Practical Guidance
to AIFC Anti-Money Laundering and Counter – Terrorist Financing Framework

Approval Date: 17 November 2023 (as amended on 19 December 2024)
Commencement date: 21 November 2023 (1 January 2025)

Astana, Kazakhstan

Table of Contents

Revision history

Version	Date	Change description	Section changed
AMLPG 001	15/04/2022	n/a	n/a
AMLPG 002	17/11/2023	Amendments on AML audit.	Annex 7
AMLPG 003	19/12/2024	Amendments consequential to amendments to the AML Rules	Part 3 Part 4 Part 5 Part 6 Part 8 Part 9 Annex 1 Annex 2 Annex 7

Version	Date	Part 1	
AMLPG 001	15/04/2022	**Introduction**	s. 1.1 – 1.6

Subject	1	INTRODUCTION
AML Rule 2.1	1.1	This Practical Guidance to AIFC Anti-Money Laundering and Counter – Terrorist Financing Framework (the "Guidance") assists Relevant Persons in adjusting their understanding and perception of the AIFC AML/CFT framework and is intended for use by Relevant Persons and their officers and staff in respect of all AFSA regulated or supervised activities except the Authorised Firms licenced to operate a Representative Office. This Guidance also: (a) provides general background on the subjects of money laundering and terrorist financing (ML/TF), including a summary of the main provisions of the applicable AML/CFT regulations in the AIFC; and (b) assists Relevant Persons and their senior management in designing and implementing their own policies, procedures, and controls in the relevant operational areas, considering their special circumstances to meet the relevant AML/CFT statutory and regulatory requirements.
	1.2	The terms and abbreviations in this Guidance shall be interpreted by reference to the definitions set out in the AIFC Glossary.
	1.3	The relevance and usefulness of this Guidance will be kept under review, and it may be necessary to issue amendments from time to time.
	1.4	For the avoidance of doubt, the use of the word "must" or "should" in relation to an action, consideration or measure referred to in this Guidance indicates that it is a mandatory requirement. Given the significant differences that exist in the organisational and legal structures of different Relevant Persons and the nature and scope of the business activities conducted by them, there is no single set of universally applicable implementation measures. Accordingly, the content of this Guidance is not intended to be an exhaustive list of the means of meeting the statutory and regulatory requirements.

		Relevant Persons, therefore, should use this Guidance as a basis to develop measures appropriate to their structure and business activities.
	1.5	A failure by any Person to comply with any provision of this Guidance does not by itself render the person liable to any judicial or other proceedings but, in any proceedings under the AML Rules or applicable AIFC regulations and Kazakhstan laws before any court, this Guidance is admissible in evidence. If any provision set out in this Guidance appears to the court to be relevant to any question arising in the proceedings, the provision must be taken into account in determining that question.
	1.6	In addition, non-adherence to this Guidance, by Relevant Persons, could lead to adverse findings where any AML Rules/Regulations have been consequentially breached.

Version	Date	Part 2	
AMLPG 001	15/04/2022	**What Is Money Laundering**	s. 2.1 – 2.10
		▪ *Regulation and Rules related to money laundering (ML), terrorist financing (TF), financing of proliferation of weapons of mass destruction (PF) and financial sanctions*	s. 2.7 – 2.10

Subject	2	WHAT IS MONEY LAUNDERING
	2.1	Money laundering involves taking criminal proceeds and disguising their illegal sources in order to use the funds to perform legal or illegal activities. Simply put, money laundering is the process of making dirty money look clean. When a criminal activity generates substantial profits, the individual or group involved must find a way to use the funds without drawing attention to the underlying activity or persons involved in generating such profits. Criminals achieve this goal by disguising the source of funds, changing the form or moving the money to a place where it is less likely to attract attention. Criminal activities that lead to money laundering (i.e., predicate crimes) may include illegal arms sales, narcotics trafficking, contraband smuggling and other activities related to organized crime, embezzlement, insider trading, bribery and computer fraud schemes. The definition of money laundering varies in each country where it is recognised as a crime.
	2.2	From the very start in the fight against money laundering at the international level, the United Nations has taken an active role to promote the harmonisation of countermeasures and the strengthening of international cooperation. The United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, adopted in December 1988 in Vienna, was the first international instrument to address the issue of proceeds of crime, and to require States to establish money laundering as a criminal offence. The United Nations 2000 Convention Against Transnational Organised Crime, also known as the Palermo Convention, defines money laundering as: ▪ the conversion or transfer of property, knowing it is derived from a criminal offence, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his or her actions;

		▪ the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to or ownership of property knowing that it is derived from a criminal offence; and ▪ the acquisition, possession or use of property, knowing at the time of its receipt that it was derived from a criminal offence or from participation in a crime.
	2.3	An important prerequisite in the definition of money laundering is knowledge. FATF's 40 Recommendations on Money Laundering and Terrorist Financing and the Fourth European Union Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing (2015) state that "the intent and knowledge required to prove the offence of money laundering includes the concept that such a mental state may be inferred from objective factual circumstances." A number of jurisdictions also use the legal principle of willful blindness in money laundering cases to prove knowledge. Courts define willful blindness as the "deliberate avoidance of knowledge of the facts" or "purposeful indifference" and have held that willful blindness is the equivalent of actual knowledge of the illegal source of funds or of the intentions of a customer in a money laundering transaction.
AML Law (National)	2.4	Per Subparagraph 19) Article 3 of the Law of the Republic of Kazakhstan No 191-IV dated 28 August 2009 on counteracting legalisation (laundering) of proceeds obtained through criminal means and financing of terrorism (the "AML Law"), all Relevant Persons are subjects of the financial monitoring (obliged entities) and, therefore, should have regard to the AML Law in relation to their activities in/from the AIFC.
AML Law (National)	2.5	As per Subparagraph 11) Article 1 of the AML Law, legalization (laundering) of income obtained by criminal proceeds means involvement in legitimate turnover of money and (or) other assets obtained by criminal proceeds, through transactions in the form of conversion or transfer of property representing the proceeds of criminal offences, or the possession and use of such property, concealing or disguising its true nature, source, location, disposition, movement or ownership of property or its accessories, if it is known that such property is the proceed of criminal offences and/or the result of mediation in money or another asset laundering that are obtained by criminal means.
	2.6	There are three common stages in money laundering, and they frequently involve numerous transactions. Therefore, a Relevant Person should be alert to any such sign for potential criminal activities. These stages are:

		(a) Placement - the physical disposal of cash proceeds derived from illegal activities and placing it into a financial system; (b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and (c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system, and the proceeds appear to be the result of or connected to legitimate business activities.
		Regulation and Rules related to money laundering (ML), terrorist financing (TF), financing of proliferation of weapons of mass destruction (PF) and financial sanctions
	2.7	The FATF is an inter-governmental body established in 1989. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating of ML, TF, PF, and other related threats to the integrity of the international financial system. The FATF has developed a series of Recommendations that are recognised as the international standards for combating of ML, TF and PF. They form the basis for a coordinated response to these threats to the financial system's integrity and help ensure a level playing field. In order to ensure full and effective implementation of its standards at the global level, the FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow-up after the evaluations, including identifying high risk and other monitored jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large. Many major economies have joined the FATF, which has developed into a global network for international cooperation that facilitates exchanges between member jurisdictions.
	2.8	The Eurasian Group on Combating Money Laundering and financing of terrorism (the “EAG”) is a FATF-style regional body. The EAG was established in 2004 and is currently an associate member of the FATF. The EAG was created for the countries of the Eurasian region not included in the existing FATF-style regional groups and is intended to play an important role in reducing the threat of international terrorism and ensure the transparency, reliability and security of the financial systems of states and their further integration into the international infrastructure for combating money laundering and terrorism financing (AML/CFT). The creation of the group coincided with the launch of efforts to create conditions for the formation and development of effective anti-money-laundering systems in the region.

		Today the EAG brings together nine countries in the region (Belarus, China, India, Kazakhstan, Kyrgyz Republic, Russia, Tajikistan, Turkmenistan, Uzbekistan). In addition, observer status has been granted to 15 countries and 23 international organizations. The primary goal of the EAG is to ensure effective interaction and cooperation at the regional level and integration of EAG member-states into the international system of anti-money laundering and combating the financing of terrorism in accordance with the Recommendations of the FATF and the anti-money laundering and combating the financing of terrorism standards of other international organizations, to which EAG member-states are party. The main tasks of the EAG: ▪ assisting member-states in implementing the 40 FATF Recommendations; ▪ developing and conducting joint activities aimed at combating money laundering and terrorist financing; ▪ implementing a program of mutual evaluations of member-states based on the FATF 40 Recommendations, including assessment of the effectiveness of legislative and other measures adopted in the sphere of AML/CFT efforts; ▪ coordinating international cooperation and technical assistance programs with specialized international organizations, bodies, and interested states; ▪ analysing money laundering and terrorist financing trends (typologies) and exchanging best practices of combating such crimes taking into account regional specifics.
	2.9	As a member of the EAG, the Republic of Kazakhstan is obliged to implement the AML/CFT requirements as issued by the FATF, which include the latest FATF Recommendations, and it is important that the AIFC complies with the international AML/CFT standards in order to maintain its status as an international financial centre.
	2.10	The main pieces of legislation in the AIFC that are concerned with ML, TF, PF and financial sanctions are: (a) the AML Law; (b) AIFC Anti-Money Laundering, Counter – Terrorist Financing and Sanctions Rules; (c) Guidance (Requirements) applicable to the Rules of Internal Control for the purposes of counteracting the legalisation (laundering) of proceeds from crime and the financing of terrorism for financial monitoring entities of the Astana International Financial Centre (the Relevant Persons) (hereafter referred to as “AML Internal Controls Guidance”);

		(d) Guidance (Requirements) for the purposes of counteracting the legalisation (laundering) of proceeds from crime and the financing of terrorism, applicable to the Customer Due Diligence in cases when the Astana International Financial Centre Participants (the Relevant Persons) establish non-face to face business relations with customers (hereafter referred to as "CDD for non-face-to-face business relations"); (e) other related AIFC Regulations and Rules; (f) other regulations issued by the Financial Monitoring Agency of the Republic of Kazakhstan (the "FIU"). It is very important that Relevant Persons and their senior managers and staff fully understand their respective responsibilities under the above legislation.

Version	Date	Part 3	
AMLPG 003	19/12/2024	**Risk-Based Approach**	s. 3.1 – 3.21
		▪ *Business risk assessment*	s. 3.4 – 3.7
		▪ *Considering relevant risk factors*	s. 3.8 – 3.10
		▪ *Keeping risk assessment up-to-date*	s. 3.11
		▪ *Documenting risk assessment*	s. 3.12
		▪ *Obtaining senior management approval*	s. 3.13
		▪ *Group-wide ML/TF risk assessment*	s. 3.14 – 3.15
		▪ *Customer risk assessment*	s. 3.16 – 3.18
		▪ *Conducting customer risk assessment*	s. 3.19 – 3.21

Subject	3	RISK-BASED APPROACH
Chapter 4 of the AML Rules	3.1	Applying an AML/CFT risk-based approach (RBA) is recognised as an effective way to combat ML/TF. The RBA to AML/CFT means that countries, competent authorities and financial institutions should identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures that are commensurate with those risks in order to mitigate them effectively. Furthermore, the use of an RBA allows a Relevant Person to allocate its resources in the most efficient way in accordance with priorities so that the greatest risks receive the highest attention.
	3.2	Therefore, Relevant Persons should have in place a process to identify, assess and understand the ML/TF risks to which they are exposed (hereafter referred to as “business risk assessment”) so as to facilitate the design and implementation of adequate and appropriate internal AML/CFT policies, procedures, programmes and controls (hereafter collectively referred

		to as "AML/CFT Systems") that are commensurate with the ML/TF risks identified in order to properly manage and mitigate them.
	3.3	Relevant Persons should also assess the ML/TF risks associated with a customer or proposed business relationship (hereafter referred to as "customer risk assessment") to determine the degree, frequency or extent of CDD measures and ongoing monitoring conducted, which should vary in accordance with the assessed ML/TF risks associated with the customer or business relationship. The general idea is that, for instance, if the scale is from 1 to 10, then 10 will correspond to the highest risk and 1 to the lowest (the same logic should be if the scale will be from 1 to 100). Individual categories can be scored: 1–3 as lower risk, 4–7 medium risk, and 8–10 as high risk. These risk categories are then combined to produce a composite score. If the result exceeds the highest grade, it should be considered as prohibited, extremely high (intolerable). A simple model simply adds up the category totals, resulting in a score ranging. The model can be made more complex by weighting each of the factors and subfactors differently, for example by focusing more on customer type rather than on product or country. The model can be made even more complex, for example by creating combinations of factors that will determine the overall rating. The degree of complexity varies by organisation; the more complex, the more likely the rating will reflect the real client's overall risk.
AML Rule 4.2		**Business risk assessment (BURA)**
	3.4	Business risk assessment enables a Relevant Person to understand how and to what extent it is vulnerable to ML/TF.
	3.5	A Relevant Person should take appropriate steps to identify, assess, and understand its ML/TF risks which should include: (a) considering all relevant risk factors before determining the level of overall business risk and the appropriate level and type of mitigating measures to be applied (see sections 3.8 – 3.10); (b) keeping the risk assessment up-to-date (see section 3.11); (c) documenting the risk assessment (see section 3.12); (d) obtaining the approval of senior management of the risk assessment results (see section 3.13); and (e) having appropriate mechanisms to provide risk assessment information to the AFSA upon request.

	3.6	In conducting the business risk assessment, a Relevant Person should consider quantitative and qualitative information obtained from relevant internal and external sources to identify, manage and mitigate the risks. This may include consideration of relevant risk assessments and guidance issued by the FATF, inter-governmental organisations, governments and authorities from time to time, including Kazakhstan-wide ML/TF risk assessment and any higher risks notified to the Relevant Persons by the Financial Monitoring Agency of the Republic of Kazakhstan (the "FIU").
	3.7	The nature and extent of business risk assessment procedures should be commensurate with the nature, size and complexity of the business of a Relevant Person. For Relevant Persons whose businesses are smaller in size or less complex in nature (for example, where the range of products and services offered by the Relevant Person are very limited or its customers have a homogeneous risk profile), a simpler risk assessment approach might suffice. Conversely, where the Relevant Person's products and services are more varied and complex, or the Relevant Person's customers have more diverse risk profiles, a more sophisticated risk assessment process will be required.
AML Rule 4.2.1		**Considering relevant risk factors**
	3.8	A Relevant Person should holistically take into account relevant risk factors including country risk, customer risk, product/service/transaction risk, delivery/distribution channel risk and, where applicable, other risks that the Relevant Person is exposed to, depending on its specific circumstances. While there is no complete set of risk indicators, the list of risk indicators outlined in Annex 1 may help identify a higher or lower level of risk associated with the risk factors stated above that may be present in the business operations of a Relevant Person or its customer base and should be taken into account holistically whenever relevant in the business risk assessment. BURA should also consider: Complexity of business model Industries and target markets Geographic areas of main activity including transactions and customers residence Types of customers

		Characteristic of products and services in terms of exposure to financial crimes
	3.9	In determining the level of overall risk that the Relevant Person is exposed to, a Relevant Person should holistically consider a range of factors, including: (a) country risk, for example, the jurisdictions in which the Relevant Person is operating or otherwise exposed to, either through its own activities or the activities of customers, especially jurisdictions with greater vulnerability due to contextual and other risk factors such as: (i) the prevalence of crime, corruption, or financing of terrorism; (ii) the general level and quality of the jurisdiction's law enforcement efforts related to AML/CFT; (iii) the regulatory and supervisory regime and controls; and (iv) transparency of beneficial ownership; (b) customer risk, for example, the proportion of customers identified as high risk; (c) product/service/transaction risk, for example, (i) the characteristics of the products and services that it offers and transactions it executes, and the extent to which these are vulnerable to ML/TF abuse; (ii) the nature, diversity and complexity of its business, products and target markets; and (iii) whether the volume and size of transactions are in line with the usual activity of the Relevant Person and the profile of its customers; (d) delivery/distribution channel risk, for example, the distribution channels through which the Relevant Person distributes its products, including: (i) the extent to which the Relevant Person deals directly with the customer, the extent to which it relies on third parties to conduct CDD or other AML/CFT obligations and the extent to which the delivery/distribution channels are vulnerable to ML/TF abuse; and (ii) the complexity of the transaction chain (e.g. layers of distribution and sub-distribution); (e) other risks, for example, the review results of compliance, internal and external audits, as well as regulatory findings.

AML Rule 4.1.3	3.10	A Relevant Person should also identify and assess the ML/TF risks that may arise in relation to: (a) the development of new products and new business practices, including new delivery mechanisms (especially those that may lead to misuse of technological developments or facilitate anonymity in ML/TF schemes); and (b) the use of new or developing technologies for both new and pre-existing products, prior to the launch of the new products, new business practices or the use of new or developing technologies. The Relevant Person should take appropriate measures to mitigate and manage the risks identified.
AML Rule 4.3.1		**Keeping risk assessment up-to-date**
	3.11	A Relevant Person should review the business risk assessment regularly upon trigger events with material impact on the firm's business and risk exposure (e.g. a significant breach of the Relevant Person's AML/CFT Systems, the acquisition of new customer segments or delivery channels, the launch of new products and services by the Relevant Person, or a significant change of the Relevant Person's operational processes).
AML Rule 14.5.2		**Documenting risk assessment**
	3.12	A Relevant Person should maintain records and relevant documents of the business risk assessment, including the risk factors identified and assessed, the information sources taken into account, and the evaluation made on the adequacy and appropriateness of the Relevant Person's AML/CFT Systems.
		Obtaining senior management approval
	3.13	The business risk assessment should be communicated to, reviewed and approved by the senior management of the Relevant Person.
		Group-wide ML/TF risk assessment
AML Rule 14.2.1	3.14	Relevant Person with overseas branches and subsidiary undertakings should conduct a group-wide ML/TF risk assessment, to facilitate the Relevant Person to design and implement group-wide AML/CFT Systems as referred to in section 4.14.

AML Rule 14.2.2	3.15	Suppose a Relevant Person is a part of a financial group and a group – wide or regional ML/TF risk assessment has been conducted. In that case, it may make reference to or rely on those assessments provided that the assessments adequately reflect the ML/TF risks posed to the Relevant Person in the local context.
AML Rule 5.1		**Customer risk assessment**
	3.16	A Relevant Person should assess the ML/TF risks associated with a customer or a proposed business relationship and create a customer risk profile. The information obtained in the initial stages of the CDD process should enable a Relevant Person to conduct a customer risk assessment, which would determine the level of CDD measures to be applied. The measures must, however, comply with the legal requirements of the AML Rules. The general principle is that the amount and type of information obtained, and the extent to which this information is verified, should be increased where the risk associated with the business relationship is higher, or may be decreased where the associated risk is lower. Customer risk profile should include documentation of customers' intended activities and relationship with the company. The goal is to establish what is normal and expected activity, which forms baseline for monitoring unusual or suspicious activity. Customer risk profile should be created based on the triad – customer's inherent characteristics (demographics like the age, occupation, average income and source of funds/source of wealth, geographic region and products and services they are seeking. An ongoing monitoring should be based on the customer risk profile. Update of the customer risk profile should be performed according to the risk level (the higher risk, the more frequent).
	3.17	Based on a holistic view of the information obtained in the course of performing CDD measures, a Relevant Person should be able to finalise the customer risk assessment, which determines the level and type of ongoing monitoring (including keeping customer information up-to-date and transaction monitoring) and supports the decision of the Relevant Person whether to enter into, continue or terminate the business relationship. While a customer risk assessment should always be performed at the inception of a business relationship with a customer, a comprehensive risk profile for some customers may only become evident through time or based upon information received from a competent authority after establishing the business relationship. Therefore, a Relevant Person may have to

		periodically review and, where appropriate, update its risk assessment of a particular customer and adjust the extent of the CDD and ongoing monitoring to be applied to the customer.
	3.18	A Relevant Person should keep its policies and procedures under regular review and assess that its risk mitigation procedures and controls are working effectively.
AML Rule 5.1.3		**Conducting customer risk assessment**
	3.19	A Relevant Person may assess the ML/TF risks of a customer by assigning a ML/TF risk rating to its customers.
	3.20	Similar to other parts of the AML/CFT Systems, a Relevant Person should adopt an RBA in the design and implementation of its customer risk assessment framework, and the framework should be designed taking into account the results of the business risk assessment of the Relevant Person and commensurate with the risk profile and complexity of its customer base. The customer risk assessment should holistically take into account a customer's relevant risk factors, including the country risk, customer risk, product/service/transaction risk, and delivery/distribution channel risk, patterns of unusual behavior. Unusual behaviour of the customer is a behaviour that contradicts with expected activity of the customer based on available data. (For example, it may include inconsistency with the amount of initial capital, deposited funds, transactions with the provided source of funds and source of wealth, or inconsistency of the geographical area of transactions with the data provided at the onboarding stage, etc.). While there is no agreed-upon set of indicators, the list of risk indicators outlined in Annex 1 may identify a higher or lower level of risk associated with the risk factors stated above and should be taken into account holistically whenever relevant in determining the ML/TF risk rating of a customer.
AML Rule 14.5.2	3.21	Documenting customer risk assessment A Relevant Person should keep records and relevant documents of the customer risk assessment so that it can demonstrate to the AFSA, among others: (a) how it assesses its customer's ML/TF risks; and (b) the extent of CDD measures and ongoing monitoring is appropriate based on that customer's ML/TF risks.

Version	Date	Part 4	
AMLPG 003	19/12/2024	**AML/CFT Systems**	s. 4.1 – 4.17
		▪ *Internal control programmes for AML/CFT purposes*	s. 4.2 – 4.2.1
		▪ *Compliance management arrangements*	s. 4.6
		▪ *Senior management oversight*	s. 4.7 – 4.8
		▪ *Compliance officer and money laundering reporting officer*	s. 4.9 – 4.10
		▪ *Independent audit function*	s. 4.11 – 4.12
		▪ *Employee screening*	s. 4.13 – 4.13-1
		▪ *Group-wide AML/CFT Systems*	s. 4.14 – 4.17

Subject	4	AML/CFT SYSTEMS
	4.1	A Relevant Person must take all reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML/TF and to prevent a contravention of any requirement under AML Rules and AML Law. To ensure compliance with this requirement, a Relevant Person should implement appropriate AML/CFT Systems that are commensurate with the risks identified in its risk assessments.
		Internal control programmes for AML/CFT purposes
AML Law para 3 Article 11	4.2	Per paragraph 3 of Article 11 of the AML Law, a Relevant Person must develop, implement and execute its own Internal Control Rules that should include the following programmes: (a) The programme of organisation of internal control for AML/CFT purposes;

Chapters 2, 3, 4, 5, 6 of the AML Internal Controls Guidance		(b) ML/FT risk management programme; (c) Customer Identification Programme; (d) Programme for monitoring and analysing customer operations; (e) Training and education programme of the Relevant Persons in the field of the AML/CFT. A Relevant Person may develop other additional programmes pursuant to its Internal Control Rules.
Para 4 Chapter 1 of the AML Internal Controls Guidance	4.2.1	In case of amendments to the AML Law, applicable AML/CFT legislation in the AIFC, a Relevant Person must make the appropriate amendments to its Internal Control Rules within 30 calendar days.
AML Rule 4.3.1	4.3	A Relevant Person should: (a) have AML/CFT Systems, which are approved by senior management, to enable the Relevant Person to manage and mitigate the risks that have been identified; (b) monitor the implementation of the AML/CFT Systems and make enhancements if necessary; and (c) implement enhanced AML/CFT Systems to manage and mitigate the risks where higher risks are identified.
	4.4	A Relevant Person may implement simplified AML/CFT Systems to manage and mitigate the risks if lower risks are identified, provided that: (a) the lower ML/TF risk assessment is supported by an adequate analysis of risks having regard to the relevant risk factors and risk indicators; (b) the simplified AML/CFT Systems are commensurate with the lower ML/TF risks identified; and (c) the simplified AML/CFT Systems, which are approved by senior management, are subject to review from time to time. For the avoidance of doubt, a Relevant Person must not implement simplified AML/CFT Systems whenever there is any suspicion of ML/TF.

AML Rule 4.3.1	4.5	Having regard to the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses, a Relevant Person should implement adequate and appropriate policies, procedures, systems and controls which should, at minimum, include: (a) appropriate representation of AML compliance function in the managing, organising internal control system on AML matters; (b) risk management programme (BURA, CRA); (c) customer identification programme (KYC/CDD); (d) transaction monitoring and reviewing; (e) employees training and awareness programme; (f) adequate employee screening procedures (Know Your Employees); (g) independent audit to test the system. A Relevant Person may rely on a third party consultant to develop policies, procedures, systems and controls required for the purposes of AML Rule 4.3.1. Such third party consultant must perform its work with skill, care, and diligence and shall possess the following characteristics: 1) relevant knowledge and expertise, confirmed by the certificate from one of the internationally recognised professional organisations (such as ACAMS, ICA, ACFCS or analogy); 2) robust knowledge of the AIFC Acting Law and National AML regulation; 3) industry specific expertise confirmed by previous consulting experience in the AML/CFT, sanctions compliance field; 4) absence of negative feedback from the AFSA with regard to the work of such third party consultant conducted for other companies. The Relevant Person relying on such a third party shall bear ultimate responsibility for the policies, procedures, systems and controls adopted by the Relevant Person.
		Compliance management arrangements

	4.6	A Relevant Person should have appropriate compliance management arrangements that facilitate the Relevant Person to implement AML/CFT Systems to comply with relevant legal and regulatory obligations as well as to manage ML/TF risks effectively. Compliance management arrangements should, at a minimum, include oversight by the Relevant Person's senior management and appointment of a Compliance Officer (CO) and a Money Laundering Reporting Officer (MLRO).
		Senior management oversight
	4.7	The senior management of a Relevant Person is responsible for implementing effective AML/CFT Systems that can adequately manage the ML/TF risks identified. In particular, the senior management should: (a) appoint a CO at the senior management level to have the overall responsibility for the establishment and maintenance of the Relevant Person's AML/CFT Systems; and (b) appoint a senior staff member as the MLRO.
	4.8	In order that the CO and MLRO can discharge their responsibilities effectively, senior management should, as far as practicable, ensure that the CO and MLRO are: (a) appropriately qualified with sufficient AML/CFT knowledge; (b) subject to constraint of size of the Relevant Person, independent of all operational and business functions; (c) resident in the Republic of Kazakhstan – for MLRO (except in the case of the MLRO for a Registered Auditor); (d) of a sufficient level of seniority and authority within the Relevant Person; (e) provided with regular contact with, and when required, direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and that the business is taking sufficiently effective measures to protect itself against the risks of ML/TF; (f) fully conversant with the Relevant Person's statutory and regulatory requirements and the ML/TF risks arising from the Relevant Person's business; (g) capable of accessing, on a timely basis, all available information (both from internal sources such as CDD records and external sources such as circulars from the AFSA, the FIU and other relevant authorities); and

		(h) equipped with sufficient resources, including staff and appropriate cover for the absence of the CO and MLRO (i.e. an alternate or deputy CO and MLRO who should, where practicable, have the same status).
		Compliance officer (CO) and Money Laundering Reporting Officer (MLRO)
	4.9	The principal function of the CO is to act as the focal point within a Relevant Person for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the senior management to ensure that ML/TF risks are adequately identified, understood and managed. In particular, the CO should assume responsibility for: (a) developing and/or continuously reviewing the Relevant Person's AML/CFT Systems, including (where applicable) any group-wide AML/CFT Systems, to ensure they remain up-to-date, meet current statutory and regulatory requirements, and are effective in managing ML/TF risks arising from the Relevant Person's business; (b) overseeing all aspects of the Relevant Person's AML/CFT Systems, which include monitoring effectiveness and enhancing the controls and procedures where necessary; (c) communicating key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies; and (d) ensuring AML/CFT staff training is adequate, appropriate and effective.
Annex 5 – Principal functions expected from a MLRO	4.10	A Relevant Person should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the FIU and law enforcement agencies. The appointment should be carried out by the relevant decision-making body (or sole decision maker) pursuant to internal corporate arrangements of the Relevant Person. The MLRO should play an active role in identifying and reporting suspicious transactions. Principal functions expected from the MLRO are outlined in Annex 5 and include: (a) implementation of the AML/CFT – related internal controls; (b) carry out analysis of the Relevant Person's operations for AML/CFT purposes; and (c) cooperation with competent authorities. The individual appointed as MLRO needs to avoid conflicts of interest, whether real or potential. Thus, the MLRO should not combine the role of the business owner, shareholder or CEO/executive management due to the conflict of duties of the second line of defence.

		A MLRO's necessary skills and knowledge are outlined in Annex 5.
		Independent audit function
	4.11	Where practicable, a Relevant Person should establish an independent audit function which should have a direct line of communication to the senior management of the Relevant Person. Subject to appropriate segregation of duties, the function should have sufficient expertise and resources to enable it to carry out an independent review of the Relevant Person's AML/CFT Systems. The Guidance on the AML audit is outlined in the Annex 7.
	4.12	The audit function should regularly review the AML/CFT Systems to ensure effectiveness. This would include evaluating, among others: (a) the adequacy of the Relevant Person's AML/CFT Systems, ML/TF risk assessment framework and application of risk-based approach; (b) the effectiveness of the system for recognising and reporting suspicious transactions; (c) whether instances of non-compliance are reported to senior management on a timely basis; and (d) the level of awareness of staff having AML/CFT responsibilities. The frequency and extent of the review should be commensurate with the nature, size and complexity of the Relevant Person's businesses and the ML/TF risks arising from those businesses. Where appropriate, the Relevant Person should seek a review from external parties.
		Employee screening
	4.13	Relevant Persons should have adequate and appropriate screening procedures in order to ensure high standards when hiring employees (Know Your Employee).
	4.13-1	The relevant due diligence procedures should be applied to employees in sensitive roles. This could be background screening, verifying identity, checking criminal records, and references. An employee should be screened through the same lists and sources the company uses for prospective customers (sanctions, PEPs, watchlists, negative information).

		After on-boarding the new employee should be brought to the compliance culture by inoculating them with the main principles and values from the very beginning. They need to know and agree to abide by the code of conduct, ethics and compliance policy.
		Group-wide AML/CFT Systems
AML Rule 14.2.1	4.14	Subject to sections 4.15 and 4.16, a Relevant Person with overseas branches or subsidiary undertakings should implement group-wide AML/CFT Systems to apply the requirements set out in this Guidance to all of its overseas branches and subsidiary undertakings in its financial group, wherever the requirements in this Guidance is relevant and applicable to the overseas branches and subsidiary undertakings concerned. In particular, through its group-wide AML/CFT Systems, a Relevant Person should ensure that all of its overseas branches and subsidiary undertakings have procedures in place to ensure compliance with the CDD and record-keeping requirements, to the extent permitted by the laws and regulations of that place.
	4.15	Suppose the AML/CFT requirements in the jurisdiction where the overseas branch or subsidiary undertaking of a Relevant Person is located (host jurisdiction) differ from those relevant requirements referred to in section 4.14. In that case, the Relevant Person should require that branch or subsidiary undertaking to apply the higher of the two sets of requirements to the extent that the host jurisdiction's laws and regulations permit.
AML Rule 14.2.2	4.16	If the host jurisdiction's laws and regulations do not permit the branch or subsidiary undertaking of a Relevant Person to apply the higher AML/CFT requirements, particularly the CDD and record-keeping requirements, the Relevant Person should: (a) inform the AFSA of such failure; and (b) take additional measures to effectively mitigate ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the requirements.
	4.17	To the extent permitted by the laws and regulations of the jurisdictions involved and subject to adequate safeguards on the protection of confidentiality and use of the information being shared, including safeguards to prevent tipping-off, a Relevant Person should also implement, through its group-wide AML/CFT Systems for: (a) sharing information required for the purposes of CDD and ML/TF risk management; and

		(b) provision to the Relevant Person's group-level compliance, audit and/or AML/CFT functions of customer, account, and transaction information from its overseas branches and subsidiary undertakings, when necessary for AML/CFT purposes.

Version	Date	Part 5	
AMLPG 003	19/12/2024	**Customer Due Diligence**	s. 5.1 – 5.83
		▪ *What CDD measures are and when they must be carried out*	s. 5.1 – 5.2
		▪ *What CDD measures are*	s. 5.3 – 5.7
		▪ *When CDD measures must be carried out*	s. 5.8 – 5.10
		▪ *Identification and verification of the customer's identity*	s. 5.11
		▪ *Customer that is a natural person*	s. 5.12 – 5.14
		▪ *Customer that is a legal person*	s. 5.15 – 5.18
		▪ *Customer that is a trust or other similar legal arrangement*	s. 5.19 – 5.22
		▪ *Identification and verification of a beneficial owner (BO)*	s. 5.23 – 5.28
		▪ *Beneficial owner in relation to a natural person*	s. 5.29
		▪ *Beneficial owner in relation to a legal person*	s. 5.30
		▪ *Beneficial owner in relation to a Trust*	s. 5.31
		▪ *Ownership and control structure*	s. 5.32 – 5.36
		▪ *Threshold and indirect ownership*	s. 5.37 – 5.38
		▪ *Identification and verification of a person named to act on behalf of the customer*	s. 5.39 – 5.44
		▪ *Reliability of documents, data or information*	s. 5.45 – 5.49

		▪ *Purpose and intended nature of business relationship*	s. 5.50 – 5.51
		▪ *Delayed identity verification during the establishment of a business relationship*	s. 5.52 – 5.56
		▪ *Simplified customer due diligence (SDD)*	s. 5.57 – 5.60
		▪ *Listed company*	s. 5.61
		▪ *Government and public body*	s. 5.62 – 5.63
		▪ *Customer not physically present for identification purposes*	s. 5.64
		▪ *Special requirements*	s. 5.65 – 5.68
		▪ *Nominee shareholders*	s. 5.69
		▪ *Jurisdictions posing a higher risk*	s. 5.70 – 5.71
		▪ *Jurisdictions subject to a call by the FATF*	s. 5.72 – 5.73
		▪ *Reliance on CDD performed by third parties*	s. 5.74 – 5.80-1
		▪ *Third parties*	s. 5.81
		▪ *Failure to satisfactorily complete CDD measures*	s. 5.82
		▪ *Prohibition on anonymous accounts*	s. 5.83

Subject	**5**	**CUSTOMER DUE DILIGENCE**
		What CDD measures are and when they must be carried out

	5.1	The AML Rules defines what CDD measures are (see section 5.4) and also prescribes the circumstances in which a Relevant Person must carry out CDD (see section 5.8). This section provides guidance in this regard. Wherever possible, this Guidance gives Relevant Persons a degree of discretion in how they comply with the AML Rules and put in place procedures for this purpose. In addition, a Relevant Person should, in respect of each kind of customer, business relationship, product and transaction, establish and maintain effective AML/CFT Systems for complying with the CDD requirements set out in the AML Rules and this Guidance.
	5.2	Relevant Persons should determine the extent of CDD measures using an RBA, taking into account the higher or lower ML/TF risks identified in the customer risk assessment conducted by the Relevant Persons, so that preventive or mitigating measures are commensurate with the risks identified.
		What CDD measures are
	5.3	CDD information is a vital tool for recognising whether there are grounds for knowledge or suspicion of ML/TF.
	5.4	The following are CDD measures applicable to a Relevant Person: (a) identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source (see section 5.11); (b) where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity so that the Relevant Person is satisfied that it knows who the beneficial owner is, including, in the case of a legal person or trust, measures to enable the Relevant Person to understand the ownership and control structure of the legal person or trust (see sections 5.23 – 5.44); (c) obtain information on the purpose and intended nature of the business relationship (if any) established with the Relevant Person unless the purpose and intended nature are obvious (see sections 5.50 and 5.51); (d) understand and clarify the customer's sources of funds and sources of wealth; and (e) if a person purports to act on behalf of the customer: (i) identify the person and take reasonable measures to verify the person's identity using documents, data or information provided by a reliable and independent source; and

		(ii) verify the person's authority to act on behalf of the customer (see sections 5.39 – 5.44).
AIFC Glossary, AML Rule 5.1.16 (Guidance on the term "customer")	5.5	The term "customer" is defined in the AIFC Glossary and AML Rules. The meaning of "customer" and "client" should be inferred from their everyday meaning and the industry practice context.
	5.6	In determining what constitutes reasonable measures to verify the identity of a beneficial owner and reasonable measures to understand the ownership and control structure of a legal person or trust, the Relevant Person should consider and give due regard to the ML/TF risks posed by a particular customer and a particular business relationship. Due consideration should also be given to the guidance in relation to customer risk assessment set out in Part 3.
	5.7	Relevant Persons should adopt a balanced and common-sense approach with regard to customers connected with jurisdictions posing a higher risk (see sections 5.70 and 5.71). While extra care may well be justified in such cases, unless the AFSA has, through a "notice in writing", imposed a general or specific requirement (see section 5.73), it is not a requirement that Relevant Persons should refuse to do any business with such customers or automatically classify them as high risk. Rather, Relevant Persons should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/TF.
		When CDD measures must be carried out
AML Rule 6.1.1 AML Rule 6.2.1	5.8	A Relevant Person must carry out CDD measures in relation to a customer: (a) at the outset of a business relationship; (b) before performing any occasional transaction: (i) with Digital Assets the value of which singularly or in several linked operations (whether at the time or later), is equal or exceeds USD 1,000; (ii) equal to or exceeding an aggregate value of USD 15,000, whether carried out in a single operation or several operations that appear to the Relevant Person to be linked; or

		(iii) a wire transfer equal to or exceeding an aggregate value of USD 1,000, whether carried out in a single operation or several operations that appear to the Relevant Person to be linked; (c) when the Relevant Person suspects that the customer or the customer's account is involved in ML/TF; or (d) when the Relevant Person doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.
	5.9	Relevant Persons should be vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD thresholds of USD 1,000 for wire transfers or transactions with Digital Assets and USD 15,000 for other types of transactions. Where Relevant Persons become aware that these thresholds are met or exceeded, CDD measures must be carried out.
	5.10	The factors linking occasional transactions are inherent in the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over a short period, where a customer regularly transfers funds to one or more destinations. In determining whether the transactions are in fact linked, Relevant Persons should consider these factors against the timeframe within which the transactions are conducted.
		Identification and verification of the customer's identity
AML Rule 6.3.1	5.11	The Relevant Person must identify the customer and verify the customer's identity by reference to documents, data or information provided by a reliable and independent source: (a) a governmental body or public registry; (b) the AFSA's Public Register or any other authority; (c) an authority in a place outside AIFC that performs functions similar to those of the AFSA or any other authority; or (d) any other reliable and independent source.
		Customer that is a natural person
	5.12	For a customer that is a natural person, Relevant Persons should identify the customer by obtaining at least the following identification information:

		(a) full name; (b) date of birth; (c) nationality; (d) unique identification number (e.g. identity card number or passport number) and document type; and (e) registration address (if any).
	5.13	In verifying a customer's identity that is a natural person, a Relevant Person should verify the name, date of birth, unique identification number, and document type of the customer. The Relevant Person should do so by reference to documents, data or information provided by a reliable and independent source. Examples of such documents, data or information include: (a) national identity card bearing the individual's photograph; (b) valid travel document (e.g. unexpired passport); or (c) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body). The Relevant Person should retain a copy of the individual's identification document or record.
	5.14	A Relevant Person should obtain the residential address information of a customer that is a natural person.
		Customer that is a legal person
	5.15	For a customer that is a legal person, a Relevant Person should identify the customer by obtaining at least the following identification information: (a) full name; (b) date of incorporation, establishment or registration; (c) place of incorporation, establishment or registration (including address of registered office); (d) unique identification number (e.g. incorporation number or business registration number) and document type; and (e) principal (actual) place of business (if different from the address of registered office).

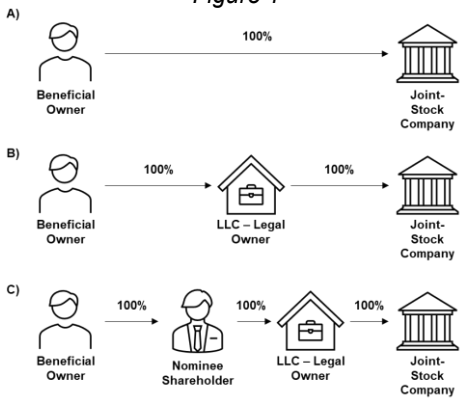
	5.16	In verifying a customer's identity that is a legal person, a Relevant Person should normally verify its name, legal form, current existence (at the time of verification), and powers that regulate and bind the legal person. The Relevant Person should do so by reference to documents, data or information provided by a reliable and independent source. Examples of such documents, data or information include: (a) certificate of incorporation; (b) record of companies registry; (c) incumbency data; (d) tax certificate; (e) record of registration; (f) partnership agreement; (g) constitutive document; or (h) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body). Examples of possible measures to verify a legal person's name, legal form, and current existence are set out in section 3 of Annex 3.
	5.17	For a customer that is a partnership or an unincorporated body, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to provide reliable and independent evidence of the identity of the customer as required in section 5.16 provided that: (a) the customer is a well-known, reputable organisation; (b) the customer has a long history in its industry; and (c) there is substantial public information about the customer, its partners and controllers.
	5.18	In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, a Relevant Person should satisfy itself as to the legitimate purpose of the organisation, e.g. by requesting sight of the constitutive document.

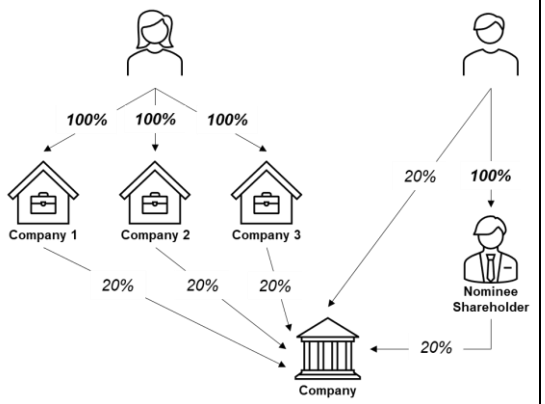
		Customer that is a trust or other similar legal arrangement
	5.19	In respect of trusts, a Relevant Person should identify and verify the trust as a customer in accordance with the requirements set out in section 5.20 and 5.21. The Relevant Person should also regard the trustee as its customer if the trustee enters into a business relationship or carries out occasional transactions on behalf of the trust, which is generally the case if the trust does not possess a separate legal personality. In such a case, a Relevant Person should identify and verify the trustee's identity in line with the identification and verification requirements for a customer that is a natural person or, where applicable, a legal person.
	5.20	For a customer that is a trust or other similar legal arrangement, Relevant Persons should identify the customer by obtaining at least the following identification information: (a) the name of the trust or legal arrangement; (b) date of establishment or settlement; (c) the jurisdiction whose laws govern the trust or legal arrangement; (d) unique identification number (if any) granted by any applicable official bodies and document type (e.g. tax identification number or registered charity or non-profit organisation number); and (e) address of registered office (if applicable).
	5.21	In verifying a customer's identity that is a trust or other similar legal arrangement, a Relevant Person should normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the trust or other similar legal arrangement. The Relevant Person should do so by reference to documents, data or information provided by a reliable and independent source. Examples of such documents, data or information include: (a) trust deed or similar instrument; (b) record of an appropriate register in the relevant country of establishment; (c) written confirmation from a trustee acting in a professional capacity; (d) written confirmation from a lawyer who has reviewed the relevant instrument; or

		(e) written confirmation from a trust company which is within the same financial group, if the trust concerned is managed by that trust company.
	5.22	A Relevant Person may adopt an RBA in determining the documents, data, or information to be obtained to verify a customer's identity that is a legal person, trust, or other similar legal arrangement.
		Identification and verification of a beneficial owner (BO)
	5.23	The issue of ultimate beneficial owners or controllers has become increasingly important internationally as it plays a central role in transparency, the integrity of the financial sector, and law enforcement efforts.
	5.24	Anonymity enables many illegal activities to take place hidden from law enforcement authorities, such as tax evasion, corruption, money laundering, and financing of terrorism. For example, money laundering can involve complex operations and transactions to make money from illicit sources, such as drug trafficking or tax evasion, appear legal. A drug trafficker, for instance, could set up a nightclub in order to appear to have legal sources of income from the sale of tickets and alcohol, while in reality, the money is from the sale of drugs. It is therefore important to know the BOs of legal entities and arrangements to prevent misuse in a business setting. That is why the FATF have included beneficial ownership requirements in their standards and conduct assessments across jurisdictions on the availability of beneficial ownership information in their systems.
	5.25	Determining whether the countries have access to information on the BOs of legal entities and arrangements is important in combatting tax evasion, corruption, money laundering, and the financing of terrorism.
	5.26	A beneficial owner is normally a natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. A Relevant Person must identify any beneficial owner in relation to a customer and take reasonable measures to verify the beneficial owner’s identity so that the Relevant Person is satisfied that it knows who the beneficial owner is.
	5.27	Where a natural person is identified as a beneficial owner, the Relevant Person should endeavour to obtain the same identification information as in section 5.12 as far as possible.
AIFC Glossary	5.28	The term “beneficial owner” is interpreted by reference to the AIFC Glossary.

		Beneficial owner in relation to a natural person
	5.29	In respect of a customer that is a natural person, there is no requirement on Relevant Persons to make proactive searches for beneficial owners of the customer in such a case, but they should make appropriate enquiries where there are indications that the customer is not acting on his own behalf.
		Beneficial owner in relation to a legal person
AIFC Companies Regulations 179-1 (a)	5.30	The AIFC Companies Regulations define beneficial owner in relation to a company as: A natural person who: in relation to a company: (i) owns or controls (directly or indirectly) Shares in the share capital of the company or other Ownership Interests in the Relevant Person of at least 25%; (ii) owns or controls (directly or indirectly) voting rights in the Relevant Person of at least 25%; (iii) owns or controls (directly or indirectly) the right to appoint or remove the majority of the Directors of the Relevant Person; or (iv) has the legal right or through other ownership interests to exercise, or actually exercises, significant control or influence over the activities of the company.
AIFC Companies Regulations 179-1 (b)	5.30.1	The AIFC Companies Regulations define beneficial owner in relation to a partnership as a natural person who has the legal right to exercise, or actually exercises, significant control or influence over the activities of the partnership.
AIFC Companies Regulations 179-1 (c)	5.30.2	The AIFC Companies Regulations define beneficial owner in relation to a Foundation or a Non-Profit Incorporated Organisation as a natural person who has the legal right to exercise, or actually exercises, significant control or influence over the activities of the Governing Body, Person or other arrangement administering the property or carrying out the objects of the Foundation, or Non-Profit Incorporated Organisation.
	5.30.3	For a customer that is a legal person, a Relevant Person should identify any natural person who ultimately has a controlling ownership interest (i.e. more than 25%) in the legal person and any natural person exercising control of the legal person or its management, and take reasonable measures to verify their identities. If there is no such natural person, the Relevant

		Person should identify the relevant natural persons who hold the position of senior managing official in the legal person and take reasonable measures to verify their identities.
AIFC Companies Regulations 179-3	5.30.4	While a Relevant Person usually can identify who the beneficial owner of a customer is in the course of understanding the ownership and control structure of the customer, the Relevant Person may obtain an undertaking or declaration from the customer on the identity of, and the information relating to, its beneficial owner. Nevertheless, in addition to the undertaking or declaration obtained, the Relevant Person should take reasonable measures to verify the beneficial owner's identity (e.g. corroborating the undertaking or declaration with publicly available information).
	5.30.5	If the ownership structure of a customer involves different types of legal persons or legal arrangements, in determining who the beneficial owner is, a Relevant Person should pay attention to who has ultimate ownership or control over the customer, or who constitutes the controlling mind and management of the customer.
		Beneficial owner in relation to a Trust
	5.31	The AIFC Trust Regulations define beneficial owner in relation to a Trust as any party to the Trust, including the Settlor, Enforcer, Protector, Beneficiaries, any other Trustees and any other natural person exercising ultimate effective control over the Trust.
	5.31.1	For trusts, a Relevant Person should identify the settlor, the protector (if any), the enforcer (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate control over the trust (including through a chain of control or ownership), and take reasonable measures to verify their identities. For other similar legal arrangements, a Relevant Person should identify any natural person in equivalent or similar positions to beneficial owner of a trust as stated above and take reasonable measures to verify the identity of such person. If a trust or other similar legal arrangement is involved in a business relationship and a Relevant Person does not regard the trustee (or equivalent in the case of other similar legal arrangement) as its customer pursuant to section 5.19 (e.g. when a trust appears as part of an intermediate layer referred to in section 5.32), the Relevant Person should also identify the trustee (or equivalent) and take reasonable measures to verify the identity of the trustee (or equivalent) so that the Relevant Person is satisfied that it knows who that person is.
	5.31.2	For a beneficiary of a trust designated by characteristics or by class, a Relevant Person should obtain sufficient information (e.g. a Relevant Person may ascertain and name the scope of the class of beneficiaries, such as children of a named

		individual) concerning the beneficiary to satisfy the Relevant Person that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights.
		Ownership and control structure
AML Rule 5.1.5	5.32	Where a customer is not a natural person, a Relevant Person should understand its ownership and control structure, including identification of any intermediate layers (e.g. by reviewing an ownership chart of the customer). The objective is to follow the chain of ownerships to the beneficial owners of the customer. A trust or other similar legal arrangement can also be part of an intermediate layer in an ownership structure, and should be dealt with in similar manner to a company being part of an intermediate layer.
	5.33	In Figure 1, a basic example demonstrates how the use of a legal entity or arrangement can obscure the identity of a beneficial owner. When an individual is the sole shareholder of a company and controls it directly, that individual is the BO of the company. However, there may be more layers involved in the ownership structure, perhaps a chain of entities between a legal vehicle and its BO. Example B) shows an additional layer – the limited liability company (LLC) – between the legal vehicle (the Joint Stock Company) and its beneficial owner. The LLC, as the shareholder of the Joint Stock Company, is its direct legal owner, while the beneficial owner indirectly controls the joint stock company through the LLC. *Figure 1*  The longer the chain of entities between a legal vehicle, the harder it is to identify the BO, given the need to determine who controls each of the layers. Another factor that makes it difficult to identify a BO is nominees, presented in example C). The use of nominees, whereby an entity allows its name to appear as a shareholder or owner in the name of someone else (whose identity remains concealed), is prohibited in some countries but legal in others. In some cases, nominee shareholders mask the real BO.
	5.34	Where a customer has a complex ownership or control structure, a Relevant Person should obtain sufficient information for the Relevant Person to satisfy itself that there is a legitimate reason behind the particular structure employed.

AML Rule 5.1.6 (e)	5.34	The ownership or control can be exercised in a variety of ways: for example, holding a controlling ownership interest (e.g. 25 per cent or more) of a legal person. Other ways include control of a significant percentage of voting rights, or the ability to name or remove the members of an entity's board of directors.
	5.36	Effective control can be exercised in other ways. For example, control may be evident in influence over or a veto of the decisions that an entity makes, through agreements among shareholders or members, through family links or other types of connections with decision-makers, or by holding negotiable shares or convertible stock from an entity. An important consideration to keep in mind is that determining the BO is independent of the BO's nationality.
		Threshold and indirect ownership
	5.37	The BOs of legal persons or trusts must always be individuals (natural persons), who are their owners or controllers, either through direct or indirect means (except for publicly traded commercial companies or public collective investment vehicles). Neither nominees nor chains of companies should prevent the BO from being identified. As Figure 2 shows, a company can have two BOs (a woman with 60 per cent through three commercial companies and a man with 40 per cent, including through a nominee), although no direct owner holds more than 25 per cent of the assets (in Figure 2, each legal shareholder holds only 20 per cent). *Figure 2* 
AML Rule 6.3.4	5.38	See also the AML Rules for Guidance on identification and verification of beneficial owners.
Guidance on customer due diligence	5.38-1	In order to correctly understand the sources of funds and wealth, the Relevant Person should collect information from the clients themselves, for instance, in the form of a special paper or digital form. This form should allow the client to indicate among others their demographic data, occupation, sources of origin and indicate their approximate average income. It is important to inform the client about the need to indicate the actual volume of existing income, and not the desired one. Depending on the information collected while establishing risk profile of the client, the Relevant Person will be able to establish an understanding of what is usual for the client with this particular set of characteristics and what will go beyond the usual behavior/activity. Thus, characteristics that go beyond the usual behavior should be a criterion that increases

		the risks of a customer at the CDD stage. In case of increased risks, the EDD procedures should be applied to verify the sources of funds and wealth. The absence of requirement to request additional documented confirmation of the source of funds or wealth in the case of standard CDD should not mislead the Relevant Person into considering that there is no need to apply enhanced verification measures and limit the use of the EDD. The risk-based verification should be applied. In particular the client risk assessment system should stipulate that the Relevant Person, adapting it to the certain characteristics and specifics of the business, determines what is usual (understandable and explainable) and what raises doubts or concerns. Factors that raise doubts or concerns should increase the level of risk and provide for appropriate enhanced measures.
AML Rule 5.1.6 Guidance on high risk customers		**Identification and verification of a person named to act on behalf of the customer**
	5.39	A person may be appointed to act on behalf of a customer to establish business relationships or may be authorised to give instructions to a Relevant Person to conduct various activities through the account or the business relationship established. Whether the person is considered to be a person acting on behalf of the customer should be determined based on the ML/TF risks associated with that person's roles and the activities which the person is authorised to conduct, as well as the ML/TF risks associated with the business relationship. Relevant Persons should implement clear policies for determining who is considered to be a person acting on behalf of the customer.
	5.40	If a person acts on behalf of the customer, Relevant Persons must: (a) identify the person and take reasonable measures to verify the person's identity by reference to documents, data or information provided by a reliable and independent source: (i) a governmental body or central registry; (ii) the AFSA's Public Register or any other authority; (iii) an authority that performs functions similar to those of the AFSA; or (iv) any other reliable and independent source; and

		(b) verify the person's authority to act on behalf of the customer.
	5.41	Relevant Person should identify a person acting on behalf of the customer in line with the identification requirements for a customer that is a natural person or, where applicable, a legal person. In taking reasonable measures to verify the identity of the person acting on behalf of the customer, Relevant Person should, as far as possible, follow the verification requirements for a customer that is a natural person or, where applicable, a legal person.
	5.42	Relevant Persons should verify the authority of each person acting on behalf of the customer by appropriate documentary evidence (e.g. board resolution or similar written authorisation).
	5.43	Where the legal owner acts on behalf of another person as a nominee or under a similar arrangement, that other person—rather than the legal owner—may be the beneficial owner. For example, most nominees hold shares or exercise other rights in an entity on behalf of another, but nominees can also hold bank accounts or act as directors. In some cases, the purpose of the nominee is to avoid disclosure of the BO.
	5.44	Nominees can arise in many forms: corporate shell entities, trusts, professional advisors, or even family members.
		Reliability of documents, data or information
	5.45	In verifying the identity of a customer, a Relevant Person needs not establish accuracy of every piece of identification information collected in sections 5.12, 5.15 and 5.20.
	5.46	A Relevant Person should ensure that documents, data or information obtained for the purpose of verifying the identity of a customer as required in sections 5.13, 5.16 and 5.21 is current at the time they are provided to or obtained by the Relevant Person.
	5.47	When using documents for verification, a Relevant Person should be aware that some types of documents are more easily forged than others, or can be reported as lost or stolen. Therefore, the Relevant Person should consider applying anti-fraud procedures that are commensurate with the risk profile of the person being verified.
	5.48	If a natural person customer or a person representing a legal person, a trust or other similar legal arrangement to establish a business relationship with a Relevant Person is physically present during the CDD process, the Relevant Person should generally have sight of original identification document by its staff and retain a copy of the document.

		However, there are a number of occasions where an original identification document cannot be produced by the customers (e.g. the original document is in electronic form). In such an occasion, the Relevant Person should take appropriate measures to ensure the reliability of identification documents obtained.
	5.49	Where the documents, data or information being used for the purposes of identification are in a foreign language, appropriate steps should be taken by the Relevant Person to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.
		Purpose and intended nature of business relationship
AML Rule 5.1.3	5.50	A Relevant Person must understand the purpose and intended nature of the business relationship. In some instances, this will be self-evident, but in many cases, the Relevant Person may have to obtain information in this regard.
	5.51	Unless the purpose and intended nature of the business relationship are obvious, Relevant Persons should obtain satisfactory information from all new customers as to the intended purpose and reason for opening the account or establishing the business relationship, and record the information on the account opening documentation. The information obtained by the Relevant Persons should be commensurate with the risk profile of the customers and the nature of the business relationships. Information that might be relevant may include: (a) nature and details of the customer's business/occupation/employment; (b) the anticipated level and nature of the activity that is to be undertaken through the business relationship (e.g. what the typical transactions are likely to be); (c) location of the customer; (d) the expected source and origin of the funds to be used in the business relationship; and (e) initial and ongoing source(s) of wealth or income.
AML Rule 6.2.3 AML Rule 6.2.4 AML Rule 6.2.5		**Delayed identity verification during the establishment of a business relationship**

	5.52	A Relevant Person should verify the identity of a customer and any beneficial owner of the customer before or during the course of establishing a business relationship or conducting transactions for occasional customers. However, Relevant Persons may, exceptionally, verify the identity of a customer and any beneficial owner of the customer after establishing the business relationship, provided that: (a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed; (b) it is necessary not to interrupt the normal conduct of business with the customer; and (a) verification is completed as soon as reasonably practicable.
	5.53	An example of a situation in the securities industry where it may be necessary not to interrupt the normal conduct of business is when companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
	5.54	If a Relevant Person allows verification of the identity of a customer and any beneficial owner of the customer after establishing the business relationship, it should adopt appropriate risk management policies and procedures concerning the conditions under which the customer may utilise the business relationship prior to verification. These policies and procedures should include: (a) establishing a reasonable timeframe for the completion of the identity verification measures and the follow-up actions if exceeding the timeframe (e.g. to suspend or terminate the business relationship); (b) placing appropriate limits on the number, types, and/or amount of transactions that can be performed; (c) monitoring of large and complex transactions being carried out outside the expected norms for that type of relationship; (d) keeping senior management periodically informed of any pending completion cases; and (e) ensuring that funds are not paid out to any third party. Exceptions may be made to allow payments to third parties subject to the following conditions: (i) there is no suspicion of ML/TF;

		(ii) the risk of ML/TF is assessed to be low; (iii) the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction; and (iv) the names of recipients do not match with watch lists such as those for terrorist suspects and PEPs.
	5.55	Verification of identity should be completed by a Relevant Person within a reasonable timeframe, which generally refers to the following: (a) the Relevant Person completing such verification no later than 30 working days after the establishment of business relationship; (b) the Relevant Person suspending business relationship with the customer and refraining from carrying out further transactions if such verification remains uncompleted within 30 working days after the establishment of business relationship; and (c) the Relevant Person terminating business relationship with the customer if such verification remains uncompleted 120 working days after the establishment of business relationship.
	5.56	If verification cannot be completed within the reasonable timeframe set in the Relevant Person's risk management policies and procedures, the Relevant Person should terminate the business relationship as soon as reasonably practicable and refrain from carrying out further transactions. The Relevant Person should also assess whether this failure provides grounds for knowledge or suspicion of ML/TF and consider making a suspicious transaction report (STR) to the FIU, particularly if the customer requests that funds or other assets be transferred to a third party or be "transformed" (e.g. from cash into a cashier order) without a justifiable reason.
		Simplified customer due diligence (SDD)
AML Rule 8.1	5.57	Relevant Persons may not to identify and take reasonable measures to verify the identities of the beneficial owners of specific types of customers (referred to as "simplified customer due diligence"; and as "SDD" hereafter). However, other aspects of CDD must be undertaken and it is still necessary to conduct ongoing monitoring of the business relationship. The use of SDD must be supported by robust assessment to ensure the conditions or circumstances of specific types of customers or products are met.

	5.58	Nonetheless, SDD must not be or continue to be applied when the Relevant Person suspects that the customer, the customer's account or the transaction is involved in ML/TF, or when the Relevant Person doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity, notwithstanding when the customer falls within section 5.59 below.
	5.59	A Relevant Person may apply SDD if the customer is – (a) an institution that is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the AFSA's; (b) a corporation listed on any stock exchange ("listed company"); (d) the Government or any public body in the Republic of Kazakhstan; or (e) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.
	5.60	For avoidance of doubt, the Relevant Person must still: (a) identify the customer and verify the customer's identity; (b) if a business relationship is to be established and its purpose and intended nature are not obvious, obtain information on the purpose and intended nature of the business relationship with the Relevant Person; and (c) if a person purports to act on behalf of the customer, (i) identify the person and take reasonable measures to verify the person's identity; and (ii) verify the person's authority to act on behalf of the customer, in accordance with the relevant requirements stipulated in this Guidance.
		Listed company
	5.61	A Relevant Person may apply SDD to a customer that is a company listed on a stock exchange. For this purpose, the Relevant Person should assess whether there are any disclosure requirements (either by stock exchange rules, or through law or enforceable means) which ensure the adequate transparency of the beneficial ownership of companies listed on

		that stock exchange. In such a case, it will be generally sufficient for a Relevant Person to obtain proof of the customer's listed status on that stock exchange.
		Government and public body
	5.62	Relevant Persons may apply SDD to a customer that is the Kazakhstan government, any public bodies in Kazakhstan, the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.
	5.63	Public body includes: (a) any executive, legislative, municipal or urban council; (b) any Government department or undertaking; (c) any local or public authority or undertaking; (d) any board, commission, committee or other body that has power to act in a public capacity under or for the purposes of any enactment.
		Customer not physically present for identification purposes
CDD for non-face-to-face business relations	5.64	Relevant Persons must apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview. Where a customer has not been physically present for identification purposes, Relevant Persons will generally not be able to determine that the documentary evidence of identity actually relates to the customer they are dealing with. Consequently, there are increased risks.
		Special requirements
	5.65	A Relevant Person should take additional measures to mitigate any risk (e.g. impersonation risk) associated with customers not physically present for identification purposes. If a customer has not been physically present for identification purposes, the Relevant Person must carry out at least one of the following additional measures to mitigate the risks posed: (a) further verifying the customer's identity on the basis of documents, data or information;

		(b) taking supplementary measures to verify information relating to the customer that has been obtained by the Relevant Person; or (c) ensuring that the first payment made into the customer's account is received from an account in the customer's name with an authorized institution or a bank operating in an equivalent jurisdiction that has measures in place to ensure compliance with AML Rules requirements and is supervised for compliance with those requirements by a banking regulator in that jurisdiction.
	5.66	The extent of additional measures set out in section 5.65 will depend on the nature and characteristics of the product or service requested and the assessed ML/TF risk presented by the customer.
	5.67	Section 5.65 (b) allows a Relevant Person to utilise different methods to mitigate the risk. These may include measures such as (i) use of an independent and appropriate person to certify identification documents; (ii) checking relevant data against reliable databases or registries; or (iii) using appropriate technology, etc. Whether a particular measure or a combination of measures is acceptable should be assessed on a case-by-case basis. The Relevant Person should ensure and be able to demonstrate to the AFSA that the supplementary measure(s) taken can adequately guard against impersonation risk.
	5.68	While the requirements to undertake additional measures generally apply to a customer that is a natural person, a Relevant Person should also mitigate any increased risk (e.g. applying additional due diligence measures set out in section 5.65 if a customer that is not a natural person establishes a business relationship with a Relevant Person through a non-face-to-face channel. The increased risk may arise from circumstances where the natural person acting on behalf of the customer to establish the business relationship is not physically present for identification purposes. In addition, where a Relevant Person is provided with copies of documents for identifying and verifying a legal person customer's identity, a Relevant Person should also mitigate any increased risk (e.g. applying additional due diligence measures set out in section 5.65).
		Nominee shareholders
	5.69	For a customer identified to have nominee shareholders in its ownership structure, a Relevant Person should obtain satisfactory evidence of the identities of the nominees, and the persons on whose behalf they are acting, as well as the details of arrangements in place, in order to determine who the beneficial owner is.
		Jurisdictions posing a higher risk

	5.70	Relevant Persons should give particular attention to, and exercise extra care in respect of: (a) business relationships and transactions with persons (including legal persons and other entities) from or in jurisdictions identified by the FATF as having strategic AML/CFT deficiencies; and (b) transactions and business connected with jurisdictions assessed as higher risk.
	5.71	In determining which jurisdictions are identified by the FATF as having strategic AML/CFT deficiencies, or may otherwise pose a higher risk, Relevant Persons should consider, among other things: (c) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems; (d) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity; (e) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the UN; or (f) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operation. "Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations.
		Jurisdictions subject to a call by the FATF
	5.72	A Relevant Persons should apply additional measures, proportionate to the risks within business relationships and transactions with natural and legal persons, and Relevant Persons, from jurisdictions for which this is called for by the FATF.
	5.73	Where mandatory enhanced measures or countermeasures are called for by the FATF, or in other circumstances independent of any call by the FATF but also considered to be higher risk, the AFSA may also, through a notice in writing require Relevant Persons to undertake specific countermeasures identified or described in the notice.

		The type of measures would be proportionate to the nature of the risks and/or deficiencies.
		Reliance on CDD performed by third parties
AML Rule 9.1	5.74	A Relevant Persons may rely upon a third party to perform any part of the CDD measures, subject to the criteria set out in the AML Rules. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the Relevant Person. In a third-party reliance scenario, the third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying Relevant Person and would apply its own procedures to perform the CDD measures.
	5.75	For the avoidance of doubt, reliance on third parties does not apply to outsourcing or agency relationships, in which the outsourced entity or agent applies the CDD measures on behalf of the Relevant Person, in accordance with the Relevant Person's procedures, and subject to the Relevant Person's control of effective implementation of these procedures by the outsourced entity or agent.
	5.76	When relying on a third party, the Relevant Person must be satisfied that the third party will on request provide a copy of any document, or a record of any data or information, obtained by the third party in the course of carrying out the CDD measures without delay.
	5.77	A Relevant Person that carries out a CDD measure by means of a third party must immediately after the intermediary has carried out that measure, obtain from the third party the data or information that the third party has obtained in the course of carrying out that measure, but nothing in this section requires the Relevant Person to obtain at the same time from the third party a copy of the document, or a record of the data or information, that is obtained by the third party in the course of carrying out that measure.
	5.78	Where these documents and records are kept by the third party, the Relevant Person should obtain an undertaking from the third party to keep all underlying CDD information throughout the continuance of the Relevant Person's business relationship with the customer and for at least six years beginning on the date on which the business relationship of a customer with the Relevant Person ends or until such time as may be specified by the AFSA. The Relevant Person must ensure that the third party will, if requested by the Relevant Person within the period specified in the record-keeping requirements of the AML Rules, provide to the Relevant Person a copy of any document, or a record

		of any data or information, obtained by the third party in the course of carrying out that measure as soon as reasonably practicable after receiving the request. The Relevant Person should also obtain an undertaking from the third party to supply copies of all underlying CDD information in circumstances where the third party is about to cease trading or does not act as a third party for the Relevant Person anymore.
	5.79	A Relevant Person should conduct sample tests from time to time to ensure CDD information and documentation is produced by the third party upon demand and without undue delay.
	5.80	Whenever a Relevant Person has doubts as to the reliability of the third party, it should take reasonable steps to review the third party's ability to perform its CDD duties. If the Relevant Person intends to terminate its relationship with the third party, it should immediately obtain all CDD information from the third party. If the Relevant Person has any doubts regarding the CDD measures carried out by the third party previously, the Relevant Person should perform the required CDD as soon as reasonably practicable.
	5.80-1	A Relevant Person must not rely on third parties to provide ongoing monitoring CDD procedures. It should be the responsibility of the Relevant Person to conduct ongoing due diligence throughout the course of the business relationship to ensure consistency of the transactions with the Relevant Person's knowledge of the customer, their business and risk profile, including, the source of funds.
		Third parties
AML Rule 9.1.1	5.81	A Relevant Person may rely on the following third parties to conduct one or more elements of CDD on its behalf: (a) an Authorised Person; (b) a law firm, notary, or other independent legal business, accounting firm, audit firm or insolvency practitioner or an equivalent person in another jurisdiction; (c) a Regulated Financial Institution; or (d) a member of the Relevant Person's Group.
		Failure to satisfactorily complete CDD measures

	5.82	Where a Relevant Person is unable to complete the CDD measures in accordance with section 5.8 or 5.52, the Relevant Person: (a) must not establish a business relationship or carry out any occasional transaction with that customer; or (b) must terminate the business relationship as soon as reasonably practicable if the Relevant Person has already established a business relationship with the customer. The Relevant Person should also assess whether this failure provides grounds for knowledge or suspicion of ML/TF and where there is relevant knowledge or suspicion, should make an STR to the FIU in relation to the customer.
		Prohibition on anonymous accounts
	5.83	Relevant Persons must not maintain anonymous accounts or accounts in fictitious names for any new or existing customer. Where numbered accounts exist, Relevant Persons must maintain them in such a way that full compliance can be achieved with the AML Rules. Relevant Persons must properly identify and verify the identity of the customer in accordance with this Guidance. In all cases, whether the relationship involves numbered accounts or not, the customer identification and verification records must be available to the AFSA, other authorities, the CO, auditors, and other staff with appropriate authority.

Version	Date	Part 6	
AMLPG 003	19/12/2024	**Politically Exposed Persons (PEPs)**	s. 6.1 – 6.14
		▪ *General*	s. 6.1 – 6.7
		▪ *Special requirements and additional measures for PEPs*	s. 6.8 – 6.15

Subject	6	POLITICALLY EXPOSED PERSONS (PEPs)
		General
	6.1	Much international attention has been paid in recent years to the risk associated with providing financial and business services to those with a prominent political profile or holding senior public status. However, PEP status itself does not automatically mean that the individuals are corrupt or that they have been incriminated in any corruption.
	6.2	However, their status and position may render PEPs vulnerable to corruption. The risks increase when the person concerned is from a foreign country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards.
AIFC Glossary	6.3	Politically Exposed Person. A PEP is a natural person (including a family member or known associate) who is or has been entrusted with a prominent public function, including but not limited to: a head of state or of government, senior politician, member of a legislative or constitutional assembly, senior government official, senior judicial official, senior military officer, ambassador, senior person in an international organisation, senior executive of a state-owned entity, a senior political party official, or an individual who has been entrusted with similar functions such as a director or a deputy director; at an international, national, or regional level. This definition does not include middle-ranking or more junior individuals in the above categories.

AML Rule 5.1.4 AML Rule Guidance on Politically Exposed Persons	6.4	A Relevant Person should implement appropriate risk management systems to identify PEPs. Under-classification of PEPs poses a higher ML/TF risk to the Relevant Person whilst over-classification of PEPs leads to an unnecessary compliance burden to the Relevant Person and its customers.
	6.5	Relevant Persons should adopt an RBA to determine whether to apply the measures in section 6.8 below in respect of PEPs.
	6.6	While a Relevant Person may refer to commercially available databases to identify PEPs, the use of these databases should never replace traditional CDD processes (e.g. understanding the occupation and employer of a customer). When using commercially available databases, a Relevant Person should be aware of their limitations, for example, the databases are not necessarily comprehensive or reliable as they generally draw solely from information that is publicly available; the definition of PEPs used by the database providers may or may not align with the definition of PEPs applied by the Relevant Person; and any technical incapability of such databases that may hinder the Relevant Person's effectiveness of PEP identification. A Relevant Person using such databases as a support tool should ensure that they are fit for the purpose.
	6.7	Relevant Persons may use publicly available information or refer to relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations to assess which countries are most vulnerable to corruption (an example of which is Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption). Relevant Persons should be vigilant where either the country to which the customer has business connections or the business/industrial sector is more vulnerable to corruption.
		Special requirements and additional measures for PEPs
	6.8	When a Relevant Person knows that a customer or beneficial owner of a customer is a PEP, it should, before (i) establishing a business relationship or (ii) continuing an existing business relationship where the customer or the beneficial owner is subsequently found to be a PEP, apply all the following measures: (a) obtaining approval from its senior management for establishing or continuing such business relationship;

		(b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds; and (c) conducting enhanced ongoing monitoring on that business relationship (see Part 7).
	6.9	Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets). This information will usually give an indication as to the size of wealth the customer would be expected to have, and a picture of how the individual acquired such wealth. Although a Relevant Person may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources. Examples of information and documents which may be used to establish source of wealth include evidence of title, copies of trust deeds, audited financial statements, salary details, tax returns and bank statements.
	6.10	Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and the Relevant Person (e.g. the amounts being invested, deposited, or wired as part of the business relationship). Source of funds information should not simply be limited to knowing from where the funds may have been transferred, but also the activity that generates the funds. The information obtained should be substantive and establish a provenance or reason for the funds having been acquired (e.g. salary payments and investment sale proceeds).
	6.11	It is for a Relevant Person to decide which measures it deems reasonable, in accordance with its assessment of the risks, to establish the source of funds and source of wealth. In practical terms, this will often amount to obtaining information from the PEP and verifying it against publicly available information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. Relevant Persons should however note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. Relevant Persons should also be aware that some jurisdictions impose restrictions on their PEP's ability to hold foreign bank accounts or to hold other office or paid employment.
	6.12	Although the measures set out in section 6.8 also apply to family members and close associates of the PEP, the risks associated with them may vary depending to some extent on the social-economic and cultural structure of the jurisdiction of the PEP.
	6.13	Since not all PEPs pose the same level of ML/TF risks, a Relevant Person should adopt an RBA in determining the extent of measures in section 6.8 taking into account relevant factors, such as:

		(a) the prominent public functions that a PEP holds; (b) the geographical risk associated with the jurisdiction where a PEP holds prominent public functions; (c) the nature of the business relationship (e.g. the delivery/distribution channel used; or the product or service offered); or (d) the level of influence that a PEP may continue to exercise after stepping down from the prominent public function.
	6.14	International organisations referred to in section 6.3 under the term "PEP" are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the UN and affiliated international organisations such as the International Maritime Organization; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization; and economic organisations such as the World Trade Organization and the Association of Southeast Asian Nations; etc.
	6.15	According to FATF Recommendation 12 the handling of a person who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits. The risk based approach requires that financial institutions and DNFBPs assess the ML/TF risk of a PEP who is no longer entrusted with a prominent public function, and take effective action to mitigate this risk. Possible risk factors are: (1) the level of (informal) influence that the individual could still exercise; the seniority of the position that the individual held as a PEP; or (2) whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

Version	Date	Part 7	
AMLPG 001	15/04/2022	**Ongoing Monitoring**	s. 7.1 – 7.20
		▪ *General*	s. 7.1
		▪ *Keeping customer information up-to-date*	s. 7.2 – 7.3
		▪ *Transaction monitoring systems and processes*	s. 7.4 – 7.8
		▪ *Risk-based approach to monitoring*	s. 7.9 – 7.12
		▪ *Review of transactions*	s. 7.13 – 7.20

Subject	7	ONGOING MONITORING
		General
	7.1	Ongoing monitoring is an essential component of effective AML/CFT Systems. A Relevant Person must continuously monitor its business relationship with a customer by: (a) reviewing from time-to-time documents, data and information relating to the customer that have been obtained by the Relevant Person for the purpose of complying with the AML Rules to ensure that they are up- to-date and relevant; (b) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the Relevant Person's knowledge of the customer, the customer's business, risk profile and source of funds; and (c) identifying transactions that (i) are complex, unusually large in amount or of an unusual pattern; and

		(ii) have no apparent economic or lawful purpose and examining the background and purposes of those transactions and setting out the findings in writing.
		Keeping customer information up-to-date
	7.2	To ensure documents, data and information of a customer obtained are up-to-date and relevant, a Relevant Person should undertake reviews of existing CDD records of customers on a regular basis and/or upon trigger events. Clear policies and procedures should be developed, especially on the frequency of periodic review or what constitutes a trigger event.
	7.3	All customers that present high ML/TF risks should be subject to a minimum of an annual review, or more frequent reviews if deemed necessary by the Relevant Person, to ensure the CDD information retained remains up-to-date and relevant.
		Transaction monitoring systems and processes
	7.4	A Relevant Person should establish and maintain adequate systems and processes (e.g. the use of large transactions exception reports which help a Relevant Person to stay apprised of operational activities) to monitor transactions. The design, degree of automation and sophistication of transaction monitoring systems and processes should be developed appropriately having regard to the following factors: (a) the size and complexity of its business; (b) the ML/TF risks arising from its business; (c) the nature of its systems and controls; (d) the monitoring procedures that already exist to satisfy other business needs; and (e) the nature of the products and services provided (which includes the means of delivery or communication).
	7.5	A Relevant Person should ensure that the transaction monitoring systems and processes can provide all relevant staff who are tasked with conducting transaction monitoring and investigation with timely and sufficient information required to identify, analyse and effectively monitor customers' transactions.
	7.6	A Relevant Person should ensure that the transaction monitoring systems and processes can support the ongoing monitoring of a business relationship in a holistic approach, which may include monitoring activities of a customer's multiple

		accounts within or across lines of business, and related customers' accounts within or across lines of business. This means preferably the Relevant Person adopts a relationship-based approach rather than on a transaction-by-transaction basis.
	7.7	In designing transaction monitoring systems and processes, including (where applicable) setting of parameters and thresholds, a Relevant Person should take into account the transaction characteristics, which may include: (a) the nature and type of transactions (e.g. abnormal size or frequency); (b) the nature of a series of transactions (e.g. structuring a single transaction into a number of cash deposits); (c) the counterparties of transactions; (d) the geographical origin/destination of a payment or receipt; and (e) the customer's normal account activity or turnover.
	7.8	A Relevant Person should regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including (where applicable) parameters and thresholds adopted. The parameters and thresholds should be properly documented and independently validated to ensure that they are appropriate to its operations and context.
		Risk-based approach to monitoring
	7.9	Relevant Persons should conduct ongoing monitoring in relation to all business relationships following the RBA. The extent of monitoring (e.g. frequency and intensity of monitoring) should be commensurate with the ML/TF risk profile of the customer. Where the ML/TF risks are higher, the Relevant Person should conduct enhanced monitoring. In lower risk situations, the Relevant Person may reduce the extent of monitoring.
	7.10	Relevant Persons must take additional measures to compensate for any risk of ML/TF in monitoring business relationships involving (a) a customer not having been physically present for identification purposes; (b) a customer or a beneficial owner of a customer being a PEP.
	7.11	Relevant Persons should be vigilant for changes of the basis of the business relationship with the customer over time. These may include where: (a) new products or services that pose higher risk are entered into;

		(b) new corporate or trust structures are created; (c) the stated activity or turnover of a customer changes or increases; or (d) the nature of transactions changes or their volume or size increases, etc.
	7.12	Where the basis of the business relationship changes significantly, Relevant Persons should carry out further CDD procedures to ensure that the ML/TF risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures must take account of the above changes.
		Review of transactions
	7.13	A Relevant Person should take appropriate steps (e.g. examining the background and purposes of the transactions; making appropriate enquiries to or obtaining additional CDD information from a customer) to identify if there are any grounds for suspicion, when: (a) the customer's transactions are not consistent with the Relevant Person's knowledge of the customer, the customer's business, risk profile or source of funds; (b) the Relevant Person identifies transactions that (i) are complex, unusually large in amount or of an unusual pattern, and (ii) have no apparent economic or lawful purpose.
	7.14	Where the Relevant Person conducts enquiries and obtains what it considers to be a satisfactory explanation of the activity or transaction, it may conclude that there are no grounds for suspicion, and therefore take no further action. Even if no suspicion is identified, the Relevant Person should consider updating the customer risk profile based on any relevant information obtained.
	7.15	However, where the Relevant Person cannot obtain a satisfactory explanation of the transaction or activity, it may conclude that there are grounds for suspicion. In any event where there is any suspicion identified during transaction monitoring, an STR should be made to the FIU.
	7.16	A Relevant Person should be aware that making enquiries to customers, when conducted properly and in good faith, will not constitute tipping-off. However, if the Relevant Person reasonably believes that performing the CDD process will tip off

		the customer, it may stop pursuing the process. The Relevant Person should document the basis for its assessment and file an STR to the FIU.
	7.17	The findings and outcomes of steps taken by the Relevant Person in section 7.13, as well as the rationale of any decision made after taking these steps, should be properly documented in writing and be available to the AFSA, other competent authorities and auditors.
	7.18	Where cash transactions (including deposits and withdrawals) and third-party deposits and payments are being proposed by customers, and such requests are not in accordance with the customer's profile and normal commercial practices, Relevant Persons must approach such situations with caution and make relevant further enquiries.
	7.19	Ongoing monitoring of a customer's account involving cash, third-party deposits and payments should be enhanced. A Relevant Person should be alert to the red flags relating to cash and third-party transactions, having regard to the list of indicators of suspicious transactions and activities outlined in Annex 2.
	7.20	Where the Relevant Person has been unable to satisfy itself that any cash transaction or third-party deposit or payment is reasonable, and therefore considers it suspicious, it should make an STR to the FIU.

Version	Date	Part 8	
AMLPG 003	19/12/2024	**Terrorist Financing, Financial Sanctions and Proliferation Financing**	s. 8.1 – 8.12
		▪ *Terrorist financing (TF)*	s. 8.1 – 8.2
		▪ *Financial sanctions & proliferation financing*	s. 8.3
		▪ *Sanctions imposed by other jurisdictions*	s. 8.4
		▪ *Database maintenance, screening and enhanced checking*	s. 8.5 – 8.12

Subject	8	TERRORIST FINANCING, FINANCIAL SANCTIONS AND PROLIFERATION FINANCING
		Terrorist financing (TF)
	8.1	TF is the financing of terrorist acts, and of terrorists and terrorist organisations. It generally refers to the carrying out of transactions involving property owned by terrorists or terrorist organisations, or that has been, or is intended to be, used to assist the commission of terrorist acts. Different from ML, the focus of which is on the handling of criminal proceeds (i.e. the source of property is what matters), the focus of TF is on the destination or use of property, which may have derived from legitimate sources.
	8.2	The United Nations Security Council (UNSC) has passed UNSCR 1373 (2001), which calls on all member states to act to prevent and suppress the financing of terrorist acts. The UN has also published the names of individuals and organisations in relation to involvement with Al-Qa'ida, ISIL (Da'esh) and the Taliban under relevant UNSCRs (e.g. UNSCR 1267 (1999), 1988 (2011), 1989 (2011), 2253 (2015), 2368 (2017) and their successor resolutions). All UN member states are required to freeze any funds, or other financial assets, or economic resources of any person(s) named in these lists and to report any suspected name matches to the relevant authorities.
AML Rule 1.4 (e)		**Financial sanctions & proliferation financing**

	8.3	To combat PF, the UNSC adopts a two-tiered approach through resolutions made under Chapter VII of the UN Charter imposing mandatory obligations on UN member states: (a) global approach under UNSCR 1540 (2004) and its successor resolutions; and (b) country-specific approach under UNSCR 1718 (2006) against the Democratic People's Republic of Korea (DPRK) and UNSCR 2231 (2015) against the Islamic Republic of Iran (Iran) and their successor resolutions.
		Sanctions imposed by other jurisdictions
	8.4	A Relevant Person operating internationally will need to be aware of the scope and focus of relevant sanctions regimes in those jurisdictions. Where these sanctions regimes may affect their operations, Relevant Persons should consider what implications exist and take appropriate measures, such as including relevant overseas designations in its database for screening purpose, where applicable. Such regimes include unilateral sanctions imposed by the US (administered by Office of Foreign Assets Control (OFAC)), the European Union (EU), and United Kingdom (administered by His Majesty's Treasury Office of Financial Sanctions Implementation (HMT UK OFSI)).
		Database maintenance, screening and enhanced checking
	8.5	A Relevant Person should establish and maintain effective policies, procedures and controls to ensure compliance with the relevant regulations and legislation on TF, financial sanctions and PF. The legal and regulatory obligations of Relevant Persons and those of their staff should be well understood and adequate guidance and training should be provided to the latter.
	8.6	It is particularly vital that a Relevant Person should be able to identify terrorist suspects and possible designated parties, and detect prohibited transactions. To this end, a Relevant Person should ensure that it maintains a database of names and particulars of terrorists and designated parties which consolidates the various lists that have been made known to the Relevant Person. Alternatively, a Relevant Person may make arrangements to access to such a database maintained by FIU or third party service providers and take appropriate measures (e.g. conduct sample testing periodically) to ensure the completeness and accuracy of the database.
	8.7	Inclusion of a country, individual, entity or activity in the UNSCR or sanctions list may constitute grounds for knowledge or suspicion for the purposes of relevant ML, TF and PF laws, thereby triggering statutory (including reporting) obligations as well as offence provisions. The FIU draw to the attention to Relevant Persons from time to time whenever there are any updates to the UNSCRs or sanctions lists relating to terrorism, TF and PF promulgated by the UNSC. The Relevant Person

		should ensure that countries, individuals and entities included in UNSCRs and sanctions lists are included in the database as soon as practicable after they are promulgated by the UNSC and regardless of whether the relevant sanctions have been implemented by legislation in the Republic of Kazakhstan.
	8.8	A Relevant Person should include in its database (i) the lists published in the relevant sources or on the website of the FIU; (ii) the lists that the FIU draw to the attention of Relevant Persons from time to time; and (iii) any relevant designations by national/overseas authorities which may affect its operations. The database should be subject to timely update whenever there are changes and should be made easily accessible by relevant staff.
	8.9	To avoid establishing business relationship or conducting transactions with any terrorist suspects and possible designated parties, a Relevant Person should implement an effective screening mechanism, which should include: (a) screening its customers and any beneficial owners of the customers against current database at the establishment of the relationship; (b) screening its customers and any beneficial owners of the customers against all new and any updated designations to the database as soon as practicable; and (c) screening all relevant parties in a cross-border wire transfer against current database before executing the transfer.
	8.10	The screening requirements set out in section 8.9 (a) and (b) should extend to other connected parties as defined in section 5.39 (persons acting on behalf of a customer) using an RBA.
	8.11	When possible, name matches are identified during screening, a Relevant Person should conduct enhanced checks to determine whether the possible matches are genuine hits. In case of any suspicions of TF, PF or sanction violations, the Relevant Person should make a report to the FIU. Records of enhanced checking results, together with all screening records, should be documented, or recorded electronically.
	8.12	The Relevant Person is reminded that the ultimate responsibility for ensuring compliance with the relevant regulations and legislation on TF, financial sanctions and PF remains with the Relevant Person.

Version	Date	Part 9	
AMLPG 003	19/12/2024	**Suspicious Transaction Reports, Threshold Transaction Reports and Law Enforcement Requests**	s. 9.1 – 9.35
		▪ *General issues*	s. 9.1
		▪ *Knowledge vs. suspicion*	s. 9.2 – 9.5
		▪ *Tipping-off*	s. 9.6
		▪ *AML/CFT Systems in relation to suspicious transaction reporting and threshold transaction reporting*	s. 9.7 – 9.8
		▪ *Money laundering reporting officer*	s. 9.9
		▪ *Identifying suspicious transactions*	s. 9.10 – 9.11
		▪ *Internal reporting*	s. 9.12 – 9.18
		▪ *Reporting to the FIU*	s. 9.19 – 9.23
		▪ *Post reporting matters*	s. 9.24 – 9.28
		▪ *Record-keeping*	s. 9.29 – 9.30
		▪ *Requests from law enforcement agencies*	s. 9.31 – 9.35

Subject	9	SUSPICIOUS TRANSACTION REPORTS, THRESHOLD TRANSACTION REPORTS AND LAW ENFORCEMENT REQUESTS
		General issues

AML Rule 13.7.5 AML Rule 13.8 AML Law	9.1	It is a statutory obligation under the AML Law and the AML Rules, that where a Relevant Person knows or suspects that any property, in whole or in part, directly or indirectly, represents any person's proceeds of, was used in connection with, or is intended to be used in connection with any indictable offence, or that any property is terrorist property, the Relevant Person shall, within a time frame specified by AML Law, file an STR with the FIU. The STR should be made together with any matter on which the knowledge or suspicion is based.
		Knowledge vs. suspicion
	9.2	Generally speaking, knowledge is likely to include: (a) actual knowledge; (b) knowledge of circumstances which would indicate facts to a reasonable person; and (c) knowledge of circumstances which would put a reasonable person on inquiry.
	9.3	Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence. As far as a Relevant Person is concerned, when a transaction or a series of transactions of a customer is not consistent with the Relevant Person's knowledge of the customer, or is unusual (e.g. in a pattern that has no apparent economic or lawful purpose, or by unnecessary routing of funds through third party accounts), the Relevant Person should take appropriate steps to further examine the transactions and identify if there is any suspicion (see sections 7.13 to 7.20). Unnecessary routing of funds through third party accounts means routing without clear economic (business) reasoning.
	9.4	For a Relevant Person to have knowledge or suspicion, he does not need to know the nature of the criminal activity underlying the ML, or that the funds themselves definitely arose from the criminal offence. Similarly, the same principle applies to TF.
	9.5	Once knowledge or suspicion has been formed, (a) a Relevant Person should file an STR even where no transaction has been conducted by or through the Relevant Person; and (b) the STR must be made within a time frame specified by the AML Law after the suspicion was first identified.

		Tipping-off
AML Rule 13.8.3 Guidance on tipping-off	9.6	It is an offence ("tipping-off") to reveal to any person any information which might prejudice an investigation; if a customer is told that a report has been made, this would prejudice the investigation and an offence would be committed. The tipping-off provision includes circumstances where a suspicion has been raised internally within a Relevant Person, but has not yet been reported to the FIU.
		AML/CFT Systems in relation to transaction reporting
	9.7	A Relevant Person should implement appropriate AML/CFT Systems in order to fulfil its statutory reporting obligation, and properly manage and mitigate the risks associated with any customer or transaction involved in an STR or threshold transactions report ("TTR"). The AML/CFT Systems should include: (a) appointment of an MLRO (see Part 4); (b) implementing clear policies and procedures over internal reporting, reporting to the FIU, post- reporting risk mitigation and prevention of tipping-off; and (c) keeping proper records of internal reports and STRs.
	9.8	The Relevant Person should have measures in place to check, on an ongoing basis, that its AML/CFT Systems in relation to suspicious transaction reporting comply with relevant legal and regulatory requirements and operate effectively. The type and extent of the measures to be taken should be appropriate having regard to the risk of ML/TF as well as the nature and size of the business. The policies, procedures, systems and controls to monitor and detect transactions above defined thresholds, and submission of TTRs to the FIU should be performed in accordance with the National AML Law.
		Money laundering reporting officer
	9.9	A Relevant Person should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the FIU and law enforcement agencies. The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions of the MLRO should include having oversight of: (a) review of internal disclosures and exception reports and, in light of all available relevant information, determination of whether or not it is necessary to make a report to the FIU;

		(b) maintenance of all records related to such internal reviews; and (c) provision of guidance on how to avoid tipping-off. To fulfil these functions, all Relevant Persons must ensure that the MLRO receives full co-operation from all staff and full access to all relevant documentation so that he is in a position to decide whether attempted or actual ML/TF is suspected or known. Principal functions expected from a MLRO are outlined in Annex 5.
		Identifying suspicious transactions
	9.10	A Relevant Person should provide sufficient guidance to its staff to enable them to form suspicion or to recognise the signs when ML/TF is taking place. The guidance should take into account the nature of the transactions and customer instructions that staff is likely to encounter, the type of product or service and the means of delivery.
	9.11	A Relevant Person should have reasonable policies and procedures to identify and analyse relevant red flags of suspicious activities for its customer accounts. A list of non-exhaustive indicators of suspicious transactions and activities is provided in Annex 2 to assist a Relevant Person in determining what types of red flags are relevant to its businesses, taking into account the nature of customer transactions, risk profile of the customers and business relationships. The list is intended solely to provide an aid to Relevant Persons and must not be applied by Relevant Persons as a routine instrument without analysis or context. The detection of any relevant red flag by a Relevant Person however should prompt further investigations and be a catalyst towards making at least initial enquiries about the source of funds. Relevant Persons should also be aware of elements of individual transactions and situations that might give rise to suspicion of TF in certain circumstances. The FATF publishes studies of methods and trends of TF from time to time, and Relevant Persons may refer to the FATF website for additional information and guidance.
		Internal reporting
	9.12	A Relevant Person should establish and maintain clear policies and procedures to ensure that: (a) all staff are made aware of the identity of the MLRO and of the procedures to follow when making an internal report; and

		(b) all internal reports must reach the MLRO without undue delay.
	9.13	While Relevant Persons may wish to set up internal systems that allow staff to consult with supervisors or managers before sending a report to the MLRO, under no circumstances should reports raised by staff be filtered out by supervisors or managers who have no responsibility for the money laundering reporting/compliance function. The legal obligation is to report within a time frame specified by the AML Law, so reporting lines should be as short as possible with the minimum number of people between the staff with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO.
	9.14	Once a staff member of a Relevant Person has reported suspicion to the MLRO in accordance with the policies and procedures established by the Relevant Person for the making of such reports, the statutory obligation of the staff member has been fully satisfied.
	9.15	The internal report should include sufficient details of the customer concerned and the information giving rise to the suspicion.
	9.16	The MLRO should acknowledge receipt of an internal report and provide a reminder of the obligation regarding tipping-off to the reporting staff member upon internal reporting.
	9.17	When evaluating an internal report, the MLRO must take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the Relevant Person concerning the customers to which the report relates. This may include: (a) a review of other transaction patterns and volumes through connected accounts, preferably adopting a relationship-based approach rather than on a transaction-by- transaction basis; (b) making reference to any previous patterns of instructions, the length of the business relationship and CDD and ongoing monitoring information and documentation; and (c) appropriate questioning of the customer per the systematic approach to identify suspicious transactions recommended by the FIU.
	9.18	The need to search for information concerning connected accounts or relationships should strike an appropriate balance between the statutory requirement to make a timely STR to the FIU and any delays that might arise in searching for more

		relevant information concerning connected accounts or relationships. The review process should be documented, together with any conclusions drawn.
		Reporting to the FIU
	9.19	If after completing the review of the internal report, the MLRO decides that there are grounds for knowledge or suspicion, he should disclose the information to the FIU within a time frame specified by the AML Law after his evaluation is complete together with the information on which that knowledge or suspicion is based. Dependent on when knowledge or suspicion arises, an STR may be made either before a suspicious transaction or activity occurs (whether the intended transaction ultimately takes place or not), or after a transaction or activity has been completed.
	9.20	Providing an MLRO acts in good faith in deciding not to file an STR with the FIU, it is unlikely that there will be any criminal liability for failing to report if the MLRO concludes that there is no suspicion after taking into account all available information. It is however vital for the MLRO to keep proper records of the deliberations and actions taken to demonstrate he has acted in reasonable manner.
	9.21	In the event that an urgent reporting is required (e.g. where a customer has instructed the Relevant Person to move funds or other property, close the account, make cash available for collection, or carry out significant changes to the business relationship, etc.), particularly when the account is part of an ongoing law enforcement investigation, a Relevant Person should indicate this in the STR.
	9.22	A Relevant Person is recommended to indicate any intention to terminate a business relationship in its initial disclosure to the FIU, thereby allowing the FIU to comment, at an early stage, on such a course of action.
	9.23	A Relevant Person should ensure STRs filed with the FIU are of high quality taking into account feedback and guidance provided by the FIU from time to time.
		Post reporting matters
	9.24	The FIU will acknowledge receipt of an STR made by a Relevant Person under the AML Law. If there is no need for imminent action, e.g. the issue of a restraint order on an account, consent will usually be given for the institution to operate the account within the time frame specified by AML Law. The FIU may, on occasion, seek additional information or clarification with a

		Relevant Person of any matter on which the knowledge or suspicion is based. If a no-consent letter is issued by the FIU, the Relevant Person should act according to the content of the letter and seek legal advice where necessary.
	9.25	Filing a report to the FIU provides Relevant Persons with a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report, provided: (a) the report is made before the Relevant Person undertakes the disclosed acts and the acts (transaction(s)) are undertaken with the consent of the FIU; or (b) the report is made after the Relevant Person has performed the disclosed acts (transaction(s)) and the report is made on the Relevant Person's own initiative and within a time frame specified by the AML Law.
	9.26	However, the statutory defence stated in section 9.25 does not absolve a Relevant Person from the legal, reputational or regulatory risks associated with the account's continued operation. A Relevant Person should also be aware that a "consent" response from the FIU should not be construed as a "clean bill of health" for the continued operation of the account or an indication that the account does not pose a risk to the Relevant Person.
	9.27	A Relevant Person should conduct an appropriate review of a business relationship upon the filing of an STR to the FIU, irrespective of any subsequent feedback provided by the FIU, and apply appropriate risk mitigating measures. Filing a report with the FIU and continuing to operate the relationship without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified is not acceptable. If necessary, the issue should be escalated to the Relevant Person's senior management to determine how to handle the relationship concerned to mitigate any potential legal or reputational risks posed by the relationship in line with the Relevant Person's business objectives, and its capacity to mitigate the risks identified.
	9.28	A Relevant Person should be aware that the reporting of a suspicion in respect of a transaction or event does not remove the need to report further suspicious transactions or events in respect of the same customer. Further suspicious transactions or events, whether of the same nature or different to the previous suspicion, must continue to be reported to the MLRO who should make further reports to the FIU if appropriate.
		Record-keeping
	9.29	A Relevant Person must establish and maintain a record of all ML/TF reports made to the MLRO. The record should include details of the date the report was made, the staff members subsequently handling the report, the results of the assessment,

		whether the internal report resulted in an STR to the FIU, and information to allow the papers relevant to the report to be located.
	9.30	A Relevant Person must establish and maintain a record of all STRs made to the FIU. The record should include details of the date of the STR, the person who made the STR, and information to allow the papers relevant to the STR to be located. This register may be combined with the register of internal reports, if considered appropriate. A Relevant Person must establish and maintain a record of all TTRs made to the FIU.
		Requests from law enforcement agencies
	9.31	A Relevant Person may receive various requests from law enforcement agencies, e.g. search warrants, production orders, restraint orders or confiscation orders, pursuant to relevant legislation in the Republic of Kazakhstan. These requests are crucial to aid law enforcement agencies, to carry out investigations as well as restrain and confiscate illicit proceeds. Therefore, a Relevant Person should establish clear policies and procedures to handle these requests in an effective and timely manner, including allocation of sufficient resources. A Relevant Person should appoint a staff member as the main point of contact with law enforcement agencies.
	9.32	A Relevant Person should respond to any search warrant and production order within the required time limit by providing all information or materials that fall within the scope of the request. Where a Relevant Person encounters difficulty in complying with the timeframes stipulated, the Relevant Person should at the earliest opportunity contact the officer-in-charge of the investigation for further guidance.
	9.33	During a law enforcement investigation, a Relevant Person may be served with a restraint order which prohibits the dealing with particular funds or property pending the outcome of an investigation. A Relevant Person must ensure that it is able to freeze the relevant property that is the subject of the order.
	9.34	Upon the conviction of a defendant, a court may order the confiscation of his criminal proceeds and a Relevant Person may be served with a confiscation order in the event that it holds funds or other property belonging to that defendant that are deemed by the Courts to represent his benefit from the crime. A court may also order the forfeiture of property where it is satisfied that the property is terrorist property.

	9.35	When a Relevant Person receives a request from a law enforcement agency, e.g. search warrant or production order, in relation to a particular customer or business relationship, the Relevant Person should assess the risk involved and the need to conduct an appropriate review on the customer or the business relationship to determine whether there is any suspicion, and should also be aware that the customer subject to the request can be a victim of crime.

Version	Date	Part 10	
AMLPG 001	15/04/2022	**Record – Keeping**	s. 10.1 – 10.10
		▪ *General*	s. 10.1 – 10.2
		▪ *Retention of records relating to CDD and transactions*	s. 10.3 – 10.7
		▪ *Records kept by third parties*	s. 10.8 – 10.10

Subject	10	RECORD – KEEPING
		General
	10.1	Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record- keeping helps the investigating authorities to establish a financial profile of a suspect, trace the criminal or terrorist property or funds and assists the Court to examine all relevant past transactions to assess whether the property or funds are the proceeds of or relate to criminal or terrorist offences.
	10.2	A Relevant Person should maintain CDD information, transaction records and other records that are necessary and sufficient to meet the record-keeping requirements under the AML Rules, this Guidance and other regulatory requirements, that are appropriate to the nature, size and complexity of its businesses. The Relevant Person should ensure that: (a) the audit trail for funds moving through the Relevant Person that relate to any customer and, where appropriate, the beneficial owner of the customer, account or transaction is clear and complete; (b) all CDD information and transaction records are available swiftly to the AFSA, other authorities and auditors upon appropriate authority; and (c) it can demonstrate compliance with any relevant requirements specified in other sections of this Guidance and other Guidance issued by the AFSA.

		Retention of records relating to CDD and transactions
	10.3	A Relevant Person should keep: (a) the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and where applicable, verifying the identity of the customer and/or beneficial owner of the customer and/or beneficiary and/or persons who purport to act on behalf of the customer and/or other connected parties to the customer; (b) other documents and records obtained throughout the CDD and ongoing monitoring process, including SDD, additional due diligence measures and other requirements for cross-border correspondent relationships, and when taking simplified and enhanced measures; (c) where applicable, the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship; (d) the original or a copy of the records and documents relating to the customer's account (e.g. account opening form; risk assessment form) and business correspondence with the customer and any beneficial owner of the customer (which at a minimum should include business correspondence material to CDD measures or significant changes to the operation of the account); and (e) the results of any analysis undertaken (e.g. inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose).
	10.4	All documents and records mentioned in section 10.3 should be kept throughout the continuance of the business relationship with the customer and for a period of at least six years after the end of the business relationship. Similarly, for occasional transaction equal to or exceeding the CDD thresholds, a Relevant Person should keep all documents and records mentioned in section 10.3 for a period of at least six years after the date of the occasional transaction.
	10.5	Relevant Persons should maintain the original or a copy of the documents, and a record of the data and information, obtained in connection with each transaction the Relevant Person carries out, both domestic and international, which should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

	10.6	All documents and records mentioned in section 10.5 should be kept for a period of at least six years after the completion of a transaction, regardless of whether the business relationship ends during the period.
	10.7	The AFSA may, by notice in writing to a Relevant Person, require it to keep the records relating to a specified transaction or customer for a period specified by the AFSA that is longer than those referred to in sections 10.4 and 10.6, where the records are relevant to an ongoing criminal or other investigation, or to any other purposes as specified in the notice.
		Records kept by third parties
	10.8	Where customer identification and verification documents are held by a third party on which the Relevant Person is relying to carry out CDD measures, a Relevant Person concerned remains responsible for compliance with all record-keeping requirements. The Relevant Person should ensure that the third party being relied on has systems in place to comply with all the record- keeping requirements under the AML Law and AML Rules, and that documents and records will be provided by the third party as soon as reasonably practicable after the third party receives the request from the Relevant Person.
	10.9	For the avoidance of doubt, a Relevant Person that relies on a third party for carrying out a CDD measure should immediately obtain the data or information that the third party has obtained in the course of carrying out that measure.
	10.10	A Relevant Person should ensure that a third party will pass the documents and records to the Relevant Person, upon termination of the services provided by the third party.

Version	Date	Part 11	
AMLPG 001	15/04/2022	**Staff Training**	s. 11.1 – 11.8

Subject	11	STAFF TRAINING
	11.1	Ongoing staff training is an important element of an effective system to prevent and detect ML/TF activities. The effective implementation of even a well-designed internal control system can be compromised if staff using the system is not adequately trained.
	11.2	It is a Relevant Person's responsibility to provide adequate training for its staff so that they are adequately trained to implement its AML/CFT Systems. The scope and frequency of training should be tailored to the specific risks faced by the Relevant Person and pitched according to the job functions, responsibilities and experience of the staff. New staff should be required to attend initial training as soon as possible after being hired or appointed. Apart from the initial training, a Relevant Person should also provide refresher training regularly to ensure that its staff are reminded of their responsibilities and are kept informed of new developments related to ML/TF.
	11.3	A Relevant Person should implement a clear and well articulated policy for ensuring that relevant staff receive adequate AML/CFT training.
	11.4	Staff should be made aware of, but not limited to: (a) their Relevant Person's and their own personal statutory obligations and the possible consequences for failure to comply with CDD and record-keeping requirements under the AML Rules; (b) their Relevant Person's and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the AML Law; (c) any other statutory and regulatory obligations that concern their Relevant Persons and themselves under the AML Law and the AML Rules, and the possible consequences of breaches of these obligations;

		(d) the Relevant Person's policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting; and (e) any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by the staff to carry out their particular roles in the Relevant Person with respect to AML/CFT.
	11.5	In addition, the following areas of training may be appropriate for certain groups of staff: (a) all new staff, irrespective of seniority: (i) an introduction to the background to ML/TF and the importance placed on ML/TF by the Relevant Person; and (ii) the need for identifying and reporting of any suspicious transactions to the MLRO, and the offence of tipping-off; (b) front-line personnel who are dealing directly with the public: (i) the importance of their roles in the Relevant Person's ML/TF strategy, as the first point of contact with potential money launderers; (ii) the Relevant Person's policies and procedures in relation to CDD and record-keeping requirements that are relevant to their job responsibilities; and (iii) training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required; (c) back-office staff, depending on their roles: (i) appropriate training on customer verification and relevant processing procedures; and (ii) how to recognise unusual activities including abnormal settlements, payments or delivery instructions; (d) managerial staff including internal audit officers and COs: (i) higher level training covering all aspects of the Relevant Person's AML/CFT regime; and (ii) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as reporting of suspicious transactions to the FIU; and (e) MLROs:

		(i) specific training in relation to their responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the FIU; and (ii) training to keep abreast of AML/CFT requirements/developments generally.
	11.6	A Relevant Person is encouraged to consider using a mix of training techniques and tools in delivering training, depending on the available resources and learning needs of their staff. These techniques and tools may include on-line learning systems, focused classroom training, relevant videos as well as paper- or intranet- based procedures manuals. A Relevant Person may consider including available FATF papers and typologies as part of the training materials. The Relevant Person should be able to demonstrate to the AFSA that all materials should be up-to-date and in line with current requirements and standards.
AML Rule 14.5.5	11.7	No matter which training approach is adopted, a Relevant Person should maintain records of who have been trained, when the staff received the training and the type of the training provided. Records should be maintained for a minimum of 3 years.
	11.8	A Relevant Person should monitor the effectiveness of the training. This may be achieved by: (a) testing staff's understanding of the Relevant Person's policies and procedures to combat ML/TF, the understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions; (b) monitoring the compliance of staff with the Relevant Person's AML/CFT Systems as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken; and (c) monitoring attendance and following up with staff who miss such training without reasonable cause.

Version	Date	Part 12	
AMLPG 001	15/04/2022	**Third – Party Deposits and Payments**	s. 12.1 – 12.10
		▪ *General*	s. 12.1 – 12.2
		▪ *Policies and procedures*	s. 12.3 – 12.4
		▪ *Due diligence process for assessing third-party deposits and payments*	s. 12.5 – 12.8
		▪ *Delayed due diligence on the source of a deposit or evaluation of a third-party deposit*	s. 12.9 – 12.10

Subject	12	THIRD – PARTY DEPOSITS AND PAYMENTS
		General
	12.1	When a customer uses a third party (any person other than the customer) to pay for or receive the proceeds of investment, there is a risk that the arrangement may be used to disguise the true beneficial owner or the source of funds. There are increased risks that these investment transactions are linked to predicate offences in securities markets (such as insider dealing and market manipulation) or used to launder illicit proceeds obtained elsewhere.
	12.2	A Relevant Person must take all reasonable measures to mitigate the ML/TF risks associated with transactions involving third-party deposits and payments.
		Policies and procedures
	12.3	Third-party deposits or payments should be accepted only under exceptional and legitimate circumstances and when they are reasonably in line with the customer's profile and normal commercial practices.

		Before a Relevant Person accepts any third-party deposit or payment arrangement, it should ensure that adequate policies and procedures are put in place to mitigate the inherently high risk and meet all applicable legal and regulatory requirements. These policies and procedures should be approved by senior management and address, among others: (a) the exceptional and legitimate circumstances under which third-party deposits or payments may be accepted and their evaluation criteria; (b) the monitoring systems and controls for identifying transactions involving third-party deposits; (c) if applicable, the due diligence process for assessing whether third-party deposits or payments meet the evaluation criteria for acceptance; (d) if a Relevant Person allows the due diligence on the source of a deposit or the evaluation of a third-party deposit to be completed after settling transactions with the deposited funds (please refer to sections 12.9 and 12.10) in exceptional situations, the identification of those exceptional situations and the risk management policies and procedures concerning the conditions under which such delayed due diligence or evaluation may be allowed; (e) the enhanced monitoring of client accounts involving third-party deposits or payments, and the reporting of any ML/TF suspicions identified to the FIU; and (f) the respective designated managers or staff members responsible for carrying out these policies and procedures. A MLRO, CO or other appropriate senior management personnel should be designated to oversee the proper design and implementation of these policies and procedures.
	12.4	To facilitate the prompt identification of the sources of deposits, Relevant Persons are strongly encouraged to require their clients to designate bank accounts held in their own names or the names of any acceptable third parties for the making of all deposits. This will make it easier for Relevant Persons to ascertain whether deposits have originated from their clients or any acceptable third parties.
		Due diligence process for assessing third-party deposits and payments
	12.5	Due diligence process for assessing third-party deposits and payments should include:

		(a) critically evaluating the reasons and the need for third-party deposits or payments; (b) taking reasonable measures on a risk-sensitive basis to: (i) verify the identities of the third parties; and (ii) ascertain the relationship between the third parties and the customers; (c) obtaining the approval of the member of senior management with a relevant role at the Relevant Person with respect to AML/CFT, or MLRO (hereafter referred to as "third-party deposit or payment approvers") for the acceptance for a third-party deposit or payment; and (d) documenting the findings of inquiries made and corroborative evidence obtained during the due diligence process as well as the approval of a third-party deposit or payment.
	12.6	While a standing approval may be given by third-party deposit or payment approvers for accepting deposits or payments from or to a particular third party after assessing the risks and reasonableness of the third-party arrangement, the standing approval should be subject to review periodically or upon trigger events to ensure that it remains appropriate.
	12.7	Given that not all third-party payors and payees pose the same level of ML/TF risk, a Relevant Person should apply enhanced scrutiny to those third parties which might pose higher risks, and require the dual approval of deposits or payments from or to such third parties by the third-party deposit or payment approvers for enhanced control.
	12.8	A Relevant Person should exercise extra caution when the relationship between the customer and the third party is hard to verify, the customer is unable to provide details of the identity of the third-party payor for verification before the deposit is made, or one third party is making or receiving payments for or from several seemingly unrelated customers.
		Delayed due diligence on the source of a deposit or evaluation of a third-party deposit
	12.9	If a Relevant Person allows third-party deposit due diligence to be delayed in exceptional situations, it should adopt appropriate risk management policies and procedures setting out the conditions under which the customer may utilise the deposited funds prior to the completion of the third-party deposit due diligence. These policies and procedures should include: (a) establishing a reasonable timeframe for the completion of the third-party deposit due diligence, and the follow-up actions if the stipulated timeframe is exceeded (e.g. to suspend or terminate the business relationship);

		(b) placing appropriate limits on the number, types, and/or amount of transactions that can be performed; (c) performing enhanced monitoring of transactions carried out by or for the customer; and (d) ensuring senior management is periodically informed of all cases involving delay in completing third-party deposit due diligence.
	12.10	If the third-party deposit due diligence cannot be completed within the reasonable timeframe set out in the Relevant Person's risk management policies and procedures, the Relevant Person should refrain from carrying out further transactions for the customer. The Relevant Person should assess whether there are grounds for knowledge or suspicion of ML/TF and filing an STR to the FIU, particularly where the customer refuses without reasonable explanation to provide information or document requested by the Relevant Person, or otherwise refuses to cooperate with the third-party deposit due diligence process.

ANNEX 1

RISK INDICATORS FOR ASSESSING ML/TF RISKS

The following is a list of non-exhaustive illustrative risk indicators for business risk assessment and customer risk assessment. These examples of indicators associated with each risk factor mentioned in sections 3.8 and 3.20 may indicate higher or lower ML/TF risks as the case may be.

Country risk	1	Examples of countries or jurisdictions that may present higher ML/TF risk include: (a) countries or jurisdictions that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies; (b) countries or jurisdictions subject to sanctions, embargos or similar measures issued by, for example, the UN; (c) countries or jurisdictions which are more vulnerable to corruption; and (d) countries or jurisdictions that are believed to have strong links to terrorist activities. Examples of countries or jurisdictions that may be considered to carry lower ML/TF risk include: (a) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems; and (b) countries or jurisdictions identified by credible sources as having a low level of corruption or other criminal activity.
Customer risk	2	Examples of customers that may present higher ML/TF risk include: (a) the business relationships established in unusual circumstances (e.g. a customer instructs a Relevant Person to set up a discretionary management agreement for an investment vehicle owned by the customer but requests the Relevant Person to buy and sell particular securities for the investment vehicle only according to the customer's instructions); (b) non-resident customers who have no discernible reasons for opening an account with Relevant Persons in the Republic of Kazakhstan (AIFC); (c) the use of legal persons or arrangements as personal asset-holding vehicles without any commercial or other valid reasons; (d) companies that have nominee shareholders or shares in bearer form;

		(e) customers that engage in, or derive wealth or revenues from, cash-intensive businesses; (f) the ownership structure of a company appears unusual or excessively complex having considered the nature of the company's business; (g) the customer or the family member or close associate of a customer is a PEP (including where a beneficial owner of a customer is a PEP); (h) customers that have been mentioned in negative news reports from credible media, particularly those related to predicate offences for ML/TF or financial crimes; (i) nature, scope and location of business activities generating the funds may be related to high risk activities or jurisdictions posing a higher risk; (j) customers that have sanction exposure; (k) where the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified; and (l) a customer introduced by an overseas financial institution, affiliate or other investor, both of which are based in jurisdictions posing a higher risk; (m) the activity or transactions of the customer does not correspond the customer risk profile. Examples of customers that may be considered to carry lower ML/TF risk include: (a) specific types of customers that may be eligible for SDD as specified in section 5.59; (b) customers who are employment-based or with a regular source of income from a known legitimate source which supports the activity being undertaken; and (c) the reputation of the customer, e.g. a well-known, reputable private company, with a long history that is well documented by independent sources, including information regarding its ownership and control.
Product/service/ transaction risk	3	Examples of products, services or transactions that may present higher ML/TF risk include: (a) products or services that may inherently favour anonymity or obscure information about underlying customer transactions; (b) products that have the ability to pool underlying customers/funds;

		(c) deposits from or payments to unknown or unrelated third parties; (d) the products or services offered to customers associated with jurisdictions posing a higher risk (e.g. where a customer resides in a jurisdiction posing a higher risk or where the customer's source of funds or source of wealth is mainly derived from jurisdictions posing a higher risk); (e) products with unusual complexity or structure and with no obvious economic purpose; (f) products or services that permit the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly from jurisdictions posing a higher risk; (g) use of new technologies or payment methods not used in the normal course of business by the Relevant Person; (h) the purchase of securities using physical cash; and (i) securities-related products or services funded by payments from or instructions given by unexpected third parties, particularly from jurisdictions posing a higher risk.
Delivery/distribution channel risk	4	Examples of delivery/distribution channels that may present higher ML/TF risk include: (a) business relationships established using a non-face-to- face approach or transactions conducted by customer through non-face-to-face channels, where increased risks (e.g. impersonation or identity fraud) could not be adequately mitigated and/or are more susceptible to risk situations such as unauthorised trading and related ML/TF abuse; and (b) products or services distributed or sold through intermediaries (i.e. business relationship between a Relevant Person and the end customer may become indirect), especially if the intermediaries are: (i) suspected of criminal activities, particularly financial crimes or association with criminal associates; (ii) located in a higher risk country or in a country with a weak AML/CFT regime; (iii) serving high risk customers without appropriate risk mitigating measures; or (iv) with a history of non-compliance with laws or regulation or that have been the subject of relevant negative attention from credible media or law enforcement. Examples of delivery/distribution channels that may be considered to carry lower ML/TF risk include:

		(a) business relationships established or transactions conducted by customers through channels that are less susceptible to risk situations such as unauthorised trading and related ML/TF abuse; and (b) products or services distributed or sold directly to the customer.

ANNEX 2

INDICATORS OF SUSPICIOUS TRANSACTIONS AND ACTIVITIES

The following is a list of non-exhaustive indicators of suspicious transactions and activities that, along with the FIU's list set out in its regulation, may help assess whether or not transactions and activities might give rise to grounds of ML/TF suspicion.

Customer-related	1	(a) A customer who has no discernible reason for using the Relevant Person's services (e.g. a customer has opened an account for discretionary management services but directs the Relevant Person to carry out his own investment decisions or a customer located in a place outside the Republic of Kazakhstan who uses local accounts to trade on stock or futures exchanges located in that place); (b) A customer who has requested, without reasonable explanation, transactions that are out of the ordinary range of services normally requested, or are outside the experience of the financial services business in relation to the particular customer; (c) Extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services; (d) A legal person customer with bearer shares constituting a large part of its issued capital; (e) A customer who has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason; (f) A customer's legal or mailing address is associated with other apparently unrelated accounts; or does not seem connected to the customer; (g) The source of the funds is unclear or not consistent with the customers' profile and apparent standing; (h) Customer, who is a public official, opens account in the name of a family member who begins making large deposits not consistent with the known sources of legitimate family income; (i) Customer, who is a student, uncharacteristically transfers or exchanges large sums of money; (j) Account shows high velocity in the movement of funds, but maintains low beginning and ending daily balances; (k) Transaction involves unfamiliar countries or islands that are hard to find on an atlas or map; (l) Agent, attorney or financial advisor acts for another person without proper documentation, such as a power of attorney;

		(m) A customer who refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process; (n) A customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation; (o) A customer who exhibits unusual concern with the Relevant Person's AML/CFT Systems including policies, controls, record-keeping, monitoring or reporting thresholds; (p) Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance; (q) A customer who does not exhibit any concern with the cost of transactions or fees; and (r) A customer who is known to have criminal, civil or regulatory proceedings against it for corruption, misuse of public funds, other financial crimes or regulatory non- compliance, or is known to associate with such persons.
Employee-related	2	(a) Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays without reasonable cause; (b) Unusual or unexpected increase in the sales performance of an employee; (c) The employee's supporting documentation for customers' accounts or orders is incomplete or missing; (d) Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the bank requires; (e) The use of an address which is not the customer's home or office address, e.g. utilisation of an employee's address for the dispatch of customer documentation or correspondence; (f) Employee frequently overrides internal controls or established approval authority or circumvents policy; (g) Employee assists transactions where the identity of the ultimate beneficiary or counter party is undisclosed; (h) Employee avoids taking periodic vacations.
Unusual cash transactions	3	(a) Customer makes large cash deposit without having counted the cash; (b) Customer frequently exchanges small bills for large bills; (c) Customer's cash deposits often contain counterfeit bills or musty or extremely dirty bills;

		(d) Customer comes in with another customer and they go to different tellers to conduct currency transactions under the reporting threshold; (e) Customer makes large cash deposit containing many larger denomination bills; (f) Customer opens several accounts in one or more names, and then makes several cash deposits under the reporting threshold; (g) Customer withdraws cash in amounts under the reporting threshold; (h) Customer withdraws cash from one of his or her accounts and deposits the cash into another account the customer owns; (i) Customer makes frequent deposits or withdrawals of large amounts of currency for no apparent business reason or for a business that generally does not generate large amounts of cash; (j) Customer conducts large cash transactions at different branches on the same day, or coordinates others to do so on his or her behalf; (k) Customer deposits cash into several accounts in amounts below the reporting threshold and then consolidates the funds into one account and wire transfers them abroad; (l) Customer attempts to take back a portion of a cash deposit that exceeds the reporting threshold after learning that a currency transaction report will be filed; (m) Customer makes frequent purchases of monetary instruments with cash in amounts less than the reporting threshold; (n) Customer conducts an unusual number of foreign currency exchange transactions; (o) Customer indulges in foreign exchange transactions/currency swaps without caring about the margins; (p) Noncustomer deposits cash into a customer account, which was subsequently withdrawn in a different geographic location.
Unusual wire transfer transactions	4	(a) Wire transfers are sent or received from the same person to or from different accounts; (b) Nonaccount holder sends wire transfer with funds that include numerous monetary instruments, each in an amount under the reporting threshold;

		(c) An incoming wire transfer has instructions to convert the funds to cashier's checks and to mail them to a nonaccount holder; (d) Wire transfer activity to and from secrecy havens or higher risk geographic locations without apparent business reason or is inconsistent with a customer's transaction history; (e) An incoming wire transfer, followed by an immediate purchase by the beneficiary of monetary instruments for payment to another party; (f) An increase in international wire transfer activity in an account with no history of such activity or where the stated business of the customer does not warrant it; (g) Customer frequently shifts purported international profits by wire transfer out of the country; (h) Customer receives many small incoming wire transfers and then orders a large outgoing wire transfer to another country.
Unusual activity in credit transactions	5	(a) A customer's financial statement makes representations that do not conform to accounting principles; (b) A transaction is made to appear more complicated than it needs to be by use of impressive but nonsensical terms such as emission rate, prime bank notes, standby commitment, arbitrage or hedge contracts; (c) Customer requests loans either made to offshore companies or secured by obligations of offshore banks; (d) Customer suddenly pays off a large problem loan with no plausible explanation as to the source of funds; (e) Customer purchases certificates of deposit and uses them as collateral for a loan; (f) Customer collateralizes a loan with cash deposits; (g) Customer uses cash collateral located offshore to obtain a loan; (h) Customer's loan proceeds are unexpectedly transferred offshore.
Unusual activity in a broker-dealer setting	6	(a) The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information, or is otherwise evasive regarding that person or entity; (b) For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter account or third-party transfers;

		(c) The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity; (d) The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds from the account; (e) The customer requests that a transaction be processed in such a manner so as to avoid the firm's normal documentation requirements; (f) The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, which, although legitimate, have been used in connection with fraudulent schemes and money laundering activity; (g) The customer's account shows an unexplained high level of activity with very low levels of securities transactions.
Unusual activity indicative of trade-based money laundering	7	(a) Discrepancies in the description of goods or commodity in the invoice or of the actual goods shipped; (b) Amended letters of credit without justification; (c) No apparent business relationship between the parties and transactions; (d) Funds transferred into an account and moved to a high-risk country in the same amount; (e) Companies operating in jurisdictions where their business purpose is not fully understood and there are difficulties in determining ownership; (f) Lack of appropriate documentation to support transactions; (g) Negotiable instruments used to fund transactions in sequential numbers and/or missing payee information.
Unusual activity indicative of potential terrorist financing	8	**Behavior indicators** (a) The parties to the transaction (owner, beneficiary, etc.) being from countries known to support terrorist activities and organizations; (b) Use of false corporations, including shell companies; (c) Inclusion of the individual in the United Nations Sanctions list;

		(d) Media reports that the account holder is linked to known terrorist organization or is engaged in terrorist activities; (e) Beneficial owner of the account is not properly identified; (f) Use of nominees, trusts, family member or third-party accounts; (g) Use of false identification; (h) Abuse of nonprofit organizations;
	8.1	**Indicators linked to financial transactions** (i) The use of funds by nonprofit organization is not consistent with the purpose for which it was established; (j) The transaction is not economically justified considering the account holder's business or profession; (k) A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds; (l) Transactions that are inconsistent with the account's normal activity; (m) Deposits were structured below the reporting requirements to avoid detection; (n) Multiple cash deposits and withdrawals with suspicious references; (o) No business rationale or economic justifications for the transactions; (p) Unusual cash activity in foreign bank accounts; (q) Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country; (r) Use of multiple foreign bank accounts.
Unusual activity for virtual currency (VC), virtual assets (VA), virtual asset service providers (VASPs)	9	**Indicators linked to operations** (a) Structuring transactions with DA (transactions of exchange or transfer), carried out in a similar way to structuring transactions with cash, by breaking into small amounts or into amounts that do not exceed the thresholds established for mandatory registration of transactions or for reporting; (b) Making multiple high-value transactions or in short succession, such as within a 24-hour period; or in a staggered and regular pattern, with no further transactions recorded during a long period afterwards (which is particularly common in ransomware-related cases) or to a newly created or to a previously inactive account;

		(c) Transferring DAs immediately to multiple DASPs, especially to DASPs registered or operated in another jurisdiction where there is no relation to where the customer lives or conducts business; or o there is non-existent or weak AML/CFT regulation; (d) Depositing DAs at an exchange and then often immediately – (i) withdrawing the DAs without additional exchange activity to other DAs (which is an unnecessary step and incurs transaction fees); (i) converting the DAs to multiple types of DAs, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or (ii) withdrawing the DAs from a DASP immediately to a private wallet (this effectively turns the exchange/DASP into an ML mixer); (e) Accepting funds suspected as stolen or fraudulent – (i) depositing funds from DA addresses that have been identified as holding stolen funds, or DA addresses linked to the holders of stolen funds.
	9.1	**Indicators related to Transaction Patterns** *New user transactions* (a) Conducting a large initial deposit to open a new relationship with a DASP, while the amount funded is inconsistent with the customer profile; (b) Conducting a large initial deposit to open a new relationship with a DASP and funding the entire deposit the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after (as most VAs have a transactional limit for deposits, laundering in large amounts could also be done through over-the-counter-trading); (c) A new user attempts to trade the entire balance of VAs, or withdraws the DAs and attempts to send the entire balance off the platform; *Transactions relative to all users* (d) Transactions involving the use of multiple DAs, or multiple accounts, with no logical business explanation;

		(e) Frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same DA account – or by more than one person; or from the same IP address by one or more persons; or concerning large amounts; (f) Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. (Such transactions by a number of related accumulating accounts may initially use DAs instead of fiat currency); (g) Conducting DA-fiat currency exchange at a potential loss (e.g. when the value of DA is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation); (h) Converting a large amount of fiat currency into DAs, or a large amount of one type of DA into other types of DAs, with no logical business explanation.
	9.2	**Indicators related to anonymity** (a) Transactions by a customer involving more than one type of DA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins; (b) Moving a DA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin; (c) Customers that operate as an unregistered/unlicensed DASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of DA transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions; (d) Abnormal transactional activity (level and volume) of DAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation; (e) VAs transferred to or from wallets that show previous patterns of activity associated with the use of DASPs that operate mixing or tumbling services or P2P platforms; (f) Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces;

		(g) Funds deposited or withdrawn from a DA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports; (h) The use of decentralised/unhosted, hardware or paper wallets to transport DAs across borders; (i) Users entering the DASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names; (j) Users entering the DASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a DASP; (k) A large number of seemingly unrelated DA wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other; (l) Use of DAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes; (m) Receiving funds from or sending funds to DASPs whose CDD or know your customer (KYC) processes are demonstrably weak or non-exist; (n) Using D~~V~~A ATMs/kiosks – (i) despite the higher transaction fees and including those commonly used by mules or scam victims; (ii) in high-risk locations where increased criminal activities occur.
	9.3	**Indicators related to senders or recipients** *Irregularities observed during account creation* (a) Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by DASPs; (b) Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious;

		(c) Trying to open an account frequently within the same DASP from the same IP address; (d) Regarding merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration; *Irregularities observed during CDD process* (e) Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds; (f) Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty; (g) Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process; *Customer Profile* (h) A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account; (i) Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated; (j) A customer's DA address appears on public forums associated with illegal activity; (k) A customer is known via publicly available information to law enforcement due to previous criminal association; *Profile of potential money mule or scam victims* (l) Sender does not appear to be familiar with DA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins; (m) A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a DA money mule or a victim of elder financial exploitation; (n) A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business;

		(o) Customer purchases large amounts of DA not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim; *Other unusual behaviour* (p) A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer; (q) A customer tries to enter into one or more DASPs from different IP addresses frequently over the course of a day; (r) Use of language in DA message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information; (s) A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. (This could indicate potential account takeover and attempted extraction of victim balances via trade, or ML scheme to obfuscate funds flow with a DASP infrastructure).
	9.4	**Indicators related to the source of wealth or funds** (a) Transacting with DA addresses or bank cards that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites; (b) DA transactions originating from or destined to online gambling services; (c) The use of one or multiple credit and/or debit cards that are linked to a DA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing DAs are sourced from cash deposits into credit cards; (d) Deposits into an account or a DA address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds; (e) Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal; (f) A customer's funds which are sourced directly from third-party mixing services or wallet tumblers; (g) Bulk of a customer's source of wealth is derived from investments in DAs, ICOs, or fraudulent ICOs, etc;

		(h) A customer's source of wealth is disproportionately drawn from DAs originating from other DASPs that lack AML/CFT controls.
	9.5	**Indicators related to geographical risks** (a) Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located; (b) Customer utilises a DA exchange or foreign-located MVTS in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures; (c) Customer sends funds to DASPs operating in jurisdictions that have no DA regulation, or have not implemented AML/CFT controls; (d) Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing DAs, or sets up new offices in jurisdictions where there is no clear business rationale to do so.

ANNEX 3

OTHER EXAMPLES AND FURTHER GUIDANCE

Examples of possible simplified measures in relation to RBA	1	Examples include: (a) limiting the type or extent of CDD measures, such as altering the type or range of documents, data or information used for verifying the identity of a customer; (b) reducing the frequency of review of the existing CDD records; (c) reducing the degree of ongoing monitoring and scrutiny of transactions based on a reasonable monetary threshold; or (d) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and intended nature from the type of transactions or business relationship established.
Examples of possible enhanced measures in relation to RBA	2	Examples include: (a) obtaining additional information from a wide variety of sources on the customer and (where appropriate) the beneficial owner of the customer before the establishment of the business relationship, and for performing ongoing customer risk assessment; (b) increasing the frequency of review of the existing CDD records; (c) corroborating it with other available sources on the purpose and intended nature of the business relationship or transaction; (d) obtaining additional information and corroborating it with other available sources on the customer's source of wealth or source of funds involved in the transaction or business relationship; (e) increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination; (f) where the customer is a financial institution, obtaining additional or more particular information about the financial institution's underlying customer base and its AML/CFT controls;

		(g) evaluating the information provided by the customer with regard to destination of funds involved in the transaction and the reason for the transaction to better assess the risk of ML/TF; (h) requiring that investment sale proceeds are paid to the customer's bank account from which the funds for investment were originally transferred.
Examples of possible measures in relation to the verification of the name, legal form and current existence of a customer that is a legal person	3	Examples of possible measures to verify the name, legal form and current existence of a legal person: for a locally incorporated company: (a) performing a search of file at the public registries to obtain a company report (or obtaining from the customer a certified true copy of a company search report issued and certified by a company registry or professional person); for a company incorporated overseas: (b) performing a similar company search enquiry of the registry in the place of incorporation to obtain a company report; (c) obtaining a certificate of incumbency or equivalent issued by the company's registered agent in the place of incorporation (or accepting a certified true copy of a certificate of incumbency certified by a professional person); or (d) obtaining a similar or comparable document to a company search report or a certificate of incumbency certified by a professional person in the relevant jurisdiction.
Examples of information which may be collected to identify the intermediate layers of the corporate structure of a legal person with multiple layers in its ownership structure	4	If the customer's ownership structure consists of multiple layers of companies, a Relevant Person should determine on a risk-sensitive basis the amount of information in relation to the intermediate layers to be collected, which may include obtaining a director's declaration incorporating or annexing an ownership chart describing the intermediate layers (the information to be included should be determined on a risk-sensitive basis but at a minimum should include company name and place of incorporation, and where applicable, the rationale behind the particular structure employed). Relevant Persons need not, as a matter of routine, verify the details of the intermediate companies in the ownership structure of a company. Complex ownership structures (e.g. structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to ensure that the Relevant Person is satisfied on reasonable grounds as to the identities of the beneficial owners.

		The need to verify the intermediate corporate layers of the ownership structure of a company will therefore depend upon the Relevant Person's overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for the Relevant Person to consider if it has taken adequate measures to identify the beneficial owners. Where the ownership is dispersed, the Relevant Person may concentrate on identifying and taking reasonable measures to verify the identities of those who exercise ultimate control over the management of the company.
Examples of procedures to establish whether the identification documents offered by customers are genuine, or have been reported as lost or stolen	5	If suspicions are raised in relation to any identification document offered by customers, Relevant Persons should take whatever practical and proportionate steps that are available to establish whether the document offered is genuine, or has been reported as lost or stolen. This may include: (a) searching publicly available information; (b) approaching relevant authorities; or (c) requesting corroboratory evidence from the customer. Where suspicion cannot be eliminated, the document should not be accepted and consideration should be given to making a report to the authorities.
Use of an independent and appropriate person to certify identification documents	6	Use of an independent and appropriate person to certify verification of identification documents guards against the risk that documentation provided does not correspond to the customer whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation.
	6.1	The following is a list of non-exhaustive examples of appropriate persons to certify verification of identification documents: (a) a member of the judiciary in an equivalent jurisdiction; (b) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; (c) other professional person such as certified lawyer, notary public, etc.

	6.2	The certifier should sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it. The certifier should state that it is a true copy of the original (or words to similar effect).
	6.3	Relevant Persons remain liable for failure to carry out prescribed CDD and therefore should exercise caution when considering accepting certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. In any circumstances where a Relevant Person is unsure of the authenticity of certified documents, or that the documents relate to the customer, Relevant Persons should take additional measures to mitigate the ML/TF risk.
Examples of trigger events upon which existing records of customers should be reviewed	7	Examples of trigger events include: (a) when a significant transaction is to take place; (b) when a material change occurs in the way the customer's account is operated; (c) when the Relevant Person's customer documentation standards change substantially; or (d) when the Relevant Person is aware that it lacks sufficient information about the customer concerned.

ANNEX 4

INDICATORS OF CONCEALED BENEFICIAL OWNERSHIP

The list of risk indicators summarised below is not exhaustive and a Relevant Person may identify other indicators.

Indicators about the client or customer	1	(a) The client is reluctant to provide personal information. (b) The client is reluctant or unable to explain: (i) their business activities and corporate history; (ii) the identity of the beneficial owner; (iii) their source of wealth/funds; (iv) why they are conducting their activities in a certain manner; (v) who they are transacting with; (vi) the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions). (c) Individuals or connected persons: (i) insist on the use of an intermediary (either professional or informal) in all interactions without sufficient justification; (ii) are actively avoiding personal contact without sufficient justification; (iii) are foreign nationals with no significant dealings in the country in which they are procuring professional or financial services; (iv) refuse to co-operate or provide information, data, and documents usually required to facilitate a transaction; (v) are politically exposed persons, or have familial or professional associations with a person who is politically exposed; (vi) are conducting transactions which appear strange given an individual's age (this is particularly relevant for underage customers); (vii) have previously been convicted for fraud, tax evasion, or serious crimes;

		(viii) are under investigation or have known connections with criminals; (ix) have previously been prohibited from holding a directorship role in a company or operating a Trust and company service provider (TCSP); (x) are the signatory to company accounts without sufficient explanation; (xi) conduct financial activities and transactions inconsistent with their customer profile; (xii) have declared income which is inconsistent with their assets, transactions, or lifestyle. (d) Legal persons or legal arrangements: (i) have demonstrated a long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activities; (ii) describe themselves as a commercial business but cannot be found on the internet or social business network platforms (such as LinkedIn, XING, etc.); (iii) are registered under a name that does not indicate the activity of the company; (iv) are registered under a name that indicates that the company performs activities or services that it does not provide; (v) are registered under a name that appears to mimic the name of other companies, particularly high-profile multinational corporations; (vi) use an email address with an unusual domain (such as Hotmail, Gmail, Yahoo, etc.); (vii) are registered at an address that does not match the profile of the company; (viii) are registered at an address that cannot be located on internet mapping services (such as Google Maps); (ix) are registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service; (x) where the director or controlling shareholder(s) cannot be located or contacted; (xi) where the director or controlling shareholder(s) do not appear to have an active role in the company; (xii) where the director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements, indicating the use of professional nominees;

		(xiii) have declared an unusually large number of beneficiaries and other controlling interests; (xiv) have authorised numerous signatories without sufficient explanation or business justification; (xv) are incorporated/formed in a jurisdiction that is considered to pose a high money laundering or terrorism financing risk; (xvi) conduct a large number of transactions with a small number of recipients; (xvii) conduct a small number of high-value transactions with a small number of recipients; (xviii) regularly conduct transactions with international companies without sufficient corporate or trade justification; (xix) maintain relationships with foreign professional intermediaries in the absence of genuine business transactions in the professional's country of operation; (xx) receive large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification; (xxi) maintain a bank balance of close to zero, despite frequent incoming and outgoing transactions; (xxii) conduct financial activities and transactions inconsistent with the corporate profile; (xxiii) are incorporated/formed in a jurisdiction that does not require companies to report beneficial owners to a central registry; (xxiv) operate using accounts opened in countries other than the country in which the company is registered; (xxv) involve multiple shareholders who each hold an ownership interest just below the threshold required to trigger enhanced due diligence measures. (e) There is a discrepancy between the supposed wealth of the settlor and the object of the settlement. (f) Individuals, legal persons and/or legal arrangements: (i) make frequent payments to foreign professional intermediaries; (ii) are using multiple bank accounts without good reason; (iii) are using bank accounts in multiple international jurisdictions without good reason;

		(iv) appear focused on aggressive tax minimisation strategies; (v) are interested in foreign company formation, particularly in jurisdictions known to offer low-tax or secrecy incentives, without sufficient commercial explanation; (vi) demonstrate limited business acumen despite substantial interests in legal persons; (vii) ask for short-cuts or excessively quick transactions, even when it poses an unnecessary business risk or expense; (viii) appear uninterested in the structure of a company they are establishing; (ix) require introduction to financial institutions to help secure banking facilities; (x) request the formation of complex company structures without sufficient business rationale; (xi) have not filed correct documents with the tax authority; (xii) provide falsified records or counterfeit documentation; (xiii) are designated persons or groups; (xiv) appear to engage multiple professionals in the same country to facilitate the same (or closely related) aspects of a transaction without a clear reason for doing so. (g) Examination of business records indicate: (i) a discrepancy between purchase and sales invoices; (ii) double invoicing between jurisdictions; (iii) fabricated corporate ownership records; (iv) false invoices created for services not carried out; (v) falsified paper trail; (vi) inflated asset sales between entities controlled by the same beneficial owner; (vii)agreements for nominee directors and shareholders; (viii) family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements;

		(ix) employees of professional intermediary firms acting as nominee directors and shareholders; (x) the resignation and replacement of directors or key shareholders shortly after incorporation; (xi) the location of the business changes frequently without an apparent business justification; (xii) officials or board members change frequently without an appropriate rationale. (h) Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense. (i) Simple banking relationships are established using professional intermediaries.
Indicators of shell companies	2	(a) Nominee owners and directors: (i) formal nominees (formal nominees may be "mass" nominees who are nominated agents for a large number of shell companies); (ii) informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise; (b) Address of mass registration (usually the address of a TCSP that manages a number of shell companies on behalf of its customers). (c) Only a post-box address (often used in the absence of professional TCSP services and in conjunction with informal nominees). (d) No real business activities undertaken. (e) Exclusively facilitates transit transactions and does not appear to generate wealth or income (transactions appear to flow through the company in a short period of time with little other perceived purpose). (f) No personnel (or only a single person as a staff member). (g) Pays no taxes, superannuation, retirement fund contributions or social benefits. (h) Does not have a physical presence.
Indicators about the transaction		(a) The customer is both the ordering and beneficiary customer for multiple outgoing international funds transfers.

		(b) The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client. (c) Finance is provided by a lender, whether a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification. (d) Loans are received from private third parties without any supporting loan agreements, collateral, or regular interest repayments. (e) The transaction: (i) is occurring between two or more parties that are connected without an apparent business or trade rationale; (ii) is a business transaction that involves family members of one or more of the parties without a legitimate business rationale; (iii) is a repeat transaction between parties over a contracted period of time; (iv) is a large or repeat transaction, and the executing customer is a signatory to the account, but is not listed as having a controlling interest in the company or assets; (v) is executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile; (vi) is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile; (vii) appears cyclical (outgoing and incoming transactions are similar in size and are sent to, and received from, the same accounts, indicating that outgoing funds are being returned with little loss) (aka "round-robin" transactions); (viii) involves the two-way transfer of funds between a client and a professional intermediary for similar sums of money; (ix) involves two legal persons with similar or identical directors, shareholders, or beneficial owners; (x) involves a professional intermediary without due cause or apparent justification; (xi) involves complicated transaction routings without sufficient explanation or trade records;

		(xii) involves the transfer of real property from a natural to a legal person in an off-market sale; (xiii) involves the use of multiple large cash payments to pay down a loan; (xiv) involves licensing contracts between corporations owned by the same individual; (xv) involves the purchase of high-value goods in cash; (xvi) involves the transfer of (bearer) shares in an off-market sale; (xvii) a loan or mortgage is paid off ahead of schedule, incurring a loss; (xviii) includes contractual agreements with terms that do not make business sense for the parties involved; (xix) includes contractual agreements with unusual clauses allowing for parties to be shielded from liability but make the majority of profits at the beginning of the deal. (f) The funds involved in the transaction: (i) are unusual in the context of the client or customer's profile; (ii) are anomalous in comparison to previous transactions; (iii) are sent to, or received from, a foreign country when there is no apparent connection between the country and the client, and/or (iv) are sent to, or received from, a jurisdiction that is considered to pose a high money laundering or terrorism financing risk. (g) An asset is purchased with cash and then used as collateral for a loan within a short period of time. (h) Unexplained use of powers of attorney or other delegation processes (for example, the use of representative offices). (i) Unexplained use of express trusts, and/or incongruous or unexplained relationships between beneficiaries (or persons who are objects of a power) and the settlor. (j) Unexplained or incongruous classes of beneficiaries in a trust.

ANNEX 5

PRINCIPAL FUNCTIONS EXPECTED FROM A MLRO

This Section provides assistance to Relevant Persons in conducting an individual review to satisfy itself that its MLRO is able to demonstrate expected principal functions, skills and knowledge in the field of AML/CFT.

While this is not an exhaustive list, the Relevant Persons are encouraged to expand their expectations with regard to a MLRO, to the extent practicable, proportionate to the nature, scale, complexity and money laundering risks of the activities of the Relevant Person's business.

Functions		Description
Implementation of the AML/CFT-related internal controls	1	(a) Ensure that the AML/CFT-related internal controls are developed, regularly updated and monitored, and communicated to, reviewed and approved by the senior management of the Relevant Person; (b) Develop the Relevant Person's AML/CFT-related internal control rules and ensure it is regularly updated; (c) Identification of transactions subject to control for AML/CFT purposes; (d) Provide ongoing training to the Relevant Person's staff so that they are adequately trained to implement its AML/CFT Systems; (e) Ensure appropriate procedures for carrying out ML/TF risk assessment and CDD measures in relation to a customer or proposed business relationship; (f) Communicate breach of the AML/CFT Systems to the Relevant Person's senior management; (g) Communicate to the Relevant Person's senior management the assessment outcomes of complying with the AML/CFT-related internal control rules and follow-up measures to improve ML/TF/PF risk management policies and procedures; (h) Coordinate collecting qualitative and quantitative data across the firm for the ML/TF exposure assessment purposes; (i) Monitor compliance by the Relevant Person's staff with the procedure of STR/TTR detection and filing to the FIU; (j) Carry out ML/TF exposure assessment of the Relevant Person's products and service;

		(k) Develop methods and measures to control and assess the effectiveness of the AML/CFT Systems implementation; (l) Develop a course of action of employees and relevant divisions of the Relevant Person to implement AML/CFT-related internal control rules.
Carry out analysis of the operations (transactions) for AML/CFT purposes	2	(a) Classify indicators and criteria for suspicious activity for AML/CFT purposes; (b) Monitor client activity and carry out analysis of their transactions to identify ML/TF-related suspicious activity; (c) Establish the workflow for identification of transactions and activity subject to control for AML/CFT purposes; (d) Make a decision about whether a STR is justified and about rejecting a transaction with further filling to the FIU, according to the order envisaged by internal control rules; (e) Make a decision about whether a client transaction involves complex, unusual operations, considering the nature of the Relevant Person's business, and (or) relates to known ML/TF typologies and methods; (f) Carry out analysis of information on suspicious transactions and activity, investigations, identification of ML/TF schemes; (g) Keep records of and document information on transactions subject to mandatory control measures; (h) Provide recommendations for the Relevant Person's AML/CFT Systems improvement; (i) Develop a methodology for carrying out analysis of information for AML/CFT purposes.
Cooperation with competent authorities	3	(a) Establish a sustainable communication channel with the competent authority for filing information subject to financial monitoring. (b) Establish a workflow for cooperation with the competent authority (TTR/STR workflow procedure (c) Collect data and file an TTR/STR to the competent authority per the AML Law requirements; (d) Ensure that the competent authority accepted the filed reports; (e) Adjust the information filed to the competent authority (f) Consolidate the data and prepare a report on self-assessment and follow-up measures outcomes.

		(g) Prepare annual AML returns per AML Rules; (h) Participate in preparing responses to competent and financial authorities; (i) File relevant requests to the competent authority for decision-making purposes.
Necessary skills		A Relevant Person should satisfy itself that its MLRO is able to demonstrate at least the following skills: (a) Design and implement the AML/CFT internal control rules; (b) Monitor changes (amendments) to the AML/CFT regulations; (c) Apply the requirements set out in the AML/CFT regulations to a Relevant Person's internal and business activities; (d) Provide adequate training for the Relevant Person's staff on the AML/CFT regulations, rules and internal control programmes; (e) Identify unusual and (or) suspicious activity to mitigate ML/TF/PF risks; (f) Prepare analytical reports and research deliverables based on justified outcomes; (g) Apply the risk-based approach to combat ML/FT/PF; (h) Apply professional terminology.
Necessary knowledge		A Relevant Person should satisfy itself that its MLRO is able to demonstrate at least the following knowledge of: (a) AML Law, AIFC AML Rules, AML Internal Controls Guidance, CDD for non-face-to-face business relations, other relevant AIFC rules and regulations, relevant AML international standards and recommendations; (b) Requirements and procedures on filling reports to the FIU; (c) Liability for breaching the AML/CFT legislation; (d) What is Money Laundering, ML/TF/PF typologies and predicate offences; (e) The sources of information for FATF non-cooperative countries and jurisdictions, the lists of organisations and persons connected to ML/TF/PF; (f) Possess an understanding of the extent to which the financial products and services are exposed to ML/TF/PF;

		(g) Key competencies of the law enforcement and financial authorities in the field of AML/CFT/PF; (h) Baseline standards of the international and regional organisations in the field of AML/CFT; (i) Main methods of collection, processing and analysis of the AML/CFT-related information; (j) Specialised IT tools and products used in the professional activities; (k) The use and structure of shell/shelf companies and their exposure to ML/TF/PF risks; (l) Main types of the industry-related financial services and products, their industry function and application; (m) Main types of approach to assessing the effectiveness of risk management; (n) Indicators (red flags) of off-shore jurisdictions and the risks involved; (o) Techniques and methods of searching and selection of information using open source data (public sources); (p) ML/TF/PF indicators (red flags); (q) Unusual business processes and operations for companies and transactions; (r) Main documentation requirements for a customer profile; (s) A Relevant Person's products and services; (t) Methods and techniques for verifying the source of wealth and source of funds.

ANNEX 6

SELF – ASSESSMENT

This Section provides assistance to Relevant Persons in conducting an individual review to identify elements that can be improved or to evaluate the current status of the Relevant Person's AML/CFT regime. Along with AML/CFT elements, this self-assessment questionnaire also covers other financial crime-related areas that constitute the interrelated risk factors.

While this is not an exhaustive list of self-assessment questions, the Relevant Persons are encouraged to expand their performance self-review, to the extent practicable, proportionate to the nature, scale, complexity and money laundering risks of the activities of the Relevant Person's business.

Subject	**1**	**Money laundering and terrorist financing**
	1.1	**Governance**
		▪ Who has overall responsibility for establishing and maintaining effective AML controls? Are they sufficiently senior? ▪ What are the reporting lines and channels? ▪ Do senior management receive informative, objective information that is sufficient to enable them to meet their AML obligations? ▪ How regularly do senior management commission reports from the MLRO? What do they do with the reports they receive? What follow-up is there on any recommendations the MLRO makes? ▪ How are senior management involved in approving relationships with high risk customers, including politically exposed persons (PEPs)?
	1.2	**Money Laundering Reporting Officer (MLRO)**
		▪ Does the MLRO have sufficient resources, experience, knowledge, access and seniority to carry out their role effectively? ▪ Do the firm's staff, including its senior management, consult the MLRO on matters relating to money-laundering?

		▪ Does the MLRO escalate relevant matters to senior management and, where appropriate, the board? ▪ What awareness and oversight does the MLRO have of the highest risk relationships?
	1.3	**Risk assessment**
		▪ Which parts of the business present greater risks of money laundering? (Has your firm identified the risks associated with different types of customer or beneficial owner, product, transactions, business line, geographical location and delivery channel (e.g. internet, telephone, branches)? Has it assessed the extent to which these risks are likely to be an issue for the firm?) ▪ How does the risk assessment inform your day-to-day operations? (For example, is there evidence that it informs the level of customer due diligence you apply or your decisions about accepting or maintaining relationships?)
	1.4	**Customer due diligence (CDD)**
		▪ Does your firm apply customer due diligence procedures in a risk- sensitive way? ▪ Do your CDD processes provide you with a comprehensive understanding of the risk associated with individual business relationships? ▪ How does the firm identify the customer's beneficial owner(s)? Are you satisfied that your firm takes risk-based and adequate steps to verify the beneficial owner's identity in all cases? Do you understand the rationale for beneficial owners using complex corporate structures? ▪ Are procedures sufficiently flexible to cope with customers who cannot provide more common forms of identification (ID)?
	1.5	**Ongoing monitoring**
		▪ How are transactions monitored to spot potential money laundering? Are you satisfied that your monitoring (whether automatic, manual or both) is adequate and effective considering such factors as the size, nature and complexity of your business?

		▪ Does the firm challenge unusual activity and explanations provided by the customer where appropriate? ▪ How are unusual transactions reviewed? (Many alerts will be false alarms, particularly when generated by automated systems. How does your firm decide whether behaviour really is suspicious?) ▪ How do you feed the findings from monitoring back into the customer's risk profile?
	1.6	**Enhanced due diligence (EDD)**
		▪ How does EDD differ from standard CDD? How are issues that are flagged during the due diligence process followed up and resolved? Is this adequately documented? ▪ How is EDD information gathered, analysed, used and stored? ▪ What involvement do senior management or committees have in approving high risk customers? What information do they receive to inform any decision-making in which they are involved?
	1.7	**Enhanced ongoing monitoring**
		▪ How does your firm monitor its high risk business relationships? How does enhanced ongoing monitoring differ from ongoing monitoring of other business relationships? ▪ Are reviews carried out independently of relationship managers? ▪ What information do you store in the files of high risk customers? Is it useful? (Does it include risk assessment, verification evidence, expected account activity, profile of customer or business relationship and, where applicable, information about the ultimate beneficial owner?)
	1.8	**Liaison with law enforcement**
		▪ Is it clear who is responsible for different types of liaison with the authorities? ▪ How does the decision-making process related to SARs work in the firm? ▪ Are procedures clear to staff?

		▪ Do staff report suspicions to the nominated officer? If not, does the nominated officer take steps to identify why reports are not being made? How does the nominated officer deal with reports received? ▪ What evidence is there of the rationale underpinning decisions about whether a STR is justified? ▪ Is there a documented process for responding to Production Orders, with clear timetables?
	1.9	**Record-keeping and reliance on third parties**
		▪ Can your firm retrieve records promptly in response to the request? ▪ If the firm relies on third parties to carry out AML checks, is this within the limits permitted by the AML Rules? ▪ How does the Relevant Person satisfy itself that it can rely on these firms?
	1.10	**Countering the finance of terrorism**
		▪ How have risks associated with terrorist finance been assessed? Did assessments consider, for example, risks associated with the customer base, geographical locations, product types, distribution channels, etc.? ▪ Is it clear who is responsible for liaison with the authorities on matters related to countering the finance of terrorism?
	1.11	**Customer payments**
		▪ How does your firm ensure that customer payment instructions contain complete payer and payee information? (For example, does it have appropriate procedures in place for checking payments it has received?) ▪ Does the firm review its respondent banks' track record on providing payer data and using appropriate SWIFT messages for cover payments?
Subject	**2**	**Fraud**
	2.1	**Fraud risk mitigation**

		▪ What information do senior management receive about fraud trends? Are fraud losses accounted for clearly and separately to other losses? ▪ Does the firm have a clear picture of what parts of the business are targeted by fraudsters? Which products, services and distribution channels are vulnerable? ▪ How does the firm respond when reported fraud increases? ▪ Does the firm's investment in anti-fraud systems reflect fraud trends? ▪ Are systems and controls to detect and prevent fraud coordinated across the firm, with resources allocated on the basis of an assessment of where they can be used to best effect? ▪ How and when does your firm engage with cross-industry information-sharing exercises? ▪ When processing applications, does your firm consider whether the information the applicant provides is consistent? (For example, is declared income believable compared with stated employment?)
	2.2	**Investment fraud**
		▪ Have the risks of investment fraud (and other frauds where customers and third parties suffer losses) been considered by the firm? ▪ Are resources allocated to mitigating these risks as the result of purposive decisions by management? ▪ Are the firm's anti-money laundering controls able to identify customers who are complicit in investment fraud?
Subject	**3**	**Data security**
	3.1	**Governance**
		▪ How is responsibility for data security apportioned? ▪ Has the firm ever lost customer data? If so, what remedial actions did it take? Did it contact customers? Did it review its systems? ▪ How does the firm monitor that suppliers of outsourced services treat customer data appropriately?

		▪ Are data security standards set in outsourcing agreements, with suppliers' performance subject to monitoring?
	3.2	**Controls**
		▪ Is your firm's customer data taken off-site, whether by staff (sales people, those working from home) or third parties (suppliers, consultants, IT contractors etc)? ▪ If so, what levels of security exist? (For example, does the firm require automatic encryption of laptops that leave the premises, or measures to ensure no sensitive data is taken off-site? If customer data is transferred electronically, does the firm use secure internet links?) ▪ How does the firm keep track of its digital assets? ▪ How does it dispose of documents, computers, and imaging equipment such as photocopiers that retain records of copies? Are accredited suppliers used to, for example, destroy documents and hard disks? How does the firm satisfy itself that data is disposed of competently? ▪ How are access to the premises and sensitive areas of the business controlled? ▪ When are staff access rights reviewed? (It is good practice to review them at least on recruitment, when staff change roles, and when they leave the firm.) ▪ Is there enhanced vetting of staff with access to lots of data? ▪ How are staff made aware of data security risks?
Subject	**4**	**Bribery and corruption**
	4.1	**Governance**
		▪ What role do senior management play in the firm's anti-bribery and corruption effort? Do they approve and periodically review the strategies and policies for managing, monitoring and mitigating this risk? What steps do they take to ensure staff are aware of their interest in this area? ▪ Can your firm's board and senior management demonstrate a good understanding of the bribery and corruption risks faced by the firm, the materiality to its business and how to apply a risk-based approach to anti-bribery and corruption?

		▪ How are integrity and compliance with relevant anti-corruption legislation considered when discussing business opportunities? ▪ What information do senior management receive in relation to bribery and corruption, and how frequently? Is it sufficient for senior management effectively to fulfil their functions in relation to anti- bribery and corruption?
	4.2	**Risk assessment**
		▪ Where is your firm exposed to bribery and corruption risk? (Have you considered risk associated with the products and services you offer, the customers and jurisdictions with which you do business, your exposure to public officials and public office holders and your own business practices, for example your approach to providing corporate hospitality, charitable and political donations and your use of third parties?) ▪ Has the risk of staff or third parties acting on the firm's behalf offering or receiving bribes or other corrupt advantage been assessed across the business? ▪ Who is responsible for carrying out a bribery and corruption risk assessment and keeping it up to date? Do they have sufficient levels of expertise and seniority?
	4.3	**Policies and procedures**
		▪ Do your anti-bribery and corruption policies adequately address all areas of bribery and corruption risk to which your firm is exposed, either in a stand-alone document or as part of separate policies? (for example, do your policies and procedures cover: expected standards of behaviour; escalation processes; conflicts of interest; expenses, gifts and hospitality; the use of third parties to win business; whistleblowing; monitoring and review mechanisms; and disciplinary sanctions for breaches?) ▪ Have you considered the extent to which corporate hospitality might influence, or be perceived to influence, a business decision? Do you impose and enforce limits that are appropriate to your business and proportionate to the bribery and corruption risk associated with your business relationships? ▪ How do you satisfy yourself that your anti-corruption policies and procedures are applied effectively? ▪ How do your firm's policies and procedures help it to identify whether someone acting on behalf of the firm is corrupt?

		▪ How does your firm react to suspicions or allegations of bribery or corruption involving people with whom the firm is connected?
	4.4	**Dealing with third parties**
		▪ Do your firm's policies and procedures clearly define 'third party'? ▪ Do you know your third party? ▪ What is your firm's policy on selecting third parties? How do you check whether it is being followed? ▪ To what extent are third-party relationships monitored and reviewed? Is the frequency and depth of the monitoring and review commensurate to the risk associated with the relationship? ▪ Is the extent of due diligence on third parties determined on a risk-sensitive basis? Do you seek to identify any bribery and corruption issues as part of your due diligence work, e.g. negative allegations against the third party or any political connections? Is due diligence applied consistently when establishing and reviewing third-party relationships? ▪ Is the risk assessment and due diligence information kept up to date? How? ▪ Do you have effective systems and controls in place to ensure payments to third parties are in line with what is both expected and approved?
Subject	**5**	**Sanctions and asset freezes**
	5.1	**Governance**
		▪ Has your firm clearly allocated responsibility for adherence to the sanctions regime? To whom? ▪ How does the firm monitor performance? (For example, statistical or narrative reports on matches or breaches.)
	5.2	**Risk assessment**
		▪ Does your firm have a clear view on where within the firm breaches are most likely to occur? (This may cover different business lines, sales channels, customer types, geographical locations, etc.)

		▪ How is the risk assessment kept up to date, particularly after the firm enters a new jurisdiction or introduces a new product?
	5.3	**Screening customers against sanctions lists**
		▪ When are customers screened against lists, whether the consolidated list, internal watchlists is maintained by the firm, or lists from commercial providers? (Screening should take place at the time of customer take-on.) ▪ If a customer was referred to the firm, how does the firm ensure the person is not listed? (Does the firm screen the customer against the list itself, or does it seek assurances from the referring party?) ▪ How does the firm become aware of changes to the consolidated list? (Are there manual or automated systems? Are customer lists rescreened after each update is issued?)
	5.4	**Matches and escalation**
		▪ What steps does your firm take to identify whether a name match is real? (For example, does the firm look at a range of identifier information such as name, date of birth, address or other customer data?) ▪ Is there a clear procedure if there is a breach? (This might cover, for example, alerting senior management, the AFSA, and giving consideration to a Suspicious Transaction Report.)
	5.5	**Weapons proliferation**
		▪ Does your firm finance trade with high risk countries? If so, is enhanced due diligence carried out on counterparties and goods? Where doubt remains, is evidence sought from exporters that the trade is legitimate? ▪ Does your firm have customers from high risk countries, or with a history of dealing with individuals and entities from such places? If so, has the firm reviewed how the sanctions situation could affect such counterparties, and discussed with them how they may be affected by relevant regulations? ▪ What other business takes place with high risk jurisdictions, and what measures are in place to contain the risks of transactions being related to proliferation?

Subject	6	Insider dealing and market manipulation
	6.1	**Governance**
		▪ Does the firm's senior management team understand the legal definitions of insider dealing and market manipulation, and the ways in which the firm may be exposed to the risk of these crimes? ▪ Does the firm's senior management team regularly receive management information in relation to suspected insider dealing or market manipulation? ▪ How does senior management make sure that the firm's systems and controls for detecting insider dealing and market manipulation are robust? How do they set the tone from the top? ▪ How does the firm's MLRO interact with the individual/departments responsible for order and trade surveillance/monitoring? ▪ How does senior management make decisions in relation to concerns about potential insider dealing or market manipulation raised to them by Compliance or another function? Do they act appropriately to mitigate these risks? ▪ How does senior management make sure that its employees have the appropriate training to identify potential insider dealing and market manipulation?
	6.2	**Risk assessment**
		▪ Has the firm considered whether any of the products/services it offers, or the clients it has, pose a greater risk that the firm might be used to facilitate insider dealing or market manipulation? How has the firm determined this? ▪ Who is responsible for carrying out the risk assessment and keeping it up to date? Do they have sufficient levels of expertise (including markets and financial crime knowledge) and seniority? What framework does the firm have in place for assessing the risk of insider dealing and market manipulation being committed by its employees? ▪ How does the firm use its risk assessment when deciding which business to accept?

		▪ How often is the risk framework reviewed and who approves it? ▪ How does the firm's risk framework for countering the risk of insider dealing and market manipulation interact with the firm's AML risk framework? Are the risk assessments aligned?
	6.3	**Policies and procedures**
		▪ Does the policy define how the firm will counter the risk of being used to facilitate insider dealing and market manipulation? For example, in what circumstances would the firm conduct enhanced monitoring or stop providing trading access to a particular client or employee? ▪ Does the firm have established procedures for following up and reviewing possibly suspicious behaviour? ▪ Do front office staff understand how insider dealing and market manipulation might be committed through the firm, to escalate potentially suspicious activity when appropriate, and challenge client or employee orders (where relevant), if they believe the activity will amount to financial crime? Does the firm have effective whistleblowing arrangements in place to support appropriate financial crime detection and reporting?
	6.4	**Ongoing monitoring**
		▪ Does the firm consider its obligations to counter financial crime when a client's or employee's activity is determined as suspicious via surveillance systems and subsequent investigation? ▪ How do the firm's monitoring arrangements interact with the client-on-boarding process / AML framework? ▪ Does the firm undertake enhanced monitoring for high risk clients? ▪ Does the firm's monitoring cover the activity of any employee trading? ▪ In instances where a firm is concerned about a client which is not the individual or entity who is making the decision to trade, has the firm considered information it has access to, or ways it can gain information, to allow it to counter the risk of being used to further financial crime?

Annex 7

INDEPENDENT AML AUDIT

This Section provides assistance to Authorised Persons in adjusting their understanding of how to organize an independent AML audit and how to find a proper auditor. In addition, the guidance below represents the AFSA expectations with respect to requirements related to the AML Auditors

Guidance on AML Audit	**1.**	**Introduction**
	1.1	Developing an Anti-Money Laundering/Countering Terrorism Financing ("AML/CTF") programmes is the first step after business risk assessment towards ensuring compliance, protecting the reputation, and implementing appropriate AML/CTF measures. According to Rule 14.6.1 (Audit obligation) of the AIFC AML Rules an Authorised Person must ensure that its audit function includes regular reviews and assessments of the effectiveness of the Authorised Person's AML policies, procedures, systems, and controls, and its compliance with its obligations in AIFC AML Rules. The review and assessment undertaken for the purposes of Rule 14.6.1 of the AIFC AML Rules may be undertaken either internally by the Authorised Person's internal audit function, or by a competent firm of independent auditors or compliance professionals.
	1.2	Therefore, it is a legal requirement for all Authorised Persons to conduct an ongoing AML audit to assess their AML/CTF programmes. The purpose of this audit is to ensure that established policies, procedures, systems, and controls are suitable for their activities and that ML/TF risks are identified and mitigated. During an independent AML audit, the company's AML framework is thoroughly examined to identify weaknesses and areas where improvements can be made. Depending on the severity of the findings, penalties may be imposed. However, an AML audit is a valuable opportunity to detect and address weaknesses promptly, enabling the company to improve its compliance efforts. It also helps the company pinpoint areas that require refocusing to achieve the necessary level of compliance.

	1.3	Selecting the appropriate auditor is imperative for the company because they not only provide a critical evaluation but also offer crucial guidance for any required remediation, protecting the company from failure. In order to fully reap the benefits of an AML audit, companies must take several critical steps. It is imperative that companies follow this guidance to ensure they maximize the value of an independent AML audit.
	2.	**Preparation for the AML audit**
	2.1	Like any other process, the audit should begin with proper preparation. To ensure an efficient audit, the company should evaluate its own AML/CTF programs over time, as this will be the first thing the auditor checks and assesses. Here are some questions to help focus on the relevant areas for preparation: ▪ Are the Business Risk Assessment and AML Policies and Internal Control Rules up to date? ▪ How the real procedures and controls are correlated with those outlined in Company's AML/CTF Programmes? ▪ When the last AML/CTF training took place and are the employees, including senior management, up to date with their AML/CTF training? ▪ Has the relevant function been doing Customer Due Diligence and Enhanced Due Diligence? ▪ Have the Customer's dossiers and Customer's AML/CTF profiles been updated? ▪ Has the relevant function undertaken transaction monitoring? ▪ Has the relevant function fulfilled the reporting requirements? ▪ Has the record-keeping been properly organised? ▪ Has the senior management and the MLRO been keeping frequent (regular) dialogue?
	2.2	One of the main Principles of Authorised Persons in accordance with the AIFC Acting Laws the high standards of integrity, which the company should observe and follow. It is crucial to be truthful and upfront with auditors. Attempts by the company to conceal non-compliant areas, such as falsifying records or hastily completing work right before the audit, will be evident to experienced auditors and will reflect poorly on the company's compliance culture. Conversely, discussing shortcomings and corrective actions in

		a cooperative and transparent way with auditors will enhance the audit report and process and demonstrate the company's dedication to integrity and compliance.
	2.3	Considering that the AML audit must be done regularly, the best time to prepare for the next audit is shortly after the previous audit. The results in the final audit report allow the company to make a remediation plan to address all findings (breaches and weaknesses). Such behavior demonstrates that the senior management of the company is taking AML/CTF matter seriously. It also minimises the risk of repeating the same mistakes further and helps to avoid the same breaches again.
	3.	**Research for an appropriate auditor**
	3.1	The AFSA recommends looking for the auditor with respective care given the audit results will affect the company's perception and reflect its maturity. An independent AML audit is not a financial audit and does not require the relevant license of the AIFC. However, the AML audit is a comprehensive scrutiny or examination to understand whether a company has an appropriate AML framework with all respective documents, systems, and controls according to the National AML Law[1] and AIFC AML Rules[2].
	3.2	The companies determine with the auditor the scope of the audit they needed and aspects that they need to be covered proportionate to the nature, scale, complexity and money laundering risks of the activities of the company's business. Nevertheless, the AFSA expects an AML audit generally includes the following: • The full review of the company's AML Policy, Internal Control Rules and Procedures • Testing the effectiveness of company's AML internal procedures • Evaluation of KYC - Customer Due Diligence Procedures review (EDD) • Testing and evaluation of customers transactions monitoring • Sanctions screening checks • FIU related filings review (STRs and TTRs) • Evaluation of AML training and their results • Evaluation of automated monitoring systems (if any)

[1] Law of the Republic of Kazakhstan No 191-IV dated 28 August 2009 on counteracting legalisation (laundering) of proceeds obtained through criminal means and financing of terrorism.

[2] Anti-Money Laundering, counter terrorist financing and Sanctions Rules No. FR0008 of 2017.

		• Evaluation of internal reporting on AML matters • Evaluation of KYE procedures • Review of previous audit reports to assess the efficiency of execution of implemented recommendations given before.
	4.	**The qualification requirements for the AML auditors.**
	4.1	As a regulatory body, AFSA expects all Participants to adhere to the core principles of the AIFC and conduct their activities with skill, care, and diligence. Ensure that audit team members are independent and have no conflicts of interest. To ensure compliance, the AFSA has established minimum qualification requirements for AML auditors. In order to guide research efforts, the following points should be emphasized:
	4.2	Take into account 5 main factors:
	4.2.1	Knowledge and Expertise • Are the auditors certified professionals of one of the internationally recognised professional organisations (such as ACAMS, ICA, ACFCS or analogy)? • Have they a robust knowledge of the AIFC Acting Law and National AML regulation? • Auditor's proficiency with the respective legal and regulatory framework is necessary.
	4.2.2	Industry-specific experience • What audits have they conducted before? • Have they conducted audits or previously worked in the relevant sector? • Do they have experience in the AIFC or other financial centers and understand the context?
	4.2.3	Previous AML audit experience • The prehistory / how long the auditor has been providing such service as AML audit? • What clients have they audited before? • Have they previously carried out any audits or held internal positions involving assurance-type responsibilities?

	4.2.4	Scope and Methodology To ensure that the potential auditor has a comprehensive audit scope, it is recommended to inquire about their audit methods. Will they only review documents sent to them upon request, or will they also conduct interviews with key personnel involved in the AML framework and verify internal procedures in real time? It is not enough for auditors to solely focus on reviewing a large percentage of CDD files without enquiring about other aspects of compliance with AML regulations such as Risk Management programme or Transactions monitoring. Pay special attention to high-risk customers and transactions. AFSA, when reviewing AIFC Participants, has a detailed focus on each aspect of the internal AML framework to ensure that the Company is following the requirements. A competent auditor will focus on the full range of obligations, and it is worthwhile to ask in advance how an auditor achieves this goal.
	4.2.5	Systems and Tools Technological tools and systems can support the independent AML audit function to collect, systematize, categorise, organise, record, and access information and data, and distribute this data to the relevant stakeholders. The data analysis tools and techniques might be utilized to identify unusual patterns or anomalies in financial transactions. This can help uncover potential money laundering activities.
	5.	**Important Notes:**
	5.1	Important Note 1. The current practice shows that unfortunately, some auditors willing to give a "fast pass" are quite common. It's important for the company to understand that a quick pass does not necessarily mean compliance in practice. Hiring an auditor to review things superficially is not an acceptable formal approach. If an auditor doesn't identify systemic issues in internal control or in implementing AML programmes (perhaps due to rushing the audit or not addressing all obligations), then the company may be found "non-compliant" by the AFSA, even if an independent audit yielded a positive conclusion. Additionally, if the auditor intentionally ignored obvious mistakes or deficiencies to make the report appear positive, the AFSA may view it as "willful blindness" and take action against both the company and the auditor.
	5.2	Important Note 2. One critical component for an effective independent AML audit is communication. The company and auditors should appreciate that the independent AML audit is not a regulatory examination yet, but a methodological and collaborative exercise focused on the company's AML/CTF framework with the primary goal of identifying the

		mistakes and determining main areas for improvement and recommending tangible solutions to progress. The aim of auditors is to obtain the best and most representative understanding, and this can only be achieved by maintaining open channels of communication and feedback in order to facilitate continuous improvement of the auditee's AML/CTF strategy.
	5.3	Important Note 3. Auditors can only evaluate what has been recorded, so if the work was done but not written down, the company will not give any credit for this.
	6.	**Recommendations and Tips.**
	6.1	a) Regarding the documents and materials: ▪ The documents must be duly recorded. ▪ Ensure that the auditor develops a comprehensive AML audit plan that outlines the scope, objectives, and methodologies for the audit. The plan should be tailored to your company's specific AML risks and needs. ▪ The auditor will need to read, analyze and take samples from documents. It is crucial to ensure their availability in advance. ▪ Gather relevant documents from separate file cabinets, emails, cloud storage or remote sources. Minimizing the auditor's waiting time for documents is important as prolonging of the audit can increase its costs. ▪ Gather the documents in a logical and clean manner. ▪ Ensure that the auditor will prepare not only a detailed audit report with findings but also include recommendations and advise for action plan. ▪ It is difficult to audit chaotic and incoherent documents. Therefore, it is important to make the auditing process as hassle-free as possible. ▪ Perform a logical check between AML/CFT processes and documents. b) Regarding theory and practice. AML auditors often see gaps between how something was documented and how it was implemented in practice. Has everything been doing as it was outlined in the Risk Assessment and other AML programmes?

		▪ Do a logical check to see what gaps can be encountered and update all documents where possible. ▪ Do your own internal review before the audit. ▪ To ensure compliance, it's important to assess which areas are thriving and which ones may require more attention. Conducting an internal review around six months prior allows for the correction of any weaknesses. It's recommended to check significant areas such as the organization of the AML framework, KYC/CDD, risk assessment, transaction monitoring, staff verification, and staff training. As for staff training, assess the effectiveness of AML training programmes and awareness campaigns among employees. ▪ Ensure that all registries are up to date. ▪ If staff training has been carried out or formed and suspicions were eliminated / filed, exceptions created etc., make sure it is reflected in the registries.
	6.2	Before an audit, it's best to identify any areas of concern that cannot be fixed beforehand. This is better than the auditor discovering the issues themselves. If the company acknowledges and addresses these issues voluntarily, it shows they take their AML responsibilities seriously. It also demonstrates that they understand how to implement policies, procedures, and controls and are aware of any gaps. If a remediation plan is needed, it should be approved by senior management and recorded in the minutes.