AMENDMENTS № 7 TO AIFC ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND SANCTIONS RULES

Approval Date: 15 December 2024

Commencement Date: 1 January 2025

Astana, Kazakhstan

Within the amendments to the AIFC Credit Rating Agencies framework

PROPOSED AMENDMENTS TO AIFC ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING AND SANCTIONS RULES

In these amendments, underlining indicates a new text and strikethrough indicates a removed text.

(…)

2. APPLICATION

2.1. Application

(a)The AML Rules apply to:

(i) every Relevant Person in respect of all its AFSA regulated or supervised activities except an Authorised Firm licenced to operate a Representative Office or a Credit Rating Agency; and

(ii) the persons specified in AML 2.2 as being responsible for a Relevant Person's compliance with these Rules.

(…)

Within the amendments to the AIFC AML/CFT framework

Proposed amendments to the AIFC Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Rules

In these Rules, the underlining indicates a new text and the strikethrough indicates a removed text

(…)

1. Introduction

(…)

1.2. Purpose of the AML Rules

(a) The AML Rules have been designed to provide a single reference point for all persons and entities (collectively called Relevant Persons) who are supervised by the AFSA for anti-money laundering ("AML"), countering the financing of terrorism ("CFT"), and sanctions compliance. This means that they apply to Authorised Firms, Authorised Market Institutions, Designated Non-Financial Businesses and Professions ("DNFBPs"), FinTech Lab Participants and Registered Auditors.

(…)

1.4. Financial Action Task Force

(…)

(f) In relation to unilateral sanctions imposed in specific jurisdictions such as the European Union, the United Kingdom (HM Treasury) and the United States of America (Office of Foreign Assets Control of the Department of the Treasury), a Relevant Person must consider and take ~~positive steps~~ efficient measures to ensure compliance where required or appropriate.

1.5. Structure of the AML Rules

(a) Chapter 2 sets out the application of the AML Rules.

(b) Chapter 3 sets out guidance on relevant Kazakhstan criminal law.

(c) Chapter 4 explains the meaning of the Rrisk-Bbased Aapproach ("RBA"), which must be applied when complying with these Rules~~.~~ and Business Risk Assessment ("BURA").

(d) Chapter 5 explains the concept of C~~c~~ustomer Rrisk Assessments ("CRA").

(e) Chapter 6 establishes the Rules for Customer Due Diligence ("CDD") and Chapters 7 and 8 set out the different measures that may be appropriate for higher and lower risk customers - Enhanced Due Diligence ("EDD") and Simplified Due Diligence ("SDD").

(f) Chapter 9 sets out when and how a Relevant Person may rely on a third party to undertake all or some of its CDD obligations. Reliance on a third-party CDD reduces the need to duplicate CDD already performed in respect of a customer. Alternatively, a Relevant Person may outsource some or all of its CDD obligations to a service provider.

(g) Chapter 10 sets out certain obligations in relation to correspondent banking and Chapter11 sets out obligations relating to wire transfers.

(h) Chapter 12 sets out a Relevant Person's obligations in relation to UNSC resolutions and sanctions, and government, regulatory and international findings in relation to AML, CFT, and the financing of weapons of mass destruction.

(i) Chapter 13 sets out the obligation for a Relevant Person to appoint a Money Laundering Reporting Officer ("MLRO") and the responsibilities of this role. It also sets out requirements regarding Threshold Transaction Reports ("TTRs") and Suspicious Transaction Reports ("STRs") that are required to be made under the AML Law and explains the concept of "tipping off".

(j) Chapter 14 sets out general obligations, including requirements for AML training, policies, and record keeping.

1.6. Interpretation

Words and expressions ~~used~~ specific to ~~in~~ these Rules that require defining are set out in the Annex 1. Other words and expressions used in these Rules are set out in the AIFC Glossary.

Reference to the relevant Rule in these AML Rules is made by reference to "AML" added by the relevant number of the Rule.

2. APPLICATION

2.1. Application

(a) The AML Rules apply to:

(i) every Relevant Person in respect of all its AFSA regulated or supervised activities, except an Authorised Firm licenced to operate a Representative Office; and

(ii) the persons specified in AML 2.2. as being responsible for a Relevant Person's compliance with these Rules.

(b) For the purposes of these Rules, a Relevant Person means:

(i) an Authorised Firm;

(ii) an Authorised Market Institution;

(iii) a DNFBP; ~~or~~

(iv) a Registered Auditor~~.~~; or

(v) a FinTech Lab Participant.

(…)

2.2. Responsibility for compliance with the AML Rules

(a) Responsibility for a Relevant Person's compliance with these Rules lies with every member of its senior management. Senior management must be fully engaged in ~~the decision-making processes~~ ensuring compliance with the AML Rules and must take ownership of the RBA set out in Chapter 4.

(…)

2.3. AFSA supervision powers in respect of DNFBPs

The AFSA may conduct reviews of DNFBPs to perform its AML and CFT responsibilities, including as part of its RBA to supervision.

The AFSA may conduct inspections of DNFBPs as part of its RBA to supervising DNFBPs for AML and CFT.

Guidance on AML/~~and~~CFT and sanctions supervision

The AFSA receives an annual AML Return from a DNFBP (AML~~Rule~~13.7.) which will assist the AFSA in its supervision of DNFBPs.

Additionally, the AFSA may decide to undertake periodic reviews of one or more DNFBPs as part of its RBA to supervision. The AFSA may also provide further guidance on its approach to AML and CFT supervision of DNFBPs.

The AFSA's reviews may cover matters such as reviewing the firm's systems and controls for conducting a money laundering risk assessment, CDD and complying with applicable ~~UNSC~~ resolutions and sanctions of UNSC, as well as other global economic and financial sanctions applicable in the AIFC[1].

Reviews may involve interviews with senior management and a review of relevant records.

(…)

4. THE RISK-BASED APPROACH

4.1. Obligations of the Risk-Based Approach

4.1.1. General Duty

A Relevant Person must take appropriate steps to identify and assess the risks of money laundering to which its business is exposed, and must establish and maintain policies, procedures, systems and controls to mitigate and manage the risks identified.

A Relevant Person must take appropriate steps to manage and mitigate risks considering country-wide risks, including those relevant for the Republic of Kazakhstan identified in the published reports and guidance given by the Financial Intelligence Unit of the Republic of Kazakhstan (the "FIU") regarding the FATF mutual evaluations and follow-up reports, and implement enhanced measures where higher risks are identified.

(…)

4.3. Internal policies, procedures, systems and controls

4.3.1. Requirements of policies, procedures, systems and controls

The policies, procedures, systems and controls adopted by a Relevant Person under AML 4.1.1. must be:

(a) proportionate to the nature, scale, complexity and money laundering risks of the activities of the Relevant Person's business;

(b) comprised of, at minimum, organisation of the development and maintenance of the policies, procedures, systems and controls required by AML 4.1.1.:

1 List of financial sanctions applicable in the AIFC is presented in the Practical Guidance to AIFC Anti-Money Laundering and Counter – Terrorist Financing Framework.

(i) appropriate representation of AML compliance function in the managing and organising internal control system on AML matters;
(ii) risk management programme (BURA, CRA);
(iii) customer identification programme (KYC/CDD);
(iv) transaction monitoring and reviewing;
(v) employees training and awareness programme;
~~(vi) appropriate representation of compliance function in the management;~~
(vii) adequate screening procedures to ensure high standards when hiring employees (Know Your Employee); and
(viii) independent audit function to test the system.

(c) approved by its senior management; and

(d) monitored, reviewed and updated regularly.

4.3.2. Purpose of policies, procedures, systems and controls

Purpose of policies, procedures, systems and controls is efficient detection of money laundering and terrorist financing (ML/TF), sanctions violation, prevention and minimisation of ML/TF and sanctions risks.

The policies, procedures, systems and controls must provide for the identification and scrutiny of including, but not limited to:

(a) complex or unusually large transactions, or an unusual pattern of transactions;

(b) transactions which have no apparent economic or legal purpose; ~~and~~

(c) other activity which the Relevant Person regards as particularly likely by its nature to be related to money laundering, sanctions evasion or other financial crimes;~~.~~

(d) actions aimed at evading proper verification and (or) financial monitoring;

(e) transactions with money and (or) other property, for which there is reason to believe that it is aimed at cashing out money obtained by criminal means; and

(f) transaction with money and (or) other property, the participant of which is a person registered (residing) in a geographic area (state or territory) considered to be an area of high risk.

4.3.3. Record of policies, procedures, systems and controls

A Relevant Person must maintain a written record of the policies, procedures, systems and controls established under AML 4.1.1. The ~~Rules~~ requirements regarding record-keeping for the purposes of th~~ese~~is Rule~~s~~ are in AML 14.5.

Guidance on ~~the Risk-Based Approach~~ RBA

(a) AML 4.1.1. requires a Relevant Person to adopt an approach to AML which is proportionate to the risks inherent in its business. This is illustrated in Figure 1 ~~below~~. The AFSA expects the RBA to be a key part of the Relevant Person~~'~~s AML compliance culture and to cascade down from the senior management to the rest of the organisation. It requires the full commitment and support of senior management, and the active co-operation of all employees. Embedding the RBA within its business allows a Relevant

Person to make decisions and allocate AML resources in the most efficient and effective way.

(b) No system of checks will detect and prevent all money laundering. The RBA will, however, balance the cost burden placed on Relevant Persons and their customers, against a realistic assessment of the threat of the Relevant Person's business being used in connection with money laundering. It will focus the effort where it is needed and will have most impact.

(c) In implementing the RBA, a Relevant Person is expected to have in place processes to identify and assess money laundering risks. After the risk assessment, the Relevant Person is expected to monitor, manage and mitigate the risks in a way that is proportionate to the Relevant Person's exposure to those money laundering risks. The general principle is that where there are higher risks of money laundering, a Relevant Person is required to take enhanced measures to manage and mitigate those risks, and that, correspondingly, when the risks are lower, simplified measures are permitted.

(d) The RBA discourages a "tick-box" approach to AML. Instead, a Relevant Person is required to assess relevant money laundering risks and adopt a proportionate response to such risks.

(e) RBA identifies, manages and analyses ML/TF and sanctions risks in order to develop and effectively implement appropriate procedures and controls. It is therefore critical that risk ratings accurately reflect existing risks, provide meaningful assessments leading to practical steps to reduce those risks, are reviewed periodically and, where necessary, regularly updated.

(f) The risk-based analysis should include, among other things, relevant inherent and residual risks at the country, industry, entity itself and business relationship levels. As a result of this analysis, a Relevant Person should develop a thorough understanding of the risks inherent in its customer base, products, delivery channels, services and products offered (pre-existing and new services/products), and the jurisdictions in which it and its customers do business or territories where they are registered from. This understanding should be based on operational, transactional and other internal information collected by the organisation, as well as external sources.

(g) When identifying all ML/TF risks, all relevant information must be considered. This typically requires the input of experts from business, risk management, compliance / legal departments, as well as advice from external experts when necessary. Current and new business products and services should be assessed for vulnerability to money laundering and sanctions violations, and appropriate controls should be put in place before launching them in active stage. There is also a growing number of useful ML/TF risk assessment guidelines available to the public that should be taken into account. For example, published by the FATF, FSRB, regulators and FIU and other agencies such as the UNODC, the IMF, the World Bank, Wolfsberg Group, as well as jurisdiction-specific information, advice and guidance.

(h) Risk is dynamic and requires constant management. It should also be noted that the environment in which every organisation operates is subject to constant change. Externally, political changes in a jurisdiction, as well as the introduction or lifting of economic sanctions, can affect a country's risk rating.

(i) Unless a Relevant Person understands the money laundering and sanctions risks to which it is exposed, it cannot take appropriate steps to prevent its business being used for the purposes of money laundering and sanctions violations. Money laundering risks vary from business to business depending on the nature of the business, the type of customers a business has, and the nature of the products and services sold.

(j) Relevant Persons that do not offer complex products or services and that have limited international exposure may not need an overly complex or sophisticated business risk assessment, but it should be tailored to the specifics of business and scope of the

Relevant Person.

(k) Using the RBA, a Relevant Person assesses its own vulnerabilities to money laundering and takes all reasonable steps to eliminate or manage such risks. The results of this assessment will also feed into the Relevant Person's risk assessment of its customers (see Chapter 6).

Risk management is a continuous process, carried out on a dynamic basis. A money laundering risk assessment is not a one-time exercise. The AFSA expects a Relevant Person's risk management processes for managing money laundering risks are kept under regular review and that any changes made to policies, procedures, systems and controls are recorded.

(l) The Relevant Person should develop and implement the risk assessment model based on quantitative and qualitative characteristics. Numerical values allow to determine the risk category (geography, customer type, products, services, channels used) and the customer's overall risk. Each category can be scored differently, depending on the circumstances of each company's business.

5. CUSTOMER RISK ASSESSMENT

5.1. Assessing customer money laundering risks

5.1.1. Requirement to conduct a customer risk assessment

A Relevant Person must:

(a) undertake a risk-based assessment of every customer; ~~and~~

(b) assign the customer a risk rating proportionate to the customer's money laundering risks; and

(c) create customer risk profile based on the CRA procedure.

5.1.2. Timing of the customer risk assessment

The customer risk assessment in AML 5.1.1 must be completed ~~prior to~~ while conducting CDD for new customers, and where, for an existing customer, there is a material change in circumstances.

5.1.3. Conduct of the customer risk assessment

When undertaking a risk-based assessment of a customer under AML 5.1.1, a Relevant Person must:

(a) identify the customer, any beneficial owner(s) and any person acting on behalf of a customer;

(b) obtain information on the purpose and intended nature of the business relationship;

(c) consider the type of customer, its ownership and control structure, and its beneficial ownership (if any);

(d) consider the nature of the customer's business relationship with the Relevant Person;

(e) consider the customer's country of origin, residence, nationality, place of incorporation or place of business;

(f) consider the relevant product, service or transaction;

(g) consider the consistency of the amount of transactions with the provided sources of funds and sources of wealth (SOF/SOW);

(h) ~~(g)~~ consider the beneficiary of a life insurance policy, where applicable; and

(i) ~~(h)~~ consider the outputs of the business risk assessment under Chapter 4.

(…)

5.1.6. Prohibition on relationships with Shell Banks

A Relevant Person must not establish or maintain a business relationship with a Shell Bank.

Guidance on Shell Banks

AML 5.1.6. prohibits a Relevant Person from establishing or maintaining a business relationship with a Shell Bank. The presence of a local agent or administrative staff of a bank would not constitute a physical presence in the country in which the customer is incorporated or licensed.

Guidance on customer risk assessments

(a) The findings of the customer risk assessment will assist the Relevant Person in determining the level of CDD that should be applied in respect of each customer and beneficial owner.

(b) In assessing the nature of a customer, a Relevant Person should consider such factors as the legal structure of the customer, the customer's business or occupation, the location of the customer's business and the commercial rationale for the customer's business model, the pattern of usual behaviour of the customer.

(c) In assessing the customer business relationship, a Relevant Person should consider how the customer is introduced to the Relevant Person and how the customer is serviced by the Relevant Person, including for example, whether the Person will be a private banking customer, will open a bank or trading account, or whether the business relationship will be purely advisory.

(d) The risk assessment of a customer, which is illustrated in Figure 2, requires a Relevant Person to allocate an appropriate risk rating to every customer. Risk ratings areto be described as "low", "medium" or "high", on a sliding numeric scale, for example with 1 to 3 as "low" risk, 4 to 7 as "medium" risk, and 8 to 10 as "high" risk. Numerical data (value) can be different, depending on the specific of the scoring model of the Relevant Person. Depending on the outcome of a Relevant Person's assessment of its customer's money laundering risk, a Relevant Person should decide what degree of CDD will need to be conducted.

(e) In AML 5.1.5., ownership arrangements which may prevent the Relevant Person from identifying one or more beneficial owners include bearer shares, nominee shareholder

arrangements, and other negotiable instruments in which ownership is determined by possession.

Guidance on the term "customer"

(a) The point at which a person becomes a customer will vary from business to business. However, the AFSA considers that it would usually occur at or prior to the business relationship being formalised, for example, by the signing of a customer agreement or the acceptance of terms of business.

~~(b) A person would not normally be a customer of a Relevant Person merely because such person receives marketing information from a Relevant Person or where a Relevant Person refers a person who is not a customer to a third party (including a Group member).~~

(c) A counterparty would generally be a "customer" for the purposes of these Rules and would therefore require a Relevant Person to conduct CDD on such a person. However, this would not include a counterparty in a transaction undertaken on a Regulated Exchange. Nor would it include suppliers of ordinary business services, to the Relevant Person such as cleaning, catering, stationery, IT or other similar services.

Guidance on high risk customers

(a) In complying with AML 5.1.1., a Relevant Person should consider ~~the following~~ customer risk factors which may indicate that a customer poses a higher risk of money laundering, including, but not limited to:

(i) the business relationship is conducted in unusual circumstances;

(ii) the customer is resident in a geographical area considered by the FATF to be an area of high risk;

(iii) the customer is a legal person or arrangement that is a vehicle for holding personal assets;

(iv) the customer is a company that has nominee shareholders or shares in bearer form;

(v) the customer is a cash-intensive business;

(vi) the corporate structure of the customer is unusual or excessively complex given the nature of the company's business; and

(vii) the customer has been subject to adverse press or public information related to potential money laundering activities.

(b) In complying with AML 5.1.1. a Relevant Person should also consider the following product, service, transaction or delivery channel risk factors:

(i) the product involves private banking;

(ii) the product or transaction is one which might favour anonymity;

(iii) the situation involves non-face-to-face business relationships and/or transactions, without certain safeguards, such as electronic signatures;

(iv) payments will be received from third parties who are unknown to the Relevant Person;

(v) new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for new and existing products;

(vi) the service provides nominee directors, nominee shareholders or shadow directors for hire, or offers the formation of companies in third countries; ~~and~~

(vii) the service involves undocumented or verbal agreements with counterparties or customers; and

(viii) the product has unusual complexity or structure and has no obvious economic purpose.

(c) In complying with AML 5.1.1., a Relevant Person should also consider the following geographical risk factors:

(i) countries identified by credible sources, such as FATF mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering; and

(ii) countries subject to sanctions, embargos or similar measures issued by, for example, the UNSC or identified by credible sources as having significant levels of corruption or other criminal activity and countries or geographic areas identified by credible sources as providing funding or support forterrorism.

Guidance on low risk customers

(a) In complying with AML 5.1.1., the following types of customers may pose a lower risk of money laundering:

(i) a governmental entity, or a publicly-owned enterprise from geographical area of lower risk which has AML/CFT regulation, lower level of criminal activities and corruption and which is not identified by credible sources as providing funding or support for terrorism or extremism;

(ii) an individual resident in a geographical area of lower risk which has AML/CFT regulations which are equivalent to the standards set out in the FATF Recommendations;

(iii) Customers with a long-term and active business relationship with the Relevant Person;

(iv) a regulated Financial Institution whose entire operations are subject to regulation and supervision, including AML regulation and supervision, in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF Recommendations; or

(v) a company whose Securities are listed on a Regulated Market in a jurisdiction which has AML regulations which are equivalent to the standards set out in the FATF Recommendations;

(b) In complying with AML 5.1.1., the following types of product, service, transaction or delivery channel risk factors may pose a lower risk of money laundering:

(…)

~~**Guidance on Shell Banks**~~

~~(a) AML 5.1.6 prohibits a Relevant Person from establishing or maintaining a business relationship with a Shell Bank.~~

~~(b) The presence of a local agent or administrative staff would not constitute a physical presence in the country in which the customer is incorporated or licensed.~~

6. CUSTOMER DUE DILIGENCE

6.1. Conducting Customer Due Diligence

6.1.1. Obligation to conduct Customer Due Diligence

A Relevant Person must:

(a) conduct CDD under AML 6.3.1 for each of its customers;

(a-a) conduct CDD under AML 6.3.1 for each of its customers including when the customer is carrying out occasional transactions 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; ~~and~~

(a-b) ~~including~~ conduct CDD when the customer is carrying out occasional transactions the value of which singularly or in several linked operations (whether at the time or later), is equal or exceeds USD 15,000; and

(b) In addition to (a), ~~and~~ (a-a) and (a-b), conduct EDD under AML 7.1.1 in respect of:

(i) each customer it has assigned as high risk;

(ii) business relationships and transactions with persons from a geographic area (state or territory) considered to be an area of high risk ~~countries with high geographical risk factors~~.

6.1.2. Conducting Simplified Due Diligence

(a) A Relevant Person may conduct SDD in accordance with AML 8.1.1. by modifying the CDD under AML 6.3.1. for any customer it has assigned as low risk. A Relevant Person must not conduct SDD measures in specific high-risk scenarios or when there is a suspicion of money laundering;

(b) A Relevant Person must ensure that assignment of low risk is based on an adequate risk analysis and SDD is commensurate with the risk level identified.

~~**Guidance on Customer Due Diligence**~~

~~(a) A Relevant Person should conduct CDD in a manner proportionate to the customer's money laundering risks identified under Chapter 6. When the money laundering risks are identified as high, a Relevant Person must conduct EDD under Chapter 7.~~

~~(b) This means that all customers are subject to CDD under AML 6.3.1. However, for high risk customers, additional EDD measures should also be conducted under AML 7.1.1.~~

~~(c) The broad objective is that the Relevant Person should know at the outset of the relationship who its customers (and, where relevant, beneficial owners) are, where they operate, what they do and their expected level of activity. In addition to AML 6.1.1(a), a Relevant Person must obtain documents on the legal form and the powers that regulate and bind the legal person or arrangement. The Relevant Person must then consider how~~

~~the profile of the customer's financial behaviour builds up over time, allowing the Relevant Person to identify transactions or activity that may be suspicious.~~

(…)

6.2.3. Establishing a business relationship before Customer Due Diligence is complete

A Relevant Person may establish or maintain a business relationship with a customer pending completion of the verification required by AML 6.3.1. if the following conditions are met:

(a) deferral of verification of the customer or beneficial owner is necessary in order to not to interrupt the normal conduct of business relations in the case of securities transactions. In the securities industry, companies and intermediaries may be required to complete transactions very quickly in accordance with market conditions at the time a customer contacts them, and may be required to complete a transaction before identity verification is completed;

(b) risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification have been adopted and are in place; and there is little risk of money laundering occurring and any such risks identified can be effectively managed by the Relevant Person;

(c) in relation to a bank account opening, there are adequate safeguards in place to ensure that the account is not closed and transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder) before verification has been completed; and

(d) subject to (c), the relevant verification is completed as soon as reasonably practicable before or during the establishment of a business relationship and when transactions for occasional customers are being conducted; and in any event, no later than 30 days after the establishment of a business relationship.

(…)

6.2.5. Cessation of business

The AFSA may specify a period within which a Relevant Person must complete the verification required by AML 6.2.3. failing which the AFSA may direct the Relevant Person to cease any business relationship with the customer.

Guidance on timing of Customer Due Diligence

(a) For the purposes of AML 6.2.2.(a), examples of situations which might lead a Relevant Person to have doubts about the veracity or adequacy of documents, data or information previously obtained could be where there is a suspicion of money laundering in relation to that customer, where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile, or where it appears to the Relevant Person that a person other than the customer is the real customer or in other cases as referred in AML Law and AIFC acts.

(b) ~~In~~ The cases stipulated by AML 6.2.3. are exceptional and ~~are not applicable for~~ do not apply to the most Relevant Persons. Situations that the Relevant Person may take into account include, for example, accepting subscription monies during a short offer period; executing a time critical transaction, which if not executed immediately, would or may cause a customerto incur a financial loss due to price movement or loss of opportunity; and when a customer seeks immediate insurance cover.

(c) When complying with AML 6.2.1., a Relevant Person should also, where appropriate, consider AML 6.6.1. regarding failure to conduct or complete CDD and Chapter 13 regarding STRs and tipping off.

(d) [intentionally omitted].

(e) Relevant Person needs to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification, envisaged by AML 6.2.3. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the limiting or close monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

6.3. Conducting Customer Due Diligence

6.3.1. Obligation to verify and understand

In conducting CDD required by AML 6.1.1., a Relevant Person must:

(a) verify the identity of the customer and any person acting on behalf of the customer, including his authorisation to so act, based on original or properly certified documents, data or information issued by or obtained from a reliable and independent source;

(a-a) verify the identity of any beneficial owner(s) of the customer;

(b) obtain information on and understand the purpose and intended nature of the business relationship;

(c) understand the customer's ~~sources of funds~~ SOF according to the CRA;

(d) understand the customer's ~~sources of wealth~~ SOW according to the CRA; and

(e) conduct on-going due diligence of the customer business relationship under AML 6.4.1.

6.3.2. Customer obligation for life insurance

In complying with AML 6.3.1. for life insurance or other similar policies, a Relevant Person must:

(a) verify the identity of customers as soon as reasonably practicable before or during the establishment of a business relationship and when transactions for occasional customers are being conducted;

(b) ~~(a-a)~~ verify the identity of any named beneficiaries of the insurance policy at the time of pay-out;

(c) ~~(b)~~ verify the identity of the persons in any class of beneficiary, or where these are not identifiable, ensure that it obtains sufficient information to be able to verify the identity of such persons at the time of pay-out;

(d) if a beneficiary of the insurance policy who is a legal person or a legal arrangement presents a higher risk, take enhanced measures which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of pay-out;

(e) take reasonable measures to determine whether the beneficiaries of the insurance policy and/or, where required, the beneficial owner of the beneficiary, are PEPs, at the latest, at the time of the pay-out, and, in cases of higher risks, inform senior management before the pay-out of the policy proceeds, conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a STR; and

(f) include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.

6.3.3. Customer is a Politically Exposed Person

Where a customer, or a beneficial owner of the customer, is a PEP, a Relevant Person must ensure that, in addition to AML 6.3.1., it also:

(a) increases the level of risk, the degree and nature of monitoring of the business relationship, in order to determine whether the customer's transactions or activities appear unusual or suspicious;and

(b) obtains the approval of senior management to commence a business relationship with the customer.

6.3.4 Existing customer becoming a Politically Exposed Person

A Relevant Person must not continue its business relationship with an existing customer if the customer (or a beneficial owner of the customer) becomes a PEP, unless the Relevant Person obtains the approval of its senior management.

Guidance on conducting Customer Due Diligence

(…)

(e) For ~~higher~~ factors increasing the risk ~~situations~~ level, identification information is to be independently verified, using both public and non-public sources.

(f) In complying with AML 6.3.1.(c) a Relevant Person is required to "understand" a customer's source of funds. This means understanding where the funds for a particular service or transaction will come from (i.e. origin of funds used in carrying out a business transaction). ~~e.g. a specific bank or trading account held with a specific financial institution and whether that funding is consistent with the customer's source of wealth~~ The best way of understanding the source of funds is by obtaining information directly from the customer, which will usually be obtained during the on-boarding process. The Relevant Person should keep appropriate evidence of how they were able to understand the source of funds, for example, a copy of the customer account opening form, or customer onboarding form ~~customer questionnaire or a memo of a call with the relationship manager at a financial institution~~ with confirmation of funds' initial sources taking into account customer's risk assessment and customer's behaviour in comparison with his/her risk profile.

(g) In complying with AML 6.3.1.(d) a Relevant Person is required to "understand" a customer's source of wealth. This means understanding the origin of the accumulated monetary assets of an individual, i.e. total assets. For a natural person, this might include ~~questions~~ information about the source of wealth in an application form or customer questionnaire. The understanding ~~may~~ should also be gained through interactions with the relationship manager at a financial institution. It could ~~also~~ be gained by obtaining information from a reliable ~~and independentpublicly~~ available source~~, for example, from published accounts or a reputable news source~~. The understanding need not be a dollar for dollar account of the customer's globalwealth, but it should provide sufficient detail to give the Relevant Person comfort that the customer's wealth is legitimate and also to provide a basis for subsequent on-going due diligence. The understanding of the customer's source of wealth ~~should~~ may be clearly supported by title document~~ed~~, for example, asset title document, audited financial statement, income tax return, etc. taking into account customer's risk assessment and customer's behaviour in comparison with his/her risk profile.

(h) Understanding a customer's sources of funds and wealth is also important for the

purposes of creating customer risk profile and conducting on-going due diligence under AML 6.3.1(e). Initial funding of an account or investments from an unknown or unexpected source may pose a money laundering risk. Similarly, a sound understanding of the customer's source of funds and wealth also provides useful information for a Relevant Person's transaction monitoring programme. Understanding of the customer's sources of funds or wealth shall be performed taking into account customer's risk assessment and customer's behaviour in comparison with his/her risk profile.

(i) An insurance policy which is similar to a life policy would include life-related protection, or a pension, or investment product which pays out to the policy holder or beneficiary upon a particular event occurring or upon redemption.

(j) A Relevant Person should conduct CDD in a manner proportionate to the customer's money laundering risks identified under Chapter 6. When the money laundering risks are identified as high, a Relevant Person must conduct EDD under Chapter 7.

(k) This means that all customers are subject to CDD under AML 6.3.1. However, for high risk customers, additional EDD measures should also be conducted under AML 7.1.1.

(l) The broad objective is that the Relevant Person should know at the outset of the relationship who its customers (and, where relevant, beneficial owners) are, where they operate, what they do and their expected level of activity. In addition to AML 6.1.1.(a), a Relevant Person must obtain documents on the legal form and the powers that regulate and bind the legal person or arrangement. The Relevant Person must then consider how the profile of the customer's financial behaviour builds up over time, allowing the Relevant Person to identify transactions or activity that may be suspicious.

(…)

Guidance on Politically Exposed Persons

(a) Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to a Relevant Person as their position may make them vulnerable to corruption. This risk also extends to members of their families and to their close (known) associates. PEP status itself does not incriminate individuals orentities. It does, however, put the customer into a high~~er~~ risk category until the EDD or on-going monitoring does not decrease the level of such risk.

(b) Generally, a PEP presents a high risk of money laundering because there is a greater risk that such person, if he/she was committing money laundering, would attempt to place his/her money offshore where the customer is less likely to be recognised as a PEP and where it would be more difficult for law enforcement agencies in his/her home jurisdiction to confiscate or freeze his/her criminal property.

(c) Corruption-related money laundering risk increases when a Relevant Person deals with PEPs. Corruption may involve serious crimes and has become the subject of increasing global concern. Customer relationships with family members or close associates of PEPs involve similar risks to those associated with PEPs themselves.

(d) After leaving office PEPs may remain a higher risk for money laundering if they continue to exert political influence, directly or indirectly, or otherwise pose a risk of corruption.

6.4. On-going Customer Due Diligence

6.4.1. On-going obligation

When conducting on-going CDD under AML 6.3.1., a Relevant Person must, using the RBA:

(a) monitor and review transactions undertaken during the course of its customer relationship to ensure that the transactions are consistent with the Relevant Person's knowledge of the customer, its business, its risk rating, and its source of funds;

(b) pay particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose;

(c) enquire into the background and purpose of the transactions in paragraph (b) above;

(d) periodically review the adequacy of the CDD information it holds on customers and beneficial owners to ensure that the information is kept up to date, particularly for customers with a high-risk rating;

(e) periodically review each customer to ensure that the risk rating assigned to a customer under AML 5.1.1.(b) remains appropriate for the customer in light of the money laundering risks; and

(f) at appropriate times apply CDD to existing customers based on materiality and risk considering whether and when CDD has been previously conducted and the adequacy of the CDD information obtained.

(…)

6.5. Checking against sanctions and watchlists~~lists~~

6.5.1. Sanctions and Watchlists review

A Relevant Person must review its customers, their business and transactions against UNSC sanctions lists, ~~and against any other~~ Kazakhstan Sanctions List and Watchlists and any other lists of jurisdictions that they are obliged to follow with while establishing relationships and when complying with AML 6.4.1 (a), (d).

(…)

7. ENHANCED DUE DILIGENCE

7.1. Conducting Enhanced Due Diligence

7.1.1. Obligation to conduct Enhanced Due Diligence

A Relevant Person must conduct EDD where money laundering risks are higher.

Where a Relevant Person is required to conduct EDD under AML 6.1.1, it must, to the extent applicable to the customer:

(a) obtain and verify additional:

(i) identification information on the customer and any beneficial owner;

(ii) information on the intended nature of the business relationship; and

(iii) information on the reasons for a transaction;

(b) update more regularly the CDD information which it holds on the customer and any beneficial owners;

(c) verify information on:

(i) the customer's ~~sources of funds~~ SOF;

(ii) the customer's ~~sources of wealth~~ SOW.~~;~~

(…)

8. SIMPLIFIED DUE DILIGENCE

8.1. Conduct of Simplified Due Diligence

8.1.1. Modifications to AML 6.3.1. for Simplified Due Diligence

Where a Relevant Person is permitted to conduct SDD under AML 6.1.2., modification of AML 6.3.1. may include:

(a) verifying the identity of the customer and identifying any beneficial owners after the establishment of the business relationship;

(b) deciding to reduce the frequency of, or as appropriate not undertake, customer identification updates;

(c) deciding not to verify an identified beneficial owner;

(d) deciding not to verify an identification document other than by requesting a copy;

(e) not enquiring as to a customer's ~~sources of funds~~ SOF or ~~sources of wealth~~ SOW;

(f) reducing the degree of on-going monitoring of transactions, based on a reasonable monetary threshold or on the nature of the transaction; or

(g) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring such purpose and nature from the type of transactions or business relationship established.

8.1.2. Proportionality

The modification in AML 8.1.1. must be proportionate to the customer's money laundering risks.

Guidance on Simplified Due Diligence

(a) AML 8.1.1. provides examples of SDD measures. Other measures may also be used by a Relevant Person to modify CDD in accordance with the customer risks.

(b) A Relevant Person should not use a "one size fits all" approach for all its low risk customers. Notwithstanding that the risks may be low, the degree of CDD conducted needs to be proportionate to the specific risks identified on a case by case basis. For example, for customers where the money laundering risks are very low, a Relevant Person may decide simply to identify the customer and verify such information only to theextent that this is commercially necessary. On the other hand, a low risk customer which is undertaking a complex transaction might require more comprehensive ~~SDD~~procedures.

(c) For the avoidance of doubt, a Relevant Person is always required to identify beneficial owners, except for retail investment funds which are widely held, and investment funds where the investor invests via pension contributions. However, a Relevant Person may decide not to verify beneficial owners of a low risk customer.

(d) An example of circumstances where a Relevant Person might reasonably reduce the frequency of or, as appropriate, eliminate customer identification updates would be where the money laundering risks are low and the service provided does not offer a realistic opportunity for money laundering.

(e) An example of where a Relevant Person might reasonably reduce the degree of on-going monitoring and scrutinising of transactions, based on a reasonable monetary threshold or on the nature of the transaction, would be where the transaction is a recurring, fixed contribution to a savings scheme, investment portfolio or fund or where the monetary value of the transaction is not material for money laundering purposes given the nature of the customer and the transaction type.

9. RELIANCE AND OUTSOURCING

9.1. Reliance on a third party

9.1.1. Permitted reliance

A Relevant Person may rely on the following third parties to conduct one or more elements of CDD on its behalf by entering into contractual agreement:

(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.

(…)

9.1.7 Prohibited reliance

(1) A Relevant Person must not rely on third parties to provide ongoing monitoring CDD procedures for its customers and counterparties on AML and sanctions matters.

(2) For the avoidance of doubt, reliance on third parties in this Rule does not apply to outsourcing or agency relationships established in accordance with AML 9.2. By relying to conduct one or more elements of CDD in outsourcing or agency relationship the Relevant Person is responsible for ensuring that ongoing due diligence is conducted on the business relationship and that transactions carried out in the course of that relationship are properly reviewed. The Relevant Person must ensure that customer's transactions are consistent with the Relevant Person's knowledge of the customer, its business and risk profile, including the source of funds.

(…)

12. SANCTIONS

12.1. Relevant ~~United Nations Security Council~~ resolutions and sanctions

12.1.1. Sanctions systems and controls

A Relevant Person must establish and maintain effective systems and controls to ensure that on an on-going basis it is properly informed as to, and takes reasonable measures to comply with, relevant resolutions or sanctions issued by the UNSC, ~~or~~ by the Republic of Kazakhstan

or with other sanctions applicable in the AIFC.

A Relevant Person must comply with prohibitions from conducting transactions with designated persons and entities, in accordance with the obligations set out in the relevant resolutions or sanctions issued by the UNSC, ~~or~~ by the Republic of Kazakhstan or by other jurisdictions as applicable in the AIFC[2].

A Relevant Person must freeze without delay and without prior notice,the funds or other assets of designated persons and entities pursuant to relevant resolutions or sanctions issued by the UNSC or by the Republic of Kazakhstan.

(…)

12.1.2-1. A Relevant Person must report to the AFSA any actions taken regarding the customer in compliance with the prohibition requirements of the relevant resolutions or sanctions.

12.1.3. Notification requirements

A Relevant Person must ensure that the notification stipulated in AML 12.1.2. and 12.1.2-1. above includes thefollowing information:

(a) a description of the relevant activity in AML 12.1.2.; and

(b) the action proposed to be taken or that has been taken by the Relevant Person regarding the matters specified in the notification.

Guidance on sanctions

(a) In AML 12.1.1. taking reasonable measures to comply with a resolution or sanction may mean that a Relevant Person cannot undertake a transaction for or on behalf of a person or that it may need to conduct further due diligence in respect of a person.

(b) Relevant resolutions or sanctions mentioned in AML 12.1.1. may, among other things, relate to money laundering, sanctions violation or otherwise be relevant to the activities carried on by the Relevant Person.

(c) A Relevant Person should exercise due care to ensure that it does not provide services to, or otherwise conduct business with, a person engaged in money laundering and sanctions violation.

(d) When making a notification to the AFSA in accordance with AML 12.1.2., a Relevant Person should have regard to the requirements of the AML Law in relation to freezing assets and blocking transactions and must also consider whether itis necessary to file a STR.

(e) An Authorised Market Institution should exercise due care to ensure that it does not facilitate fund raising activities or listings by persons engaged in money laundering or sanctions violation.

(f) Relevant Persons must perform checks on an on-going basis against their customer databases and records for any names appearing in resolutions or sanctions ~~issued by the UNSC~~ as well as to monitor transactions accordingly.

(g) A Relevant Person may use a database maintained elsewhere for an up-to-date list of resolutions and sanctions, or to perform checks of customers or transactions against that list. For example, it may wish to use a database maintained by its head office or a Group

2 List of financial sanctions applicable in the AIFC is presented in the Practical Guidance to AIFC Anti-Money Laundering and Counter – Terrorist Financing Framework.

member. However, the Relevant Person retains responsibility for ensuring that its systems and controls are effective to ensure compliance with these Rules.

(…)

12.2.1. Compliance with Findings

A Relevant Person must establish and maintain systems and controls to ensure that on an on-going basis it is properly informed as to, and takes reasonable measures to comply with, any findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions (each of which is referred to in this Rule as a "Finding") issued by (as applicable):

(a) the government of the Republic of Kazakhstan;

(b) the National Bank of the Republic of Kazakhstan;

(c) ~~state~~ A~~a~~gency of Financial Monitoring ~~ies~~ of the Republic of Kazakhstan;

(d) the AFSA; and

(e) the FATF,

concerning the matters in AML 12.2.2.

(…)

13. MONEY LAUNDERING REPORTING OFFICER, THRESHOLD TRANSACTIONS, SUSPICIOUS TRANSACTIONS AND TIPPING OFF

13.1. Money Laundering Reporting Officer

13.1.1. Who can act as Money Laundering Reporting Officer

The MLRO function must be carried out by an individual ~~who is a Director, Partner, Principal Representative, or Senior Manager of an Authorised Person and~~ who has responsibility for the implementation and oversight of an Authorised Person's AML policies, procedures, systems and controls and can act independently in this role.

If MLRO function is carried out solely, it must be carried out by an individual who is at an appropriate level of seniority (for example, at the same level of authority as a Director, Partner, Principal Representative, or Senior Manager of an Authorised Person).

If MLRO function is carried out as a special function delegated by a Compliance Officer to a designated individual (MLRO), then such individual's independence in decision-making must be preserved[3].

(…)

13.5.1. Organisational standing

A Relevant Person must ensure that its MLRO has:

(a) direct access to its senior management;

(b) a level of seniority and independence within the Relevant Person to enable him/her to act

3 Additional clarification is presented in the Practical Guidance to AIFC Anti-Money Laundering and Counter – Terrorist Financing Framework.

on his/her own authority and to act independently in carrying out his/her responsibility;

(c) sufficient resources, including appropriate staff and technology; and

(d) timely and unrestricted access to information sufficient to enable him/her to carry out his/her responsibilities in AML 13.6.1.

(…)

13.6. Responsibilities of Money Laundering Reporting Officer

13.6.1. Oversight responsibility

A Relevant Person must ensure that its MLRO implements and has oversight of, and is responsible for, the following matters:

(a) the day-to-day operations for compliance by the Relevant Person with its AML policies, procedures, systems and controls;

(b) acting as the point of contact to receive notifications from the Relevant Person's employees under AML 13.7.3.;

(c) taking appropriate action under AML 13.8.1. following the receipt of a notification from an employee;

(d) ensuring that the STRs and TTRs are sent to the FIU in accordance with applicable Kazakhstan law~~making STRs in accordance with applicable Kazakhstan law~~;

(e) acting as the point of contact within the Relevant Person for the AFSA, and anyother competent authority regarding money laundering issues;

(f) responding promptly to any request for information made by the AFSA, and anyother competent authority;

(g) receiving and acting upon any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in Chapter 12; ~~and~~

(h) establishing and maintaining an appropriate money laundering training programme and adequate awareness arrangements under Chapter 14~~.~~; and

(i) preparing conclusions based on the results of CDD and make decisions on the possibility of establishing relations with the client, except in cases stipulated by AML 6.3.3. (b).

(…)

13.7.3. Suspicious Activity and Transactions Controls

A Relevant Person must establish and maintain policies, procedures, systems and controls to monitor and detect suspicious activity or transactions in relation to potential money laundering.

A Relevant Person must register in the FIU reporting system for submitting STRs or TTRs before the commencement of its business activities.

(…)

13.7.5. Employee reporting to Money Laundering Reporting Officer

A Relevant Person must have policies, procedures, systems and controls to ensure that whenever any employee, acting in the ordinary course of his employment, either:

(a) knows;

(b) suspects; or

(c) has reasonable grounds for knowing or suspecting,

that a person is engaged in or attempting money laundering, that employeepromptly notifies the Relevant Person's MLRO and provides the MLRO with all relevant information within the employee's knowledge.

Guidance on Suspicious Transaction Reports

(a) Circumstances that might give rise to suspicion or reasonable grounds for suspicion include:

(i) Transactions which have no apparent purpose, which make no obvious economic sense, or which are designed or structured to avoid detection;

(ii) Transactions requested by a person without reasonable explanation, which are out of the ordinary range of services normally requested or are outside the experience of a Relevant Person in relation to a particular customer;

(iii) where the size or pattern of transactions, without reasonable explanation, is out of line with any pattern that has previously emerged or are deliberately structured to avoid detection;

(iv) where a customer refuses to provide the information requested without reasonable explanation;

(v) where a customer who has newly entered into a business relationship uses the relationship for a single transaction or for only a very short period of time;

(vi) an extensive use of offshore accounts, companies or structures in circumstances where the customer's economic needs do not support such requirements;

(vii) unnecessary routing of funds through third party accounts;

~~(viii)~~ the proffering of documents that appear fraudulent, unofficial, or are otherwise suspicious; ~~or~~

(ix) unusual transactions without an apparently profitable motive; or

(x) other circumstances as referred in national AML laws and regulations or as independently determined by the Relevant Person in accordance with its internal procedures.

(…)

13.8.3. Independence of Money Laundering Reporting Officer decision

(a) A Relevant Person must ensure that whether the MLRO decides to make or not to make a STR or TTR,his/her decision is made independently and is not subject to the consent or approval of any other person.

(b) Where a Relevant Person's MLRO has a suspicion of money laundering, and reasonably believes that performing the CDD process will tip-off the customer, he/she must not pursue the CDD process, and must submit a STR to the FIU.

(…)

14. GENERAL OBLIGATIONS

14.1. Training and Awareness

14.1.1. Training and Other Obligations

A Relevant Person must implement screening procedures to ensure high standards when hiring employees (Know Your Employee).

A Relevant Person must take appropriate measures to ensure that its employees:

(a) are made aware of the law relating to money laundering;

(b) are regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering;

(c) understand its policies, procedures, systems and controls related to money laundering and any changes to these;

(d) understand the types of activity that may constitute suspicious activity in the context of the business in which an employee is engaged and that may warrant a notification to the MLRO under AML 13.7.3.;

(e) understand its arrangements regarding the making of a notification to the MLRO under AML 13.7.3.;

(f) are aware of the prevailing techniques, methods and trends in money laundering relevant to the business of the Relevant Person;

(g) understand the risk of tipping-off and how to avoid informing a customer or potential customer that it is or may be the subject of a STR;

(h) understand the roles and responsibilities of employees in combating money laundering, including the identity and responsibility of the Relevant Person's MLRO and deputy, where applicable; and

(i) understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in Chapter 13.

(…)

14.4. Notifications

14.4.1. Notification obligation

A Relevant Person must inform the AFSA in writing quarterly about number, reasons, and outcomes ~~as soon as possible~~ if, in relation to its activities carried on as part of the AIFC or in relation to any of its branches or Subsidiaries, it:

(a) receives an ad-hoc (specific) request for providing detailed information as regards particular customer or transaction from a regulator or agency responsible for AML, CFT,

or sanctions compliance in ~~connection with~~ relation to potential money laundering or sanctions contravention[4];

(b) becomes aware, or has reasonable grounds to believe, that a money laundering event has occurred or may have occurred in or through its business;

(c) becomes aware of any money laundering or sanctions matter in relation to the Relevant Person or a member of its Group which could result in adverse reputational consequences to the Relevant Person; or

(d) becomes aware of a significant contravention of these Rules or a contravention of the relevant Kazakhstan legislation by the Relevant Person or any of its employees.

(…)

14.6. Audit

14.6.1. Audit obligation

An Authorised Person must ensure that its audit function, established under GEN 5.5.1 includes regular reviews and assessments (not less than once in two years) of the effectiveness of the Authorised Person's AML policies,procedures, systems and controls, and its compliance with its obligations in these Rules.

Guidance on audit

(a) The review and assessment undertaken for the purposes of AML 14.6.1. may be undertaken:

(i) internally by the Authorised Person's internal audit function; or

(ii) by a competent firm of independent auditors or compliance professionals.

(b) The review and assessment undertaken for the purposes of AML 14.6.1. should cover at least the following:

(i) sample testing of compliance with the Authorised Person's CDD arrangements;
(ii) the adequacy of the Authorised Person's AML/CFT Systems, ML/TF risk assessment framework and application of risk-based approach;
(iii) the effectiveness of the system for recognising and reporting suspicious transactions;

(iv) an analysis of all notifications made to the MLRO to highlight any area where procedures or training may need to be enhanced; ~~and~~

(v) a review of the nature and frequency of the dialogue between the senior management and the MLRO; and~~.~~
(vi) the level of awareness of staff having AML/CFT responsibilities

(…)

Annex 1

List of Defined Terms for AML Rules and associated guidelines and requirements

Definition	Interpretation
AML	for the purposes of these Rules means anti-money laundering

[4] Does not apply to the regular interaction between a reporting entity and FIU as regards technical issues related to filling out of F1.

AML Rules	for the purpose of these Rules means AIFC Anti-Money Laundering, Counter – Terrorist Financing and Sanctions Rules
AML Law	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
AIFC acts	AIFC acts adopted by the relevant decision-making body (Regulations, Rules, Guidance, etc.)
BURA	Business Risk Assessment
CFT	countering the financing of terrorism
CRA	Customer Risk Assessment
Criminal Code	Criminal Code of the Republic of Kazakhstan No 226-V dated 3 July 2014
geographic area (state or territory) considered to be an area of high risk	Geographic areas considered to be an area of high risk include: • countries or jurisdictions that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies; • countries or jurisdictions subject to sanctions, embargos or similar measures issued by UN, US, EU, UK; • countries or jurisdictions which are more vulnerable to corruption; • countries or jurisdictions that are believed to have strong links to terrorist activities. • countries known as tax heavens (offshore jurisdictions)
KYC	Know Your Customer, adequate customer identification procedures
KYE	Know Your Employee, adequate screening procedures to ensure high standards when hiring employees
money laundering	a reference to 'money laundering' also includes a reference to terrorist financing and financing the proliferation of weapons of mass destruction
sanctions violation	an action aimed the violation evasion or circumvention of EU, US, UK sanctions, such as but not limited to: • establishing relations with prohibited persons or entities, • breaching stipulated embargoes, • providing prohibited or restricted economic and financial services, • transferring, receiving funds or providing false information to conceal operations or funds that should be restricted or prohibited. • avoiding or circumventing sanctions
sanctions list	a list of all individuals, groups, and other entities sanctioned by the United Nations and FIU. This includes asset freezes, travel bans, and arms embargoes.
senior management	a high-level executive who oversees the operations and performance of one or more departments within a company
SOF	Source(s) of funds
SOW	Source(s) of wealth
tipping-off	to warn someone secretly about something that will happen, so that they can take action or prevent it from happening
TTR	Threshold Transaction Report
Transparency International	global civil society organisation leading the fight against corruption
UNSC	United Nations Security Council

watchlists	a set (database, register, list) of information on individuals, organisations, and countries that deserve special attention and appropriate actions, including lists of unilateral sanctions by jurisdictions or authorities (target, sanction, embargo)
Wolfsberg Group	an association of 12 global banks which aims to develop frameworks and guidance for the management of financial crime risks

Figure 1 – The Risk-Based Approach

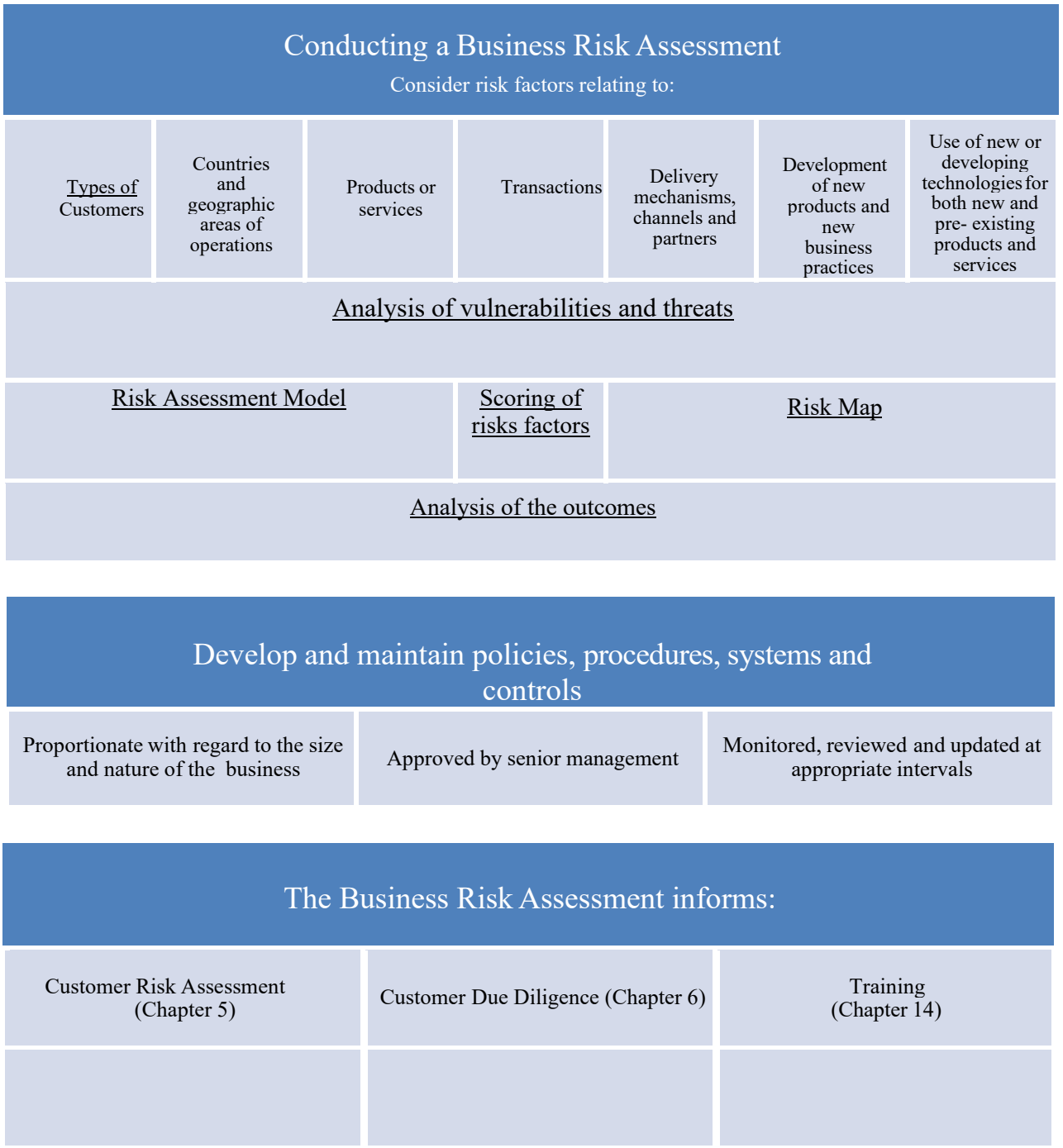

Figure 2 – Customer Risk Assessment