement all necessary freezing measures without delay. This involves the immediate freezing of funds and refrain from offering any funds or other assets or services.

NOTE: The freezing measures shall include:

- interest, profits, or other earnings due on the account;
- payments due under contracts, agreements or obligations agreed upon prior to the date on which the account has become subject to freezing.

2. Report the freezing measure, prohibition to provide funds or services, and any attempted transactions to the Executive Office – IEC and the CBUAE via the GoAML platform using via the Fund Freeze Report (FFR) within 2 business days. Where the confirmed match is a potential customer, you must reject the transaction immediately and report the case.
3. Ensure all the necessary, supporting information and documents regarding the 'confirmed match' are uploaded along with the FFR;
4. Notify and share a copy of the report with the FSRA (ADGM) and the Financial Crime Prevention Unit via the email address, fcpu@adgm.com.

NOTE - The freezing measures applied related to the 'confirmed match' are not to be removed until further instructions are received from the Executive Office – IEC.

B. Partial Match

When a 'partial match' to a listing of names of individuals, groups, or entities is identified, the following actions must be taken:

1. Suspend without delay any transaction and refrain from offering any funds or services;
2. Report the 'potential match' to the Executive Office – IEC and the CBUAE via the GoAML platform by selecting the Partial Name Match Report (PNMR) within 2 business days;
3. Ensure all the necessary, supporting information and documents regarding the name match is uploaded;
4. Notify and share a copy of the report with the FSRA (ADGM) and the Financial Crime Prevention Unit via the email address, fcpu@adgm.com.

NOTE - The freezing measures applied related to the partial name match are not to be removed until further instructions are received from Executive Office – IEC via the GoAML platform on whether to cancel the suspension measures or to implement freezing measures.

Failure to raise a TFS report when required constitutes a contravention of the administered rules, regulations, and legislations applicable to PIP, and as a result, PIP may be subject to actions taken by the FSRA as it deems appropriate.

C. False Positive Result

No regulatory action is required, however when identifying the partial name match, the following factors must be taken into consideration:

- the information and knowledge PIP has of the customer, potential customer, beneficial owner, or transaction via customer due diligence and/or
- using reasonable information (e.g., open-source information, media articles, commercial databases, etc.), an analysis (i.e. cross-check) to conduct checks against the client's data with the identifiers published on the Sanctions Lists.

Where PIP is satisfied that the individual, entity, or group is not the designated individual, entity, or group, i.e. a 'False Positive Result', no TFS measures will be implemented, and the transaction or business relationship can continue. Evidence of the process undertaken are to be recorded and maintained in accordance with PIP's record keeping requirements.

D. Negative Result

No regulatory action is required.

6.4. High Risk Country Transaction & Activity Reports

Where a Firm identifies transactions originating from, routed through or destined to high-risk jurisdictions and/or any financial or non-financial engagements involving an individual or entity hailing from a country classified as a 'High-Risk Jurisdiction subject to a Call for Action (i.e. the Blacklist)', such transactions must be reported to the FIU via the High-Risk Country Transaction Report.

If, because of the nature of the suspicious transactions, there are insufficient information to complete the mandatory sections within the Report, the High-Risk Country Activity Report must be completed, ensuring that the attributes of the transactions such as amount, account numbers, etc., are included within the Report.

Whilst filing either of the reports, the reporting entity must select a dedicated RFR (Reason for Reporting). PIP must wait for 3 days post submission, before executing any such transaction(s) unless any advice or objection has been received from the FIU on the reported transaction(s). In the absence of any response from the UAE FIU within the stipulated timeframe, PIP may choose to proceed or not proceed with such transaction(s) at its own discretion.

Reporting is done via the FIU's "GoAML" system. The MLRO is the registered user for the system.

Important Note:

A transaction that appears unusual is not necessarily suspicious. Even clients with a stable and predictable transaction profile will have periodic transactions that are unusual. Many clients will, for perfectly legitimate reasons, have an erratic pattern of transactions or account activity. Therefore, the unusual nature of a transaction or request should only be a basis for further inquiry, which may in turn require judgment as to whether it is suspicious or not. A transaction or activity may not be suspicious at the time it is detected. However, if it becomes suspicious later, it must be reported to the MLRO.

A copy of the Internal SARS Form can be found within the annexes to this Manual.

Subscription to the CBUAE's Executive Office.

The MLRO is registered with the CBUAE's Executive Office website to receive notifications related to new listing, re-listing, updates, or de-listing decisions and/or updates to the Sanctions lists issued by the UN Security Council, the Sanctions Committee or the Cabinet.

Premier Invest

3

PART THREE

FORMS AND TEMPLATES

FORMS AND TEMPLATES

Premier Invest

4

PART FOUR

DEFINITIONS

DEFINITIONS

The “Board” means the Board of Directors of PIP.

A “Close Associate” of a Senior Foreign Political Figure is a person who is widely and publicly known internationally to maintain an unusually close relationship with the Senior Foreign Political Figure and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the Senior Foreign Political Figure.

“Executive Office for Control & Non-Proliferation (“The Executive Office”)” is the communications channel for The Committee for Goods and Materials Subject to Import and Export Control (CGMSIEC) UAE, with other countries and international bodies concerned with control on exports. It is also responsible for circulating resolutions issued by the Committee, following up with competent authorities and bodies in this regard, in addition to ensuring the implementation of the decisions of UN Security Council and other concerned regional and international organizations and authorities.

The “Committee for Goods and Materials Subject to Import and Export Control (CGMSIEC)” is the governmental body responsible for all matters relating to money laundering, counter terrorist financing and targeted financial sanctions. It is responsible for implementing relevant policies and regulations and engaging in partnerships on both national and international levels and contributes actively to leveraging control on exports and preventing proliferation of weapons of mass destruction and related technologies. Their website is https://www.uaeiec.gov.ae/en-us/about-us.

“FATF” means the Financial Action Task Force, an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering. FATF is a “policy-making body” which works to generate the necessary political will to bring about national legislative and regulatory reforms to combat money laundering. FATF’s website is https://www.fatf-gafi.org/

“A FATF-Compliant Jurisdiction” is a jurisdiction that (i) is a member in good standing of FATF; and (ii) has undergone two rounds of FATF mutual evaluations.

“Foreign Bank” means an organization that (i) is organized under the laws of a foreign country; (ii) engages in the business of banking; (iii) is recognized as a bank by the bank supervisory or monetary authority of the country of its organization or principal banking operations; (iv) receives deposits to a substantial extent in the regular course of its business; and (v) has the power to accept demand deposits, but does not include the U.S. branches or agencies of a foreign bank.

“Foreign Shell Bank” means a Foreign Bank without a Physical Presence in any country but does not include a Regulated Affiliate.

The “Immediate Family” of a Senior Foreign Political Figure typically includes the political figure’s parents, siblings, spouse, children and in-laws.

“Non-Cooperative Jurisdiction” means any foreign country or territory that has been designated as noncooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization, such as FATF, of which the United States is a member and with which designation the United States representative to the group or organization continues to concur. Please see link https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html for FATF’s list of high risk and other monitored jurisdictions.

“OFAC” means the U.S. Office of Foreign Asset Control. The complete OFAC lists, including OFAC’s List of Specially Designated Nationals and Blocked Persons, may be accessed at https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

“Offshore Bank” means a Foreign Bank that is barred, pursuant to its banking license, from conducting banking activities with the citizens of, or with the local currency of, the country that issued the license, other than a Regulated Affiliate.

“Physical Presence” means a place of business that is maintained by a Foreign Bank and is located at a fixed address, other than solely a post office box or an electronic address, in a country in which the Foreign Bank is authorized to conduct banking activities, at which location the Foreign Bank: (1) employs one or more individuals on a full-time basis; (2) maintains operating records related to its banking activities; and (3) is subject to inspection by the banking authority that licensed the Foreign Bank to conduct banking activities.

A “Prohibited Investor” includes a Listed Investor, a Foreign Shell Bank and other Investors prohibited by law or regulation, as well as those prohibited by the Company in its sole discretion.

“Regulated Affiliate” means a Foreign Shell Bank that: (1) is an affiliate of a depository institution, credit union, or Foreign Bank that maintains a Physical Presence in the United States or a foreign country, as applicable; and (2) is subject to supervision by a banking authority in the country regulating such affiliated depository institution, credit union, or Foreign Bank.

“Senior Foreign Political Figure” means a senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned corporation. In addition, a Senior Foreign Political Figure includes any corporation, business or other entity that has been formed by, or for the benefit of, a Senior Foreign Political Figure.

“SEO” means the senior executive officer of PIP nominated by the Board.

Version Control History

Version	Date	Author	Details
1.0	January 2025	J. Awan & Partners	Creation of Manual

Notes