AMENDMENTS No. 1

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

Approval date: 19 December 2024

Commencement date: 1 January 2025

Astana, Kazakhstan

Within the amendments to the AIFC
AML/CFT framework

In this Practical Guidance, the underlining indicates a new text and the strikethrough indicates a removed text

(…)

Revision history

Version	Date	Change description	Section changed
AMLPG 001	15/04/2022	n/a	n/a
AMLPG 002		Amendments on AML audit.	Annex 7
AMLPG 003	____ ____________ 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 3
AMLPG 003~~1~~	~~15~~____/____~~04~~/202~~2~~4	**Risk-Based Approach**
		▪ *Business risk assessment*
		▪ *Considering relevant risk factors*
		▪ *Keeping risk assessment up-to-date*
		▪ *Documenting risk assessment*
		▪ *Obtaining senior management approval*
		▪ *Group-wide ML/TF risk assessment*

		▪ *Customer risk assessment*
		▪ *Conducting customer risk assessment*

(…)

Subject	3	**RISK-BASED APPROACH**
(…)		
	3.3	Relevant Persons should also assess the ML/TF risks associated with a custo (hereafter referred to as "customer risk assessment") to determine the degree, fre ongoing monitoring conducted, which should vary in accordance with the asse customer or business relationship. The general idea is that, for instance, if the scale is from 1 to 10, then 10 will cor lowest (the same logic should be if the scale will be from 1 to 100). Individual cate 4–7 medium risk, and 8–10 as high risk. These risk categories are then combin result exceeds the highest grade, it should be considered as prohibited, extrer simply adds up the category totals, resulting in a score ranging. The model ca each of the factors and subfactors differently, for example by focusing more on country. The model can be made even more complex, for example by creating co the overall rating. The degree of complexity varies by organisation; the more reflect the real client's overall risk.
AML Rule 4.2		**Business risk assessment (BURA)**
(…)		
AML Rule 4.2.1		**Considering relevant risk factors**
	3.8	A Relevant Person should holistically take into account relevant risk factors product/service/transaction risk, delivery/distribution channel risk and, where ap Person is exposed to, depending on its specific circumstances. While there is no complete set of risk indicators, the list of risk indicators outlined lower level of risk associated with the risk factors stated above that may be p Relevant Person or its customer base and should be taken into account holisticall 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

(…)		
AML Rule 5.1		**Customer risk assessment**
	3.16	A Relevant Person should assess the ML/TF risks associated with a customer c create a customer risk profile. The information obtained in the initial stages of the Person to conduct a customer risk assessment, which would determine the leve 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 verified, should be increased where the risk associated with the business relati where the associated risk is lower. Customer risk profile should include documentation of customers intended activi The goal is to establish what is normal and expected activity, which forms baseli activity. Customer risk profile should be created based on the triad – customer's inheren age, occupation, average income and source of funds/source of wealth), geogra 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
(…)		
	3.20.	Similar to other parts of the AML/CFT Systems, a Relevant Person shoul implementation of its customer risk assessment framework, and the framework the results of the business risk assessment of the Relevant Person and co complexity of its customer base. The customer risk assessment should holistically take into account a custome country risk, customer risk, product/service/transaction risk, and delivery/distrib behavior. Unusual behaviour of the customer is a behaviour that contradicts with on available data. (For example, it may include inconsistency with the amo transactions with the provided source of funds and source of wealth, or inco transactions with the data provided at the onboarding stage, etc.).

(…)

Version	**Date**	**Part 4**
AMLPG 00~~1~~3	~~15~~__/~~04~~__/2024~~2~~	**AML/CFT Systems**
		▪ *Internal control programmes for AML/CFT purposes*
		▪ *Compliance management arrangements*
		▪ *Senior management oversight*

		▪ *Compliance officer and money laundering reporting officer*
		▪ *Independent audit function*
		▪ *Employee screening*
		▪ *Group-wide AML/CFT Systems*

Subject	**4**	**AML/CFT SYSTEMS**
(…)		
AML Rule 4.3.1	4.5	Having regard to the nature, size and complexity of its businesses and the ML/T Relevant Person should implement adequate and appropriate policies, procedure minimum, include: (a) appropriate representation of AML compliance function in the managing 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) risk management;~~ ~~(b) customer identification;~~ ~~(c) transaction monitoring and reviewing;~~ ~~(d) compliance management arrangements;~~ ~~(e) independent audit function;~~ ~~(f) employee screening procedures; and~~ ~~(g) an ongoing employee training programme.~~ A Relevant Person may rely on a third party consultant to develop policies, proce the purposes of AML Rule 4.3.1. Such third party consultant must perform its worl possess the following characteristics: 1) relevant knowledge and expertise, confirmed by the certificate from 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

		field; 4) absence of negative feedback from the AFSA with regard to the work of s other companies. The Relevant Person relying on such a third party shall bear ultimate responsibili and controls adopted by the Relevant Person.
(…)		
		Compliance officer (CO) and Money Laundering Reporting Officer (MLRO)
(…)		
Annex 5 – Principal functions expected from a MLRO	4.10	A Relevant Person should appoint an MLRO as a central reference point for repor the main point of contact with the FIU and law enforcement agencies. The app relevant decision-making body (or sole decision maker) pursuant to internal co Person. The MLRO should play an active role in identifying and reporting susp 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 purpos (c) cooperation with competent authorities. The individual appointed as MLRO needs to avoid conflicts of interest, whether r not combine the role of the business owner, shareholder or CEO/executive man second line of defence. A MLRO's necessary skills and knowledge are outlined in Annex 5.
(…)		
		Employee screening
	4.13	Relevant Persons should have adequate and appropriate screening procedures hiring employees (Know Your Employee).
	4.13-1	The relevant due diligence procedures should be applied to employees in sen screening, verifying identity, checking criminal records, and references. An emp same lists and sources the company uses for prospective customers (sanctions, F After on-boarding the new employee should be brought to the compliance cult principles and values from the very beginning. They need to know and agree to a compliance policy.
(…)		

		▪ *What CDD measures are and when they must be carried ou*
		▪ *What CDD measures are*
		▪ *When CDD measures must be carried out*
		▪ *Identification and verification of the customer's identity*
		▪ *Customer that is a natural person*
		▪ *Customer that is a legal person*
		▪ *Customer that is a trust or other similar legal arrangement*
		▪ *Identification and verification of a beneficial owner (BO)*
		▪ *Beneficial owner in relation to a natural person*
		▪ *Beneficial owner in relation to a legal person*
		▪ *Beneficial owner in relation to a Trust*
		▪ *Ownership and control structure*
		▪ *Threshold and indirect ownership*
		▪ *Identification and verification of a person named to act on be*
		▪ *Reliability of documents, data or information*
		▪ *Purpose and intended nature of business relationship*
		▪ *Delayed identity verification during the establishment of a bu*
		▪ *Simplified customer due diligence (SDD)*
		▪ *Listed company*
		▪ *Government and public body*
		▪ *Customer not physically present for identification purposes*
		▪ *Special requirements*
		▪ *Nominee shareholders*
		▪ *Jurisdictions posing a higher risk*
		▪ *Jurisdictions subject to a call by the FATF*
		▪ *Reliance on CDD performed by third parties*

		▪ *Third parties*
		▪ *Failure to satisfactorily complete CDD measures*
		▪ *Prohibition on anonymous accounts*

Subject	**5**	**CUSTOMER DUE DILIGENCE**
(…)		
		What CDD measures are
	5.4	The following are CDD measures applicable to a Relevant Person: (a) identify the customer and verify the customer's identity using docume reliable and independent source (see section 5.11); (b) where there is a beneficial owner in relation to the customer, identify and beneficial owner's identity so that the Relevant Person is satisfied that including, in the case of a legal person or trust, measures to enable t ownership and control structure of the legal person or trust (see sections (c) obtain information on the purpose and intended nature of the business Relevant Person unless the purpose and intended nature are obvious (se (d) understand the customer's sources of funds and sources of wealth; and (e) ~~(d)~~ if a person purports to act on behalf of the customer: (i) identify the person and take reasonable measures to verify the pers information provided by a reliable and independent source; and verify the person's authority to act on behalf of the customer (see sections 5.39 –
(…)		
		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 c is equal or exceeds USD 1,000; (ii) equal to or exceeding an aggregate value of USD 15,000, whether ca operations that appear to the Relevant Person to be linked; or (iii) a wire transfer equal to or exceeding an aggregate value of USD operation or several operations that appear to the Relevant Person to

		(c) when the Relevant Person suspects that the customer or the customer's a (d) when the Relevant Person doubts the veracity or adequacy of any i purpose of identifying the customer or for the purpose of verifying the cus
	5.9	Relevant Persons should be vigilant to the possibility that a series of linked exceed the CDD thresholds of USD 1,000 for wire transfers or transactions with types of transactions. Where Relevant Persons become aware that these t measures must be carried out.
(…)		
Guidance on customer due diligence	5.38-1	In order to correctly understand the sources of funds and wealth, the Relevant the clients themselves, for instance, in the form of a special paper or digital fo indicate among others their demographic data, occupation, sources of origin a income. It is important to inform the client about the need to indicate the actual desired one. Depending on the information collected while establishing risk profi be able to establish an understanding of what is usual for the client with this parti go beyond the usual behavior/activity. Thus, characteristics that go beyond the u increases the risks of Customer at the CDD stage. In case of increased risks, th verify the sources of funds and wealth. The absence of requirement to request additional documented confirmation of th of standard CDD should not mislead the Relevant Person into considering tha verification measures and limit the use of the EDD. The risk-based verification s risk assessment system should stipulate that the Relevant Person, adapting it to of the business, determines what is usual (understandable and explainable) Factors that raise doubts or concerns should increase the level of risk and provid
(…)		
		Reliance on CDD performed by third parties
(…)		
	5.80-1	A Relevant Person must not rely on third parties to provide ongoing monitor responsibility of the Relevant Person to conduct ongoing due diligence th relationship to ensure consistency of the transactions with the Relevant Pers business and risk profile, including, the source of funds.
(…)		

Version	**Date**	**Part 6**
AMLPG 001	15/04/2022	**Politically Exposed Persons (PEPs)**

		▪ *General*
		▪ *Special requirements and additional measures for PEPs*

Subject	**6**	**POLITICALLY EXPOSED PERSONS (PEPs)**
(…)		
	6.15	According to FATF Recommendation 12 the handling of a person who is no lo function should be based on an assessment of risk and not on prescribed time li that financial institutions and DNFBPs assess the ML/TF risk of a PEP who is no l function, and take effective action to mitigate this risk. Possible risk factors are: (1) individual could still exercise; the seniority of the position that the individual held a previous and current function are linked in any way (e.g., formally by appointment the fact that the PEP continues to deal with the same substantive matters).

(…)

Version	**Date**	**Part 8**
AMLPG 00~~1~~3	~~15~~__/__~~04~~/202~~2~~4	**Terrorist Financing, Financial Sanctions and Proliferation Finar**
		▪ *Terrorist financing (TF)*
		▪ *Financial sanctions & proliferation financing*
		▪ *Sanctions imposed by other jurisdictions*
		▪ *Database maintenance, screening and enhanced checking*

Subject	**8**	**TERRORIST FINANCING, FINANCIAL SANCTIONS AND PROLIFERATION FIN**
(…)		
		Sanctions imposed by other jurisdictions
	8.4	A Relevant Person operating internationally will need to be aware of the scope an those jurisdictions. Where these sanctions regimes may affect their operations, R implications exist and take appropriate measures, such as including relevant ov screening purpose, where applicable. Such regimes include unilateral sanctions Office of Foreign Assets Control (OFAC)), the European Union (EU), and United K Treasury Office of Financial Sanctions Implementation (HMT UK OFSI)).

(…)		

Version	Date	Part 9
AMLPG 00~~1~~3	~~15~~__/__~~04~~/2024~~2~~	**Suspicious Transaction Reports, Threshold Transaction Repor Enforcement Requests**
		▪ *General issues*
		▪ *Knowledge vs. suspicion*
		▪ *Tipping-off*
		▪ *AML/CFT Systems in relation to suspicious transaction r transaction reporting*
		▪ *Money laundering reporting officer*
		▪ *Identifying suspicious transactions*
		▪ *Internal reporting*
		▪ *Reporting to the FIU*
		▪ *Post reporting matters*
		▪ *Record-keeping*
		▪ *Requests from law enforcement agencies*

Subject	9	**SUSPICIOUS TRANSACTION REPORTS, THRESHOLD TRANSACTION RE REQUESTS**
(…)		
		Knowledge vs. suspicion
(…)		
	9.3	Suspicion is more subjective. Suspicion is personal and falls short of proof based Person is concerned, when a transaction or a series of transactions of a custor Person's knowledge of the customer, or is unusual (e.g. in a pattern that has no a by unnecessary routing of funds through third party accounts), the Relevant Pe further examine the transactions and identify if there is any suspicion (see sections Unnecessary routing of funds through third party accounts means routing without c

(…)		
		AML/CFT Systems in relation to ~~suspicious~~ transaction reporting
	9.7	A Relevant Person should implement appropriate AML/CFT Systems in order to fu properly manage and mitigate the risks associated with any customer or transa 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, rep 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 bas to suspicious transaction reporting comply with relevant legal and regulatory rec type and extent of the measures to be taken should be appropriate having rega nature and size of the business. The policies, procedures, systems and controls to defined thresholds, and submission of TTRs to the FIU should be performed in acc
(…)		
		Record-keeping
(…)		
	9.30	A Relevant Person must establish and maintain a record of all STRs made to the F the date of the STR, the person who made the STR, and information to allow the p This register may be combined with the register of internal reports, if considered ap A Relevant Person must establish and maintain a record of all TTRs made to the F

(…)

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.

(…)		
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 to set up a discretionary management agreement for an investmen

		requests the Relevant Person to buy and sell particular securities for t the customer's instructions); (b) non-resident customers who have no discernible reasons for opening a Republic of Kazakhstan (AIFC); (c) the use of legal persons or arrangements as personal asset-holding ve 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-inter (f) the ownership structure of a company appears unusual or excessively c the company's business; (g) the customer or the family member or close associate of a customer owner of a customer is a PEP); (h) customers that have been mentioned in negative news reports from cre predicate offences for ML/TF or financial crimes; (i) nature, scope and location of business activities generating the funds jurisdictions posing a higher risk; (j) customers that have sanction exposure; (k) where the origin of wealth (for high risk customers and PEPs) or owners (l) a customer introduced by an overseas financial institution, affiliate or ot jurisdictions posing a higher risk;~~.~~ (m) the activity or transactions of the customer does not correspond the cus Examples of customers that may be considered to carry lower ML/TF risk incluc (a) specific types of customers that may be eligible for SDD as specified in (b) customers who are employment-based or with a regular source of ir which supports the activity being undertaken; and (c) the reputation of the customer, e.g. a well-known, reputable private cc documented by independent sources, including information regarding its

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.

(…)		
Unusual activity for virtual currency	9	**Indicators linked to operations** (a) Structuring transactions with D~~V~~A (transactions of exchange or tra

(VC), virtual assets (VA), virtual asset service providers (VASPs)		structuring transactions with cash, by breaking into small amounts c thresholds established for mandatory registration of transactions or for (b) Making multiple high-value transactions or in short succession, suc staggered and regular pattern, with no further transactions recorded d particularly common in ransomware-related cases) or to a newly create (c) Transferring D~~V~~As immediately to multiple D~~V~~ASPs, especially to D~~V~~ jurisdiction where there is no relation to where the customer lives or existent or weak AML/CFT regulation; (d) Depositing D~~V~~As at an exchange and then often immediately – (i) withdrawing the D~~V~~As without additional exchange activity to othe and incurs transaction fees); (i) converting the D~~V~~As to multiple types of D~~V~~As, again incurring logical business explanation (e.g. portfolio diversification); or (ii) withdrawing the D~~V~~As from a D~~V~~ASP immediately to a priv exchange/D~~V~~ASP into an ML mixer); (e) Accepting funds suspected as stolen or fraudulent – (i) depositing funds from D~~V~~A addresses that have been identified as 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 inconsistent with the customer profile; (b) Conducting a large initial deposit to open a new relationship with a D~~V~~ first day it is opened, and that the customer starts to trade the total am that same day or the day after, or if the customer withdraws the who have a transactional limit for deposits, laundering in large amounts counter-trading); (c) A new user attempts to trade the entire balance of VAs, or withdrav entire balance off the platform; *Transactions relative to all users* (d) Transactions involving the use of multiple D~~V~~As, or multiple accounts, (e) Frequent transfers in a certain period of time (e.g. a day, a week, a mo by more than one person; or from the same IP address by one or more (f) Incoming transactions from many unrelated wallets in relatively smal subsequent transfer to another wallet or full exchange for fiat curren related accumulating accounts may initially use D~~V~~As instead of fiat cu (g) Conducting D~~V~~A-fiat currency exchange at a potential loss (e.g. wh regardless of abnormally high commission fees as compared to indus transactions have no logical business explanation); (h) Converting a large amount of fiat currency into D~~V~~As, or a large amour D~~V~~As, with no logical business explanation.

	9.2	**Indicators related to anonymity** (a) Transactions by a customer involving more than one type of D~~V~~A, c especially those VAs that provide higher anonymity, such as anonym privacy coins; (b) Moving a D~~V~~A that operates on a public, transparent blockchain, suc and then immediately trading it for an AEC or privacy coin; (c) Customers that operate as an unregistered/unlicensed D~~V~~ASP on p particularly when there are concerns that the customers handle h customer’s behalf, and charge higher fees to its customer than t exchanges. Use of bank accounts to facilitate these P2P transactions; (d) Abnormal transactional activity (level and volume) of D~~V~~As cashed associated wallets with no logical business explanation; (e) VAs transferred to or from wallets that show previous patterns of acti that operate mixing or tumbling services or P2P platforms; (f) Transactions making use of mixing and tumbling services, suggestin funds between known wallet addresses and darknet marketplaces; (g) Funds deposited or withdrawn from a D~~V~~A address or wallet with dire suspicious sources, including darknet marketplaces, mixing/tumbling illegal activities (e.g. ransomware) and/or theft reports; (h) The use of decentralised/unhosted, hardware or paper wallets to trans (i) Users entering the D~~V~~ASP platform having registered their Internet c domain name registrars (DNS) that suppress or redact the owners of th (j) Users entering the D~~V~~ASP platform using an IP address associated that allows anonymous communication, including encrypted emails an using various anonymous encrypted communication means (e.g. for games, etc.) instead of a D~~V~~ASP; (k) A large number of seemingly unrelated D~~V~~A wallets controlled from t which may involve the use of shell wallets registered to different users (l) Use of D~~V~~As whose design is not adequately documented, or that ar aimed at implementing fraudulent schemes, such as Ponzi schemes; (m) Receiving funds from or sending funds to D~~V~~ASPs whose CDD or kn demonstrably weak or non-exist; (n) Using D~~V~~A ATMs/kiosks – (i) despite the higher transaction fees and including those commonly u (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 res imposed by D~~V~~ASPs;

(b) Transactions initiated from non-trusted IP addresses, IP addresse addresses previously flagged as suspicious;

(c) Trying to open an account frequently within the same D~~V~~ASP from the

(d) Regarding merchants/corporate users, their Internet domain registra their jurisdiction of establishment or in a jurisdiction with a weak proces

Irregularities observed during CDD process

(e) Incomplete or insufficient KYC information, or a customer declines re regarding source of funds;

(f) Sender / recipient lacking knowledge or providing inaccurate informat funds, or the relationship with the counterparty;

(g) Customer has provided forged documents or has edited photographs of the on-boarding process;

Customer Profile

(h) A customer provides identification or account credentials (e.g. a non shared by another account;

(i) Discrepancies arise between IP addresses associated with the custor which transactions are being initiated;

(j) A customer's D~~V~~A address appears on public forums associated with i

(k) A customer is known via publicly available information to law e association;

Profile of potential money mule or scam victims

(l) Sender does not appear to be familiar with DA technology or online c could be money mules recruited by professional money launderers, deceived into transferring illicit proceeds without knowledge of their ori

(m) A customer significantly older than the average age of platform users numbers of transactions, suggesting their potential role as a D~~V~~A m exploitation;

(n) A customer being a financially vulnerable person, who is often used trafficking business;

(o) Customer purchases large amounts of D~~V~~A not substantiated by avail historical financial profile, which may indicate money laundering, a mor

Other unusual behaviour

(p) A customer frequently changes his or her identification information, in or financial information, which may also indicate account takeover agai

(q) A customer tries to enter into one or more D~~V~~ASPs from different IP a day;

(r) Use of language in D~~V~~A message fields indicative of the transactio activity or in the purchase of illicit goods, such as drugs or stolen credit

(s) A customer repeatedly conducts transactions with a subset of indivi could indicate potential account takeover and attempted extraction of v

		to obfuscate funds flow with a D~~V~~ASP infrastructure).
	9.4	**Indicators related to the source of wealth or funds** (a) Transacting with D~~V~~A addresses or bank cards that are connected to schemes, sanctioned addresses, darknet marketplaces, or other illicit w (b) VA transactions originating from or destined to online gambling service (c) The use of one or multiple credit and/or debit cards that are linked to a of fiat currency (crypto-to-plastic), or funds for purchasing D~~V~~As are cards; (d) Deposits into an account or a D~~V~~A address are significantly higher th funds, followed by conversion to fiat currency, which may indicate theft (e) Lack of transparency or insufficient information on the origin and owne the use of shell companies or those funds placed in an Initial Coin investors may not be available or incoming transactions from online p cards followed by instant withdrawal; (f) A customer's funds which are sourced directly from third-party mixing s (g) Bulk of a customer's source of wealth is derived from investments in D (h) A customer's source of wealth is disproportionately drawn from D~~V~~As AML/CFT controls.
	9.5	**Indicators related to geographical risks** (a) Customer's funds originate from, or are sent to, an exchange that is either the customer or exchange is located; (b) Customer utilises a D~~V~~A exchange or foreign-located MVTS in a hig have inadequate, AML/CFT regulations for VA entities, including inade (c) Customer sends funds to D~~V~~ASPs operating in jurisdictions that implemented AML/CFT controls; (d) Customer sets up offices in or moves offices to jurisdictions that have regulations governing D~~V~~As, or sets up new offices in jurisdictions wh to do so.

(…)

Annex 7

INDEPENDENT AML AUDIT

(…)		
	2.	**Preparation for the AML audit**
	2.1	Like any other process, the audit should begin with proper preparation. To should evaluate its own AML/CTF programs over time, as this will be

		assesses. Here are some questions to help focus on the relevant areas for preparatio ▪ Are the Business Risk Assessment and AML Policies and Internal C ▪ How the real procedures and controls are correlated with th Programmes? ▪ When the last AML/CTF training took place and are the employee date with their AML/CTF training? ▪ Has the relevant function been doing Customer Due Diligence and E ▪ Have the Customer's dossiers and Customer's AML/CTF profiles be ▪ 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

(…)