IQ NET OÜ
7-208, Tornimae, Kesklina linnaosa
Harju maakond, Tallinn, Estonia

Rules on risk analysis for the prevention of money laundering and terrorist financing

IQ NET OÜ
7-208, Tornimae, Kesklina linnaosa
Harju maakond, Tallinn, Estonia

In line with Money Laundering and Terrorist Financing Prevention Act of Republic of Estonia, Payment Institution and E-money Institution Act of Republic of Estonia and Advisory Guidelines of Estonian Financial Supervision Authority - Organizational solutions and preventive measures for credit and financial institutions to take against money laundering and terrorist financing, the management board of the IQ Net OU (the "Company") adopts Rules on risk analysis for the prevention of money laundering and terrorist financing as follows:

1. Criteria phrases

In determining the risk assessment of a particular customer, business relationship, product or transaction, the company should take into account the following criteria:

1.1. type, business profile and the ownership structure of the customer;
1.2. the geographical origin of the customer;
1.3. the nature of the business relationship, product or transaction;
1.4. past experiences with the customer;
1.5. the presence of the customer at the conclusion of a business relationship or the execution of transactions, taking into account the use of new technologies enabling anonymity (eg. e-banking)
1.6. other information indicating that customer, business relationship, product or transaction may be more risky.

2. Categories of risk

Based on the risk factors business relationship and transaction fall into three main categories of risk:

2.1. High risk

Customers who fall into the category of high risk are:

1) customers whose source of funds is unknown or unclear;

2) customers that are suspected of not acting on their own account, or to carry out the instructions of a third party;

3) customers whose business activity or transaction are not carried out under normal circumstances, especially taking into account its basis, amount and manner of execution, purpose and the like. Or by which is meant:

- Significant and unexpected geographical distance between customer locations and organizational units of the taxpayer in which the customer is establishing a business relationship or perform the transaction;

- Often unexpectedly establishment, without economic justification, business relationships with more similar types of participants in the market, such as opening an account with more participants in the market, the conclusion of the contract more in a shorter period of time, etc .;

- Frequent transfers of funds from one account to another;

- Close the account immediately after the conclusion of the contract;

- Request that the funds accumulated in the individual account customer payments on the current account of a third party or on behalf of the person in the territory of which do not apply strict standards in the area of money laundering and financing of terrorism;

- Insistence on the confidentiality of transactions and the like.

4) customers where, because of the structure, legal form or complex and ambiguous relationships, difficult to determine the identity of their beneficial owners, such as offshore entities with unclear ownership structure and which has not established a company from a country that applies standards area of money laundering and financing of terrorism, which are up to the standards prescribed by the Act;

5) Customers who carry out activities which are characterized by large trade (eg. Carriers of goods and passengers);

6) side arms dealers and manufacturers of weapons;

7) customers representing persons who are in business (lawyers, accountants or other professional representatives), especially when the company is in contact only with the representatives;

8) sports society;

9) construction companies;

10) company with disproportionately small number of employees in relation to the volume of work they perform, which do not have their own infrastructure, business premises and other;

11) customers (natural or legal persons) that are on the list of persons against whom the effective measures of the United Nations or the Council of Europe;

12) customers residing or established in the entities that are not subject to international law, that is not internationally recognized as states (such entities give the possibility of fictitious registration of the legal entity, allowing the issuance of fictitious identification documents, etc.);

13) customers whose bid to establish a business relationship refused other covered by the law, no matter how learned of this fact, or a person who has a bad reputation;

14) The customer is a politically exposed person;

15) The customer is a foreign legal entity that does not conduct or which is prohibited from performing commercial, manufacturing or other activities in the country where it is registered (it is a legal entity based in the country which is known as off-shore financial center, and to whom certain restrictions apply with immediate performance of registered activities in that country);

16) The customer is a fiduciary or other similar foreign law firm with unknown or hidden owners or management;

17) customer that has a complex ownership structure or complex chain of ownership (complex ownership structure or complex chain of ownership that makes it difficult determining the beneficial owner of the customer, or the person who indirectly provides property assets, based on which has the ability to control, and which can direct or otherwise significantly influence management decisions when deciding on funding and operations);

18) customer to perform their activities should not be, and is not obliged to obtain a license appropriate supervisory body, ie, in accordance with the legislation of the parent, not the subject of the measures in the area of money laundering and financing of terrorism;

19) The customer is a non-profit organization (institution, company or other legal entity, or an entity that does not conduct economic activity) and meet one of the following conditions:

- Is based in a country that is known as offshore financial center;
- Is based in a country that is known as financial or tax haven;
- Is based in a country that is not a signatory to the Agreement on the Establishment of the EU;
- Among its members or founders of a natural or legal person who is a resident of any of the aforementioned countries;

20) The customer is a foreign legal entity, established by issuing securities to bearer.

Business relationships, transactions or products that fall into the category of high risk are:

1) transactions which significantly deviate from the standard way of execution of the transaction;
2) transactions that have no economic justification);
3) transactions are conducted in a manner that avoids the standard and usual methods of control;
4) transactions involving several participants without clear economic reasons, more interconnected transactions carried out in the short term or in the longer intervals in succession, in an amount below the limit for reporting to the Administration;
5) loans to legal entities and, in particular, loans to the founders of foreign legal entity in the country;
6) transactions where the customer apparently concealing the true basis and reason for the implementation of the transaction;
7) payment for services for which there is no market value or determinable price;
8) transactions in which the customer refuses to deliver documentation;
9) transactions where the documentation does not match the customer transactions;
10) transactions in which the source of funds is unclear or cannot be determined their relationship with the business of the customer;
11) products or transactions that might favor anonymity, such as using the services of custody;
12) announced a block trade actions, particularly when such customers appear newly created companies or companies registered in offshore destinations;
14) payment transactions services partners customer who come from off-shore areas, and from records show that the funds come from the neighboring countries;
15) transactions that were designed to persons who have been in force measures the United Nations and the Council of Europe;
16) transactions that the customer performed on behalf and for the account of a person against whom the force action of the United Nations or the Council of Europe;
17) transactions for which payment is made of funds from the account of the customer, or the payment of funds to the account of the customer, which is different from the account that the customer stated in the determination of identification, that is, through which normally operates or operated (particularly in the case of transaction abroad);
18) payments received from third parties not connected with the payment;
19) transactions intended for persons residing or established in the country which is known as financial or tax haven;
20) transactions intended for persons residing or established in the country which is known as offshore financial center;
21) transactions intended to non-profit organizations headquartered in the state known as offshore financial center;
22) business relationships involving regular or large payments from and / or to the customer's account which was opened in credit or financial institution a country outside the European Union, or business relations, which in its own name and for the account of the customer, as a proxy assemblies or carry out foreign credit or other fiduciary institutions based in the country outside the European Union;
23) business relationships coupled unattended customer in the taxpayer, and in respect of which have not been met for the implementation of simplified customer verification; and
24) new products and new jobs, including new delivery mechanisms, and the use of new technologies, development of new and old products.

Countries or geographic areas that fall into the category of high risk are:

1) which state that the United Nations, the Council of Europe or other credible international organizations apply sanctions, embargoes or similar measures;

2) countries that have been marked by the Working Group on financial measures against money laundering (referred to as the FATF), or other credible international organizations, as well as those who finance or provide support to terrorist activities, as well as those that have a certain terrorist organization operating therein;

3) states that have been marked by the FATF or other credible international organizations, as well as those that fail to apply adequate measures to prevent money laundering and terrorist financing;

4) states that have been marked by the FATF or other credible international organizations, as countries lacking internationally recognized standard for the prevention and detection of money laundering and financing of terrorism;

5) states that, based on estimates of credible international organizations, designated as a state with a high level of organized crime for trafficking in arms, narcotics, human trafficking and other criminal activities;

6) states that, on the basis of credible estimates of international organizations, established a high level of corruption and human rights violations;

7) state that, in the assessment of international organizations (FATF, the Council of Europe and others.), Classified among non-cooperative countries or territories; and

8) states that represent off-shore areas.

Information on high-risk countries can be obtained on the website of MONEYVAL, http://www.coe.int/t/dghl/monitoring/moneyval/, and FATF, http://www.fatf-gafi.org /.

As a competent international organizations to monitor the effectiveness of the implementation of measures in the field of prevention of money laundering and financing of terrorism with the provisions of international standards, the bond should be treated following international organizations:

- European Central Bank;
- Committee of the European Commission's anti-money laundering and terrorist financing,
- FATF;
- The International Monetary Fund;
- World Bank;
- International Association of Financial supervisory bodies concerned with detecting and preventing money laundering and terrorist financing - Financial Intelligence Group (Egmont Group);
- A special committee of experts of the Council of Europe for evaluation of measures for detecting and preventing money laundering and financing of terrorism (MONEYVAL);
- International Organization of Securities Commissions (IOSCO);
- European supervisory body for the securities and capital markets (ESMA);
- European supervisory authority for the insurance and pension insurance (EIOPA);
- International Association of Insurance Supervisors (IAIS); and
- European supervisory authority for the banking (EBA).

2.2. Medium risk

Company categorizes as medium risk that customer, business relationship, product or transaction which is the basis of the criteria set out in the Guidelines and risk factors can be categorized as high or low risk.

2.3. Slight risk

Customers who fall into the category of slight risk are:
1) The taxpayer referred to in Article 4 paragraph 2 items. 1, 2, 4, 5, 6, 9 and 11 of the Act or other relevant institutions based in the EU or a country from the list of countries which apply international standards in the field of prevention of money laundering and financing of terrorism, which are up to the standards of the European Union or higher;
2) state authority or local government body or other legal entity exercising public authority;
3) by a company whose stocks are admitted to trading on a regulated market or stock markets in countries that are members of the European Union or other countries in which the markets apply international standards that are at the level of European Union standards or higher;
4) a company or other form of business organization exercising public authority, which is listed on the stock exchange and which are obliged to submit information to the Stock Exchange rules or in accordance with the regulations which introduced the obligation of transparency of the actual owner of that company;
5) the geographical area which falls within less risky.

Business relationships, transactions or products that fall into the category of slight risk are:
1) life insurance policies where the premiums low;
2) savings in pension plans if there is a possibility of early raising savings and where savings can not be used as collateral;
3) pension and other plans that provide retirement income, in cases in which contributions are provided by deducting from earnings and whose rules are not allowed to transfer the yield of members;
4) financial products and institutions that provide identified and limited to a specific type of customer, in order to increase access to financial inclusion;
5) products in which the risk of money laundering and terrorist financing depends on other factors, such as restrictions on the amount of electronic money or transparency of ownership.

Countries or geographic areas that fall into the category of slight risk are:
1) Member States of the European Union;
2) countries that have an efficient system of combating money laundering and financing of terrorism, recognized by the FATF;
3) state with recognized low level of corruption and other criminal activities; and
4) states that implement the recommendations of FATF to combat money laundering and financing of terrorism and for which the controlled compliance with these recommendations.

3. Determination of risk

Company is required to identify and verify the identity of the customer (natural person/legal entity), its agent, the beneficial owner of the customer (for legal entities) and other persons authorized by the customer to represent him before the taxpayer, in the manner prescribed by law.

Company is obliged to implement the measures of establishing and verifying the identity of the customer and monitoring of customer's business as stipulated in all cases prescribed by law.

The company has a solution for automated verification of the authenticity of photos and scanned copies of physical check documents. The company has a solution for automated tracking and monitoring of all transactions.

3.1. Identifying the beneficial owner

The concept of beneficial owner is defined by law and the manner of determining the real owner is set out by law. The company sets terms, requirements and conditions on which the company is able to verify an individual's identity information for lawful purposes of identity verification, fraud prevention or enforcement of laws designed to prevent money laundering.

3.2. Special forms of verification and monitoring of customer's business

There are special forms of verification and monitoring of customer's business, such as:

- deepened verification and monitoring of customer's business; and
- simplified checking and monitoring of customer's business.

a) Enhanced verification and monitoring of customer's business

Politically exposed person

Before establishing a business relationship with a customer is a politically exposed person or customer whose real owner is a politically exposed person, the employees of reporting entities are required to obtain written consent of the senior manager, and if the business relationship is already established, it is necessary to obtain the written consent of senior managers to set business relations.

In order to identify politically exposed persons, payers are required to:

- require the customer fill out a form for politically exposed persons;
- to collect information from public sources;
- collect information on the basis of the database containing the list of politically exposed persons (eg. A list of politically exposed persons on the website of the Board, World Check PEP List, etc.).
- to collect information on the basis of the records of the Commission for prevention of conflict of interest.

In the event that, when completing this form for politically exposed persons, the customer does not respond as a politically exposed person, the obligor shall, on the basis of the above modes, check

whether the customer is a politically exposed person, and if it turns out it is, take measures deepened verification and monitoring operations.

After establishing a business relationship with a politically exposed person, the company is obliged to keep separate records on the persons and transactions that are concluded in the name and on behalf of such persons, in electronic form.

After obtaining the consent of the senior manager for the establishment or continuation of a business relationship with a politically exposed person, the employees of reporting entities are not required to obtain approval from senior manager to take each individual transaction performed for politically exposed persons. However, employees of reporting entities are required to give special attention to transactions and other business activities with the obligor by a politically exposed person, and, if necessary, on these transactions inform the authorized person as soon as possible.

b) simplified checking and monitoring of customer's business

Company may carry out measures of simplified verification and monitoring of customer's business. These cases relate to customers, business relationships, transactions or products for which the taxpayer is found to belong to the category with slight risk.

4. Monitoring of accounts and transactions

Company is obliged to continuously supervise the accounts and transactions to prevent money laundering and terrorist financing. Company is obliged to provide that after the customer deposits fiat money for buying cryptocurrency on the Company's account, that cryptocurrency is settled the same banking day to customers account. Company can effectively control and reduce the risk only if there is information on the operations of the customer to be able to identify the transaction in accordance with the customer's profile. In this sense, the company is required to establish appropriate procedures for regular and careful monitoring of business activities of the customer. Company should particularly pay attention to all complex, unusually large transactions and all unusual customer activity which have no apparent economic purpose. The subject of intensive control the accounts and transactions associated with customers who are included in the high risk category for which the company has defined key performance indicators, such as the origin of funds, type of activity, place of business and more.

The supervision of the accounts and transactions of customers depending on the risk category:

- the category of high risk - at least quarterly;
- the category of medium risk - at least twice a year; and
- category with a slight risk - at least once a year.

Company is required to actively monitor customer transactions carried out during the business relationship for the sake of verifying the transaction of the customer, the type of work, source of funds, purpose and intended nature of the business relationship or transaction.
Measures for monitoring business activity in particular include:

- verification of compliance with the customer's business nature and purpose of the contractual relationship;

- monitoring and verification of compliance of customer business with its usual scope of business;
- monitoring and regularly update documents and customer data, which includes conducting repeated annual control of customer.

5. Managing the risks of money laundering and terrorist financing

Company is obliged to continuously manage the risks of money laundering and terrorist financing which it is exposed in its operations. In this sense the company is required to determine those areas of business that are considering the possibility of money laundering and terrorist financing more or less risky, and to establish and determine the major risks in these areas and measures to address them.

The system for managing risk of money laundering and terrorist financing, includes at least:

- developed processes for risk management;
- clearly defined powers and responsibilities for risk management;
- an effective and reliable system of information technology;
- the manner and timing of reporting and management information the company risk management.

System for risk management of money laundering and terrorist financing is provided:

- identification of risks;
- risk assessment;
- monitoring and analyzing risk;
- controlling risks;
- taking measures and minimize the risk; and
- informing the supervisory authority.

6. Internal Control

The Company performs an annual audit the accuracy and efficiency of implementation of risk analysis in the context of internal controls in the area of money laundering and terrorist financing. The purpose of internal control is to detect and correct deficiencies in the assessment and evaluation of risk factors for money laundering or terrorist financing.

This ordinance shall take effect and be implemented from the date of 31.05.2018. year.

Last reviewed on the 01.07.2021.