**Annex 2**

1. **RISK FACTORS IN BANKS**

**Risk factors that refer to the client**

1. When identifying the risk associated with the client, the bank shall take into account the risks associated with the activity or professional involvement of the client, his/her/its reputation, as well as the nature of his/her/its behavior.
2. The risk factors related to the activity or professional involvement of the client that the bank analyzes shall be the following:
* whether the client is associated with activities that are exposed to higher corruption risks, such as: construction, pharmacy, health, arms trade, defense, mining industry or public procurements;
* whether the client is associated with activities that are exposed to a higher risk of MLFT, such as: money transfer, organizers of games of chance or trade in precious metals;
* whether the client is associated with activities that involve significant amounts of cash as part of the regular operations (such as: restaurants, gas stations, licensed currency exchange operators, organizers of games of chance, etc.);
* whether the client trades in goods and services with great value (cars, art works, oil, precious metals, etc.) or value which is difficult to estimate (software, consulting services, market research, etc.);
* whether the client is a legal entity, what the purpose of its establishment is and what its activity is;
* whether the client and its beneficial owner are politically exposed persons or are close associates with politically exposed persons;
* whether the client is a legal entity with a disproportionately small number of employees in terms of the volume of activities and the activity it performs;
* whether the client is a legal entity that is required to disclose data which provide publicly available information about the beneficial owner of the client (such as: joint stock company whose shares are traded on a regulated market);
* whether the client is a bank or a payment institution operating in a country that has no efficient anti-MLFT system and that is not subject to supervision in terms of the obligation for anti-money laundering and financing of terrorism and
* whether the client is a bank or financial payment institution against which sanctions or other measures have been imposed by a competent authority in the past 5 years due to non-fulfillment of the obligations for anti-MLFT.
1. The risk factors related to the client's reputation that the bank analyzes shall be the following:
* whether there are negative information from credible and reliable media or other sources of information about the client, such as facts about crimes or links with terrorism or terrorism financing and proliferation. These facts do not require the adoption of an effective court decision;
* whether due to administrative or criminal proceedings or facts about terrorist activity or terrorism financing and proliferation, the assets of the client, its beneficial owner or of any person for whom it is known that he/she is closely related thereto, have been frozen or the bank has grounds for suspicion that the assets of the client are frozen;
* whether the bank has other negative information about the integrity of the client and its beneficial owner, which were obtained by the bank during the business relation.
1. The bank shall bear in mind that some of the risk factors related to the nature and behavior of the client or its beneficial owner cannot be determined when establishing the business relationship, i.e. they may arise once the business relation is established.
2. Risk factors related to the nature and behavior of the client that are analyzed by the bank shall be the following:
* whether the client has a complex ownership structure (more than two levels of legal entities in the ownership chain);
* whether the client issues bearer shares or has nominee shareholders;
* whether the ownership or management structure of the client changed more than three times in the last three years;
* whether there are frequent notifications (alert) on the client, indicating an existence of complex and unusual transactions;
* whether the client carries out transactions below the thresholds referred to in Article 13 paragraph (1) indent b) and c) and Article 64 of the Law on AMLCFT;
* whether the provided information about the source of wealth or the source of funds of the client is typical of that type of natural persons (such as: salary, inheritance, loans) or legal entities (such as: inflows related to the client's activity).

**Geographical risk factors**

1. When identifying the geographical risk factor, the bank shall take into account the risks associated with the head office/residence of the client, his/her/its activity/profession, the purpose and nature of the business relation, the effectiveness of the anti-MLFT system and the level of transparency and tax discipline of the country in which the client and its beneficial owner have their own head office/residence.
2. When identifying the geographical risk, the bank shall analyze the risks associated with the countries and geographical locations in which the client and its beneficial owner:
* have their own head office or residence;
* have a geographical location where they predominantly perform their activity;
* have significant business activities.
1. When assessing the geographical risk, the bank shall take into account the nature and purpose of the business relation of the client, for example:
* when it comes to transactions with high-risk countries;
* when the bank’s client is another bank or payment institution, the bank shall analyze the appropriateness of the anti-MLFT system in the country in which this client has a head office;
* when the client is a subject to legal entity, the entity shall analyze the degree of meeting the international standards for tax transparency in the country where the client and its beneficial owner are registered/have their own residence;
* the beneficial owner of the client has his/her own residence in a high-risk country (offshore financial center, tax haven, state under sanctions);
* whether the client is a government body or legal entity from a highly corrupt country (for example: according to the Transparency International index“).
1. The sources of information for determining the effectiveness of the anti-MLFT system in a particular country shall include: the high-risk countries determined by the National MLFT Risk Assessment of the Republic of North Macedonia, the FATF assessment reports or other regional bodies similar to the FATF; the FATF list of high-risk countries, etc.
2. The sources of information that the bank takes into account when determining the level of risk of terrorism financing and proliferation related to a particular country shall be the following:
* information from authorities competent for criminal prosecution or other information from commercial data bases whether that country finances or supports terrorist activity and
* information whether that country is subject to international restrictive measures related to money laundering, terrorism, terrorism financing or armaments established by the UN or the European Union.

1. The sources of information that the bank analyzes when determining the level of transparency and tax discipline of the countries shall be the following:
* information from multiple reliable sources that the country is complied with the international tax transparency and exchange of information standards, as well as evidence that these rules are properly applied in practice;
* Reports from the Global Forum on Transparency and Exchange of Information for Tax Purposes by the OECD, where the countries are assessed for the purposes of tax transparency and exchange of information;
* assessing compliance with the FATF recommendations or the regional bodies within FATF, as well as IMF assessments and
* information whether the country has established registries of beneficial owners and account registries for the needs of the entities and government bodies.

**Risk factors that refer to products, services or transactions offered by the bank**

1. The risk factors that the bank analyzes when identifying the risks associated with products, services or transactions shall be the following:
* the degree of anonymity of products, services or transactions;
* the complexity of products, services or transactions;
* the value or scope of products, services or transactions.
1. the risk factor that the bank analyzes when identifying the risks associated with the anonymity of a particular product, service or transaction is the extent to which a product or service ensures anonymity or facilitates the concealment of the identity of the client or beneficial owner (such as: anonymous accounts, virtual assets, etc.)
2. The risk factors that the bank analyzes when identifying the risks associated with the complexity of a particular product, service or transaction shall be the following:
* the degree of complexity of a particular transaction and involvement of multiple clients or countries;
* whether the bank has knowledge of the risks when launching a new product or service, especially when it involves using new technologies or payment methods.
1. The risk factors that the bank analyzes when identifying the risk associated with the value or size of a particular product, service or transaction shall be the following:
* the extent to which products or services enable using cash;
* the extent to which products or services facilitate or encourage the high value transactions;
* the existence of certain limitations in terms of the maximum value of the transaction or of the price of the service which would limit the use of products or services for the purposes of MLFT.

**Risk factors that refer to distribution channels**

1. When identifying the risk associated with the manner in which products or services are delivered to the client, the bank shall analyze the risk when the client is not physically present and conducts an analysis of the nature of the business relation between the intermediary and the entity.
2. Risk factors that are considered when identifying the risks associated with the distribution channels shall be the following:
* client’s presence or absence;
* application of new technologies such as: m-commerce; using virtual assets, for example bitcoin (based on the method of consecutive execution of transactions); payment over the Internet - “PayPal”, “Amazon Pay”, “Google Wallet”, etc.
1. **RISK FACTORS IN PAYMENT INSTUTIONS**
2. When identifying the inherent risk level, the payment institution shall take into account at least the following factors:
* the type and size of payment institution, including the number of subsidies and agents, as well as type of products and services offered to clients;
* the predominant role of cash transactions in the variety of offered services;
* the predominant role of temporary transactions in establishing a business relationship;
* whether the payment institution’s head office is in a high-risk country;
* the large volume of transactions;
* the use of new technologies in establishing non-face-to-face business relationship and
* distribution channels (agent network)

**Risk factors that refer to the client**

1. Regarding the risks associated to clients at least the following risk factors shall be taken into account:
* number of politically exposed persons;
* non-resident natural persons clients and
* legal entities clients (organizers of games of chance and virtual assets service providers).

**Geographical risk factors**

1. Regarding the geographical risk, at least the following risk factors shall be taken into account:
* customers with residence/address in high-risk countries and/or who execute transactions with high-risk countries;
* countries with a high level of organized crime, corruption, drug trafficking, human trafficking etc.;
* countries under sanctions, embargoes and other measures of international organizations
* countries with strategic deficiencies identified by the FATF.
1. Regarding the products and services, at least the following risk factors shall be taken into account:
* the use of new technologies (establishing non-face-to-face business relationship and trade in virtual assets);
* the use of cash and
* execution of temporary transactions.

**Risk factors that refer to products and services**

1. Regarding the use of intermediaries (agents), the risk factor when one agent cooperates with multiple payment institutions shall be taken into account.

**Risk factors that refer to distribution channels**

1. Regarding the distribution channel, the number of agents that deliver the service to the customer shall be taken into account.
2. **RISK ASSESSMENT OF LICENSED CURRENCY EXCHANGE OFFICES**
3. The provisions of item 2 paragraph 1 indents 1, 2, 3, 4 and 6; item 3; item 5 paragraph 1 indents 4, 5 and 6; item 7 paragraph 1 indent 1; item 9; item 10, item 12 paragraph 1 indent 3 and item 15 paragraph 1 indent 1 of these Annex, that refer to natural persons/customers shall be properly applied by the licensed currency exchange operator in the area of executing occasional transactions and monitoring the business relation with the customer.
4. When determining the vulnerability arising from the content of internal regulations (policies and procedures), one shall take into account:
* the procedures for identifying the natural person by prescribing the minimum documentation required for identifying the natural person in the moment of execution of the transaction;
* in the event when the licensed currency exchange operator has a business relation with the customer, the procedures shall include an appropriate type of data that show whether the customer’s transactions are in accordance with the purpose of the business relation, the customer’s risk profile, his/her financial condition and his/her sources of financing (such as: the profession of the customer, the employer, the amount of the monthly wage, etc.).
1. The vulnerability arising from the activities of the person authorized for prevention of MLFT shall include:
* identification and verification of the identity of the natural person by applying the standard documents for identification of natural persons specified by the Law on AMLCFT and verification of the identity of the natural person by using data and information from reliable and independent sources;
* permanent insight into the numbered register in order to determine the frequency of execution of transactions by a particular natural person, in order to require from him/her to submit additional documentation that will determine the purpose of execution of the transaction and its economic justification;
* client due diligence (in case of an existence of a business relationship or in case of an occurrence of suspicious activity indicators) by gathering information on his/her profession, the source of his/her assets, the economic justification of the executed transaction, etc.;
* The Financial Intelligence Office shall be notified of cash, connected and suspicious transactions in a manner and deadlines specified by the Law on AMLCFT. The notification on suspicious transactions shall be documented, appropriately elaborated and supported by the indicators for identifying suspicious transactions adopted by the Financial Intelligence Office.
1. The vulnerability arising from the internal control systems shall include the following:
* in the event when the natural person is a politically exposed person, the licensed currency exchange operator shall take the measures of enhanced due diligence specified by the Law on AMLCFT and shall assign a high risk level to the natural person;
* in the event when the natural person has residence in a high-risk country, the licensed currency exchange operator shall take the measures of enhanced due diligence specified by the Law on AMLCFT and shall assign a high risk level to the natural person;
* implementation of the restrictive measures in accordance with the regulations that regulate the international and national restrictive measures;
* the training of staff shall be adequate to the nature of the activity of the licensed currency exchange operator, adjusted to the type of clients and contain all the relevant provisions of the Law on AMLCFT and bylaws that regulate this matter.
* the Internal Audit Department or the person authorized for internal audit shall analyze and test the adequacy of written policies and procedures; select a sample of clients, thus testing the appropriateness of the due diligence of the clients and their risk profile, as well as the submission of reports to the Financial Intelligence Office; reporting to the responsible person of the licensed currency exchange operator on the findings of the controls, etc.
1. The entity shall establish a record system for identifying connected transaction when transactions that exceed 500 euros are made in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia. Regarding the record system, the entity shall apply client due diligence and monitor transactions.

When monitoring transactions referred to in paragraph 1 of this item, the entity shall establish and use a list of indicators for identifying suspicious transactions.

1. **RISK ASSESSMENT OF TERORIST AND PROLIFERATION FINANCING**
2. When identifying the risk of terrorist and proliferation financing, the entity shall take into account at least the following risk factors:

a) Regarding the client as a risk factor, the following elements shall be taken into account:

* residential status (resident and non-resident),
* high-risk category of clients (non-face-to-face business relationship, politically exposed persons, correspondent banks and payment institutions, non-profit organizations, clients who are based or reside in high-risk countries),
* number of clients reported to the Financial Intelligence Office on suspicious transaction for terrorist financing,
* clients and/or their beneficial owner which are on the list of sanctions and
* the rejected business relationship.

b) Regarding the geographical risk, the following elements shall be taken into account:

* countries at war or countries where terrorist activities occur,
* Borderlands of countries with a neighboring country at war or countries where terrorist activities occur,
* countries where recruitments for foreign terrorist fighters are carried out.

c) Regarding the risk of products, services or transactions, the following elements shall be taken into account:

* cash and cashless transactions,
* domestic and international payment operations
* transactions with high-risk countries (inflows and outflows),
* transactions of non-profit organizations,
* rejected and withheld transactions,
* transactions executed through a payment institution;

d) Regarding the risk of distribution channels, the following elements shall be taken into account:

* transactions executed through a payment institution agent
* e-banking transactions and
* m-commerce transactions.
1. The entity shall identify the vulnerability by providing information on the sources of terrorist and proliferation financing risks and undertake appropriate measures to mitigate them. The risk mitigating measures shall include at least the following:

a) well defined risk appetite and appropriate client acceptance policies (including their beneficial owners);

b) appropriate procedures for enhanced client due diligence;

c) regular updating of data and client documents;

d) effectiveness of the internal procedure for monitoring the lists of sanctions and

e) appropriate software which will enable implementation of the restrictive measures by the entity.

1. Before establishing the business relationship, i.e. before executing occasional transaction, as well as during the implementation of measures and activities for permanent business relationship monitoring, the entity shall be obliged to check whether the potential or current clients (including their beneficiary owners) are on the lists of sanctions.
2. The entity shall be obliged to apply the restrictive measures in accordance with the legal regulations, i.e. to prohibit, immediately and without prior notice, the use, transfer, conversion or any other dispose of property, to prohibit allowing direct or indirect dispose of any property, as well as to prohibit establishment or continuation of business relationship for all natural and legal entities (including their beneficiary owners) which are on sanctions list.

The obligation of the entity referred to in paragraph 1 of this item shall refer to the overall funds owned or controlled by persons on sanctions lists, not only those that could be linked to a particular terrorist act, conspiracy or threat.

1. The entity shall undertake activities to suspend the financial measure against terrorism and/or proliferation after the announcement of the decision repealing the financial measure against terrorism and/or proliferation adopted by the Government of the Republic of North Macedonia.