



Pursuant to Article 35, paragraph 1, sub-paragraph 1.1 of the Law No. 03/L209 on the Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No. 77/16 August 2010), Prishtina), amended and supplemented by Law No. 05/L-150 (Official Gazette of the Republic of Kosovo, No. 10 / 03 April 2017, Prishtina), Article 85, paragraph 1 of the Law No. 04/L-093 on Banks, Microfinance Institutions and Non-Bank Financial Institutions (Official Gazette of the Republic of Kosovo No. 11 / 11 May 11 2012, Prishtina), Article 4 paragraph 3, of Law No. 05/L-045 on Insurances (Official Gazette of the Republic of Kosovo No. 38 / 24 December 2015, Prishtina), as well as Article 66, paragraph 2, of Law No. 05/L-096 on the Prevention of Money Laundering and Combating Terrorist Financing (Official Gazette of the Republic of Kosovo No. 18 / 15 June 2016, Prishtina), the Board of the Central Bank, in the meeting held on 26 June 2024, approved the following:

REGULATION ON PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

CHAPTER I General provisions

Article 1 Purpose

The purpose of this Regulation is to define the criteria and procedures required for managing the process of prevention of money laundering and terrorist financing in compliance with the Law No. 05/L096 on the Prevention of Money Laundering and Combating Financing of Terrorism.

Article 2 Scope

This Regulation shall apply to all banks, branches of foreign banks, microfinance institutions, non-bank financial institutions, payment service providers, insurers and currency exchange offices (hereinafter for the purposes of this regulation referred to as financial institutions).

Article 3 Definitions

1. All terms used in this Regulation shall have the same meaning with the terms defined in the Law on the Prevention of Money Laundering and Combating the Financing of Terrorism (hereinafter – Law on PML/CFT) and/or with the following definitions for the purpose of this Regulation:
 - 1.1. **Senior Manager** – shall mean senior manager as defined in the Law on Banks, Microfinance

Institutions and Non-Bank Financial Institutions (hereinafter the Law on Banks).

- 1.2. **Financial services** – shall mean financial activities as defined in the Law on Banks, Law No. 05/L-045 on Insurances and as described in the definition of “financial institution” in the Law on PML/CFT.
- 1.3. **FIU-K** – Financial Intelligence Unit of the Republic of Kosovo.
- 1.4. **Shell bank** – shall mean a bank, or an institution engaged in equivalent activities, established in a country where it has no physical presence, which makes possible to exercise an actual direction and management without being affiliated with any regulated financial group.
- 1.5. **Payment through account** – shall mean correspondent accounts where respondent banks allow direct access for clients of the correspondent bank.
- 1.6. **Resident** – shall mean a natural person who has a principal residence in Kosovo or is physically present in Kosovo for more than one hundred and eighty-three (183) days in any twelve (12) month period of time.

CHAPTER II

Requirements and compliance with PML/CFT

Article 4

Responsibilities of Financial Institutions

1. For the purpose of Preventing Money Laundering and Combating Financing of Terrorism (hereinafter PML/CFT), the Board of Directors of financial institutions within the program for PML/CFT, shall:
 - 1.1. adopt effective PML/CFT policies;
 - 1.2. ensure that the PML/CFT policies and procedures are fully implemented in practice;
 - 1.3. appoint and dismiss the Head of PML/CFT Function who will assume the responsibility of “compliance officer” according to the Article 21 of the Law on PML/CFT. In case of branches of foreign financial institutions, the Board of Directors of Financial Institution which operates through the branch in Kosovo shall appoint or dismiss the Head of PML/CFT Function, in consultation with senior management of the branch in Kosovo.
 - 1.4. ensure that internal PML/CFT function is technically equipped and staffed with personnel who have full knowledge of PML/CFT policies and procedures, as well as possessing high ethical standards and relevant expertise;
 - 1.5. adopt a policy on establishing and maintaining business relationships, particularly those involving higher risk, including politically exposed persons and for this purpose develop effective risk-sensitive procedures for receiving and removing customers, products and services;
 - 1.6. determine risk policies related to the money laundering and terrorist financing, including risk acceptance and management;
 - 1.7. adopt the policy for accepting customers within the institution risk management;

- 1.8. take decisions on issues referred to the field of their operational responsibility in compliance with the provisions of this Regulation.
- 1.9. receive and discuss the internal audit reports regarding PML/CFT policies and procedures implementation;
- 1.10. adopt such other measures as may be required from time to time by the relevant institutions.
2. Financial institutions management shall be responsible for:
 - 2.1. adopting procedures for implementation of PML/CFT policies;
 - 2.2. ensuring compliance with the procedures for prevention of money laundering and terrorist financing in those fields of the institution for which they are responsible;
 - 2.3. ensuring effective implementation of all PML/CFT policies and procedures on daily basis;
 - 2.4. provide in due time the Head of the PML/CFT Function, the appropriate assistance and the necessary information for the purpose of exercising the tasks and responsibilities for PML/CFT.
3. All employees of the financial institution shall be trained and informed:
 - 3.1. to be vigilant against the possibility of institution products and services being used for money laundering and terrorist financing;
 - 3.2. on the manner on how to report to the Head of PML/CFT Function all transactions, actions or persons suspected for money laundering or terrorist financing and transaction in the amount determined in Article 26 of the Law on PML/CFT. In case of absence of the Head of PML/CFT Function, they shall report to his/her Deputy, as determined in Article 21 of the Law on PML/CFT.
 - 3.3. to effectively implement procedures of prevention of money laundering and combating terrorist financing, as determined in the Law on PML/CFT, this Regulation, and internal policies and procedures of their institution, especially customer due diligence, continuous monitoring of transactions and data retention; and
 - 3.4. to actively participate in training sessions and awareness-raising sessions provided by the financial institution.
4. For financial institutions which by the nature of their organization have not established Board of Directors, obligations according to this Regulation shall be fulfilled by the Management.

Article 5
Program for PML/CFT

1. Financial institutions shall draft and maintain a PML/CFT program with risk-based approach.
2. The main purpose of the PML/CFT program is to identify, reduce and manage the risk that the provision of a particular service by a financial institution may, intentionally or unintentionally, involve or facilitate money laundering or terrorist financing.
3. PML/CFT program shall determine customer identification and due diligence procedures for financial institution's customers.

4. Commonly referred to as the four pillars, the basic elements that must be addressed in a PML/CFT program are:
 - 4.1. policies, procedures and internal controls for PML/CFT (first line of defense)
 - 4.2. compliance function for PML/CFT and the head of the function (second line of defense).
 - 4.3. the program for the continuous training of employees and
 - 4.4. an independent ongoing audit function to test the overall effectiveness of the PML/CFT program (the third line of defense).

Article 6
Internal PML/CFT function

1. Financial institutions shall appoint a qualified individual with relevant experience as Head of Compliance who will act as the responsible compliance person in accordance with the Law on PML/CFT and paragraphs 2 and 3 of this Article, and this shall be considered as a minimal criterion for compliance with this Regulation. Financial institutions may set up the PML/CFT compliance function to a higher level in their organizational structure, provided that the function maintains its independence.
2. Banks shall establish the internal PML/CFT function which shall be independent of other functions within the bank and is led by senior manager who shall directly report to the Chief Executive Officer and on periodic basis to the Board of Directors in compliance with the conditions and procedures established under this Regulation.
3. The Head of Internal PML/CFT Function, when performing his/her duties, shall have:
 - 3.1. full and unlimited access to all data, records, documentation and information of the bank or financial institution;
 - 3.2. necessary human resources based on the size of the financial institution;
 - 3.3. necessary IT materials and equipment and working space necessary and appropriate to fulfil obligations deriving from the Law on PML/CFT and this Regulation;
 - 3.4. technical conditions for an appropriate level of protection for the data that are confidential and accessible for compliance officers;
 - 3.5. ongoing professional training in the field of PML/CFT;
 - 3.6. protection in relation to the disclosure of their data to unauthorized persons
4. A person cannot not be Head of PML/CFT Function if he/she is:
 - 4.1. not a resident person in Kosovo;
 - 4.2. a member of board of directors, executive director or holds any other standing position in the financial institution that may be in conflict with the his/her role as head of unit;
 - 4.3. employed in the financial institution dealing within the internal audit;
 - 4.4. employed in the financial institution responsible for controlling activities and operational monitoring.

5. PML/CFT Compliance Function at exchange offices may be exercised by the Director of Exchange Office, unless the latter designates another person to exercise this function.
6. For banks, Head of the Internal PML/CFT Function shall be considered as a senior manager in compliance with the Law on Banks.
7. Financial institutions shall notify the FIU-K and CBK for appointment of the Head of PML/CFT Function within the legal time limits set in the paragraph 8 of Article 21 of the Law on PML/CFT.
8. On the occasion of removal of the Head of Internal PML/CFT Function – financial institutions shall notify FIU-K and CBK within the legal time limits determined in paragraph 8 of Article 21 of the Law on PML/CFT, explaining the reasons for his/her dismissal.
9. Internal PML/CFT Function of financial institution shall advise and assist the Board of Directors and Senior Management in implementing the applicable legislation for PML/CFT. This function shall be coordinator or responsible for, among others:
 - 9.1. preparing internal PML/CFT policies and procedures according to Article 5 of this Regulation for approval by the Board of Directors and Management;
 - 9.2. monitoring and implementing internal PML/CFT policies and procedures;
 - 9.3. cooperation with internal auditors, external auditors and management for issues related to PML/CFT;
 - 9.4. planning and supervising the training and awareness of employees of financial institution in relation to PML/CFT;
 - 9.5. determining criteria for business relationships, including higher risk as described in Article 6 of this Regulation;
 - 9.6. conducting as a minimum on annual basis, an assessment of all risks deriving from existing and new customers, new products and services provided by financial institution, in compliance with Article 7 of this Regulation.
 - 9.7. conducting an assessment of effectiveness of internal procedures using statistical information collected within the country and those held by financial institutions, as may be determined by FIU–K and CBK.
 - 9.8. receiving internal suspicious activities reports and carrying out internal reviews of such reports in order to determine whether the suspicion is justified and if so, reporting to FIU-K, as determined in Article 26 of the Law on PML/CFT
 - 9.9. reporting other information to FIU-K in compliance with the legal provisions of the Law on PML/CFT;
 - 9.10. cooperation between the bank or financial institution and relevant authorities according to Article 26 of the Law on PML/CFT in relation to suspicious acts or reports of transactions presented to FIU-K.

9.11. other duties assigned by the Board of Directors and/or Senior Management to help in preventing the use of bank for money laundering or purposes of terrorist financing

Article 7

Internal PML/CFT policies and procedures

1. Financial institutions shall adopt internal PML/CFT policies and procedures and communicate them to all relevant staff.
2. Internal policies and procedures referred to in paragraph 1 of this Article shall at a minimum set out:
 - 2.1. a policy on customer due diligence in compliance with the Law on PML/CFT and this Regulation, including the procedure for identification and accepting the new customer within the risk appetite of the financial institution;
 - 2.2. procedure for collecting and maintaining information and records in accordance with Law on PML/CFT and this Regulation;
 - 2.3. procedure for reporting to FIU-K according to Article 26 of the Law on PML/CFT;
 - 2.4. criteria to be applied in identifying business relationships which involve higher risk;
 - 2.5. procedure for identifying and treating politically exposed persons;
 - 2.6. procedure for assessing risk and monitoring risk for customers, business relationships, products and transactions;
 - 2.7. procedure for the development by the financial institution of indicators of money laundering and terrorist financing activities based on recommendations of FATF, guidelines of FIU-K and requirements of CBK;
 - 2.8. the situations in which the internal PML/CFT Function must be consulted by staff and cases in which the Board of Directors and/or Senior Management must be notified of events relevant to PML/CFT;
 - 2.9. procedures for staff vetting and training for PML/CFT purposes;
3. Financial institutions shall establish internal policies and procedures for protection of compliance staff and other staff dealing with reporting suspicious transactions.

Article 8

ML/TF risk assessment

1. In order to make an objective decision for accepting customers, and especially when customers may pose high risk for the institution, the financial institutions should have in place a policy for the risk level, which should be managed consistently. Financial institutions shall create and maintain a “risk acceptance” strategy which should be favorable to help in their customer acceptance policies.
2. In accordance with the provisions of Article 18 of the Law on PML/CFT, financial institutions shall prepare a risk analysis and draft the risk assessment for customers, business relationships, products or transactions related to the possibility of abusing them for money laundering or terrorist

financing. Financial institutions shall understand and accept risks and weaknesses that may expose the institution to possible abuses of its products and services.

3. Risk assessment shall consider the following risk elements that are present at all business relationships:
 - 3.1. Customer risk (risk posed by customer type);
 - 3.2. Product, services and transactions risk (risk posed by the product purpose itself);
 - 3.3. Country risk (risk posed by the geographical maturity of economic activities of business relationships);
4. Elements set forth in paragraph 3 of this Article shall be combined together in order to create a risk profile. Risk profile or the procedure to establish the risk profile shall present specific characteristics of organizations and its activity (e.g. its size and composition, business scope and structure, type of customers with which the organization does business and types of products provided by the organization) as determined in Article 12 of this Regulation.
5. PML/CFT risk analysis shall be carried out in two phases:
 - 5.1. Risk assessment based on products, services and geographical distribution of the financial institution in which the institution exercises its activity.
 - 5.2. Risk assessment based on the relationships of customers of financial institution and products and services used by their customers, as well as geographical location in which they reside, work or do business and other similar risk factors.
6. Risk assessment according to point 5.1 of this Article shall mean good knowledge of business operations of the institution and exercise of sound judgment in such a way that the risk for money laundering and terrorist financing may be assessed both according to the individual factor and as a combination of them. Although the tools developed for risk assessment aim to provide objectivity, a subjectivity element remains for determining the risk factor and thus the better informed the decision-making process, the more realistic will be the judgment of risk factor level. Risk assessment element is not static and shall change over time, parallel with changes on the manner in which financial institutions operate and their products and services provided develop.
7. The risk assessment according to point 5.2 of this Article shall mean the type of risk based relationships assessment which follows a methodology that ultimately manages to identify the risk level posed by a particular client and thus enables financial institutions to determine whether the acceptance of this new customer would pose risk that could be harmful.
8. Financial institutions shall identify and assess risks of money laundering or terrorist financing that may arise in relation to:
 - 8.1. development of new products and business practices, including new distribution mechanisms, and
 - 8.2. usage of new or emerging technologies, both for new and pre-existing products.
9. Such risk assessment shall be carried out prior to bringing into use of new products, business practices or usage of new or emerging technologies. They should take appropriate measures to manage and reduce these risks.

Article 9
Customer due diligence

1. PML/CFT program determines applicable customer identification and due diligence procedures for customers of financial institutions. Financial institution shall conduct customer due diligence for:
 - 1.1. customers;
 - 1.2. any beneficial owner of the customer;
 - 1.3. any person acting on behalf of a customer.
2. For the purposes of this Regulation and based on the Article 19 of the Law on PML/CFT and in compliance with international standards, customer due diligence consists of, but not limited to:
 - 2.1. identification and verification of customer identity on the basis of valid documents issued by competent authorities;
 - 2.2. determining the beneficial owner and taking appropriate risk-based measures in order to verify his/her identity;
 - 2.3. obtaining information on the purpose and nature of business relationships and creating a customer profile based on collected information;
 - 2.4. conducting ongoing due diligence and monitoring of customer business relationships and transactions in compliance with customer profile;
 - 2.5. implementing prescribed policies and practices on electronic or wire transfers and correspondent banking; and
 - 2.6. record-keeping and retention.
3. Taking into account the level of risk, financial institutions will develop due diligence or enhanced due diligence towards customers.
4. Financial institutions must conduct customer due diligence in accordance with the terms and conditions set forth in the following circumstances, but not limited to:
 - 4.1. when establishing a business relationship with a new customer;
 - 4.2. when in relation to an existing customer there has been a material change in the nature or purpose of the business relationship, considering that there is insufficient information about the customer;
 - 4.3. when there are doubts about the authenticity and accuracy of the customer or beneficial owner information, obtained in advance;
 - 4.4. when an occasional cash transaction is made that amounts to 10,000 euros or more or the equivalent value in foreign currency, if the transaction is carried out in a single operation or in several actions (transactions) which are visibly connected and carried out in a single day;
 - 4.5. during the performance of an occasional transaction that is a local or international electronic transfer in a value greater than 1,000 euros.
 - 4.6. whenever there is a suspicion of money laundering or financing of terrorism.

Article 10

Identification, verification and acceptance of new customers

1. Financial institutions shall ensure that they know the true identity of the customer and have full knowledge of customer business prior to establishing business relationships, according to the obligations set forth in Article 19 of the Law on PML/CFT. In addition, before establishing business relationships with a customer, financial institutions shall refer to the updated international list of persons wanted for terrorist financing as part of undertaking an assessment based on relationships or risk-based assessment of customers in compliance with Article 7 of this Regulation.
2. Financial institutions shall take additional steps to ensure the proper identification of customers when doubts arise on the authenticity and accuracy of identification data obtained before or when there is a suspicion that customer is or may be involved in money laundering or financing of terrorism.
3. Financial institutions shall verify identification data with an independent source, as specified in Article 19 of the Law on PML/CFT. Verification process is separate from but complementary to the identification process. In addition to the requirements set forth in Article 19 of the Law on PML/CFT, financial institutions may require and obtain any additional identification documentation for the purpose of verification as they may deem reasonable and proper for circumstances of all cases in order to complete the due diligence process in a satisfactory manner.
4. In addition to the requirements set forth in Article 19 of the Law on PML/CFT for verification of identity of customers who are natural persons, financial institutions shall use reliable documents, documents from an independent source, data or information, such as identity card, passport, driver license or birth certificate with photo. Identification of natural persons and verification of their identity shall include the full name, address, date and place of birth.
5. In addition to the requirements set forth in Article 19 of the Law on PML/CFT, in the process of obtaining and verifying information on legal persons identification, financial institutions shall use documents proving:
 - 5.1. customer name and legal form, including the proof of incorporation or any other similar evidence of establishment or existence (such as certificate of incorporation or certificate of establishment of trust);
 - 5.2. names and addresses of members of the controlling body of customers, as for directors of companies, administrators/trustees of trusts, limited liability companies, general partnerships and senior managers, such as chief executive officer;
 - 5.3. documents indicating the customer status (such as memorandum and status or certificate of establishment of trust)
 - 5.4. documents authorizing persons to act on behalf of customer (such as decision of the Board of Directors or the declaration of administrator in opening an account and giving authority to those that may operate with account);
 - 5.5. identity of the natural person purporting to act on behalf of the customer,
6. In case the customer is represented by a third person through a representation act, the bank or financial institution shall require data for identification of customer and his/her representative and

keep the file of the customer for all documents provided by the third person, including the original or copy of notarized authorization.

7. In cases where the customer is not "physically present", adequate measures must be taken as defined in paragraph 2 of article 22 of the Law on PML/CFT.
8. In the circumstances when, under the conditions of paragraph 7 of this article of this Regulation, financial institutions create relationships or undertake a transaction without the physical presence of the customer, financial institutions must apply additional due diligence measures as required in Article 22 of the PML/CFT Law which mandatory relationship is considered a high-risk situation.
9. Financial institutions shall not establish business relationships, open accounts or undertake transactions on behalf of a potential customer until the adequate completion of the full identification and the verification process. In cases when a bank or financial institution is not able to fulfil sub-paragraphs a), b) and c) of paragraph 2 of Article 8 of this Regulation in compliance with the Chapter III of the Law on PML/CFT, the financial institution shall reject the transaction or business relationship and shall consider filing a suspicious transaction report to FIU–K in compliance with determined reporting procedures.
10. Financial institutions shall develop clear customer acceptance policies and procedures within their risk appetite and as an integral part of their risk-based approach. Such customer acceptance policies and procedures shall include a description of the types of customers that may pose a higher-than-average risk in a financial institution in order that enhanced due diligence measures may be applied to higher risk customers. Factors such as customer’s background, country of origin, public or high-profile position, linked accounts, business activities and other risk indicators shall be considered.
11. Customers who fulfil criteria set forth in the Law on PML/CFT and this Regulation may open an account or do business with the financial institution. A natural or legal person who does not fulfil the criteria set with the policy and procedures of accepting customers shall not be allowed to open an account or carry out any transaction.

Article 11

Determination of property right holders (beneficial owners)

1. Law on PML/CFT defines a beneficial owner as the “natural person who ultimately owns or controls a customer or an account, the person on whose behalf a transaction is being conducted, or the person who ultimately exercises effective control over a legal person or arrangement”- Article 2, paragraph (1), sub-paragraph (1.36). Article 19, paragraph (1) subparagraph (1.2) of the Law on PML/CFT stipulates that “all reporting entities shall identify beneficial owner and/or natural person or persons who directly or indirectly control 25% or more of a legal person”.
2. Financial institutions shall take measures to determine whether a customer is acting on behalf of one or more beneficial owners in compliance with the Chapter III of the Law on PML/CFT. In order to identify and verify the identity of customer and beneficial owner(s), financial institutions shall act in accordance with Article 19 of the Law on PML/CFT and Article 9 of this Regulation. Financial institutions shall verify identification data and information from an independent source, as specified in Article 19 of the Law on PML/CFT.
3. Financial institutions shall ensure that a person acting on behalf of another person is authorized and shall keep a copy of the authorization document provided.

4. For customers who are entities (legal persons), as determined in the Law on PML/CFT, financial institutions shall take significant measures in order to understand the ownership and control structure of entity. Financial institutions shall identify “decision-makers and management” of the legal person and ultimately (natural person) beneficial owners who, directly or indirectly, control 25% or more of the legal person. By identifying the beneficial owner(s), banks and financial institutions shall determine through their procedures for customer risk assessment if such beneficial owner(s) corresponds to the status of politically exposed person, in compliance with the conditions of the Law on PML/CFT. In such cases, banks and other financial institutions shall apply enhanced measures for politically exposed persons, as provided for in the Law on PML/CFT and this Regulation.
5. For purposes of this Regulation, “a person shall be considered as exercising direct or indirect control over a legal person in any of the following situations:
 - 5.1. by holding 25% or more of the share capital of the legal person registered in that person’s name;
 - 5.2. by holding 25% or more of the voting rights of the legal person, regardless of the shares held;
 - 5.3. when, acting in cooperation with other persons that person exercises control by holding of 25% or more of the share capital or voting rights;
 - 5.4. by holding 25% or more of the share capital of the legal person registered in the name of another legal person who is ultimately owned by that person;
 - 5.5. by holding 25% or more of the voting rights of a legal person by another legal person who is ultimately owned by that person.
6. For entities that are non-profit organizations/NGO, financial institutions shall ensure the identification of the structure of control and understand the legitimate purpose of the organization by reviewing its status, establishment or document of trust.
7. For other legal arrangements such as trusts, in addition to the identification of the trustee, the settlor and/or director, financial institutions shall identify beneficiaries of the trust of 25% or more of the property, where beneficiaries have been defined or when beneficiaries have not been defined, the classification of persons on whose interest the legal arrangement has been concluded or operates. For other types of legal agreements, the financial institutions shall identify persons with equivalent or similar position.

Article 12

Creating the customer profile

1. Financial institutions shall collect information on ongoing bases related to the intended purpose and intended nature of the business relationship. Documents, data or information collected under the customer due diligence research process shall be kept up to date and relevant by undertaking periodical reviews of the existing data, including transaction records.
2. Financial institutions shall create and maintain a customer profile for each customer, with sufficient details to enable bank or the financial institution to monitor customer transactions, to apply customer due diligence when necessary and detect suspicious transactions/acts as required in Chapter III of the Law on PML/CFT and this Regulation. Data and information included in the

profile shall be in compliance with the risk level expected to be posed by the customer.

- Customer profile shall include relevant information for normal and reasonable actions for different types of customers taking into account the nature of customer business, as well as full understanding of customers transactions (including source and legitimacy of funds, as necessary) and overall relationships with bank or financial institution.

Article 13

Monitoring of business relationships and transactions

- Financial institutions shall conduct ongoing due diligence on business relationships and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions undertaken are consistent with the institution’s knowledge of the customer, their business and risk profile, and undertake review or updating of existing data in order to ensure that customer data is kept up-to-date and relevant. To this end, in addition to the requirements set forth in Article 19 of the Law on PML/CFT, in circumstances when financial institutions deem necessary, information should be sought to confirm the source of funds. Financial institutions shall have systems in place to detect large or complex transactions undertaken (completed) outside the expected norms (knowledge) for that type of customer.
- Financial institutions shall ensure that the scope and frequency of implementation of measures from paragraph 1 of this Article are consistent with due diligence and risk assessment and that they are adapted to the risk of money laundering and financing of terrorism to which the financial institution is exposed during the performance of a specific business activity or transaction, i.e. within the framework of the business relationship with the customer.
- Financial institutions shall apply (intensified) frequent monitoring for higher risk customers. Every financial institution shall determine key indicators for such accounts taking into account the customer background, country of origin and source of funds, type of transactions involved and other risk factors as determined in Law on PML/CFT and this Regulation.
- Structuring of the ongoing process of monitoring accounts, transactions and identification of customers and information on their profile will be presented according to the table below.

Risk category	Monitoring minimum frequency
3. High	Transactions: <i>Daily</i> Account: <i>Monthly</i> Customer Information: <i>Annual</i>
2. Medium	Transactions: <i>Weekly</i> Account: <i>Semi-annual</i> Customer Information: <i>Triennial</i>
1. Low	Transactions: <i>Monthly</i> Account: <i>Annual</i> Customer information: <i>Quinquennial</i>

- Frequency of monitoring according to table in paragraph 4 of this Article shall not apply when

there are suspicions for money laundering or terrorist financing or when the bank or financial institution identifies major changes in transactions based on the risk profile of the customer.

In situations where the financial institution, in accordance with the Guidelines for ML/FT risk factors, considers that the ML/FT risk is low, for vulnerable groups of customers, it may apply mitigated measures for data review. Before these measures are applied, the financial institution must document the low risk assessment based on detailed analysis.

Article 14

Electronic transfers

In the case of domestic or international electronic transfers, financial institutions must implement the measures defined in the Law on PML/CFT, this Regulation and the Regulation on the information that must accompany fund transfers.

Article 15

Correspondent relationships

1. Article 22 of the Law on PML/CFT requires the establishment of mandatory measures in addition to standard measures to extend due diligence in correspondent banking relationships, which represent a higher risk. Financial institutions will develop and implement policies and procedures related to correspondent relationships and which address high risks in such relationships.
2. For the purpose of this Article, correspondent relationship shall be defined as a means of providing banking services from one bank (correspondent) to another bank (respondent), which may include loans, deposits, collection, clearing or payment services, as well as relations between financial institutions and between financial institutions where similar services are provided, including but not limited to those relationships established for securities transactions or fund transfers.
3. Banks in Kosovo shall act as "respondent banks", when they establish relationships for receiving banking services from another bank (correspondent banks) or as "correspondent banks", when they establish relationships for providing banking services to another bank (respondent bank).
4. Financial institutions shall exercise caution and due diligence with regards to the correspondent bank's potential controls against money laundering and terrorist financing and determine that such controls are adequate and effective and shall document the respective PML/CFT responsibilities of each institution. Financial institutions shall not undertake business relationships with shell banks, whereas regarding the correspondent banks from countries posing higher risk of money laundering and terrorist financing the bank shall ensure that it may apply enhanced measures to mitigate such risks, as required in Article 18 of this Regulation.
5. In order to assess the potential respondent bank controls against money laundering and terrorist financing based on requirements set forth in paragraph 3 of this Article, the bank should gather sufficient information on the potential respondent bank in order to understand their business and to determine from available public information the reputation of the institution, quality of supervision and whether it has been subject of investigation for money laundering and terrorist financing or regulatory actions. In general, the bank shall establish or continue correspondent relationships with a foreign respondent bank only if it is convinced that an authority is effectively

supervising the respondent bank. In particular, a bank shall not establish or continue a correspondent banking relationship with a shell bank, as determined in the Law on PML/CFT.

6. Particular care should be exercised when respondent banks allow the direct use of correspondent account by third parties to do business on their behalf (payment through accounts). The bank shall be convinced that the respondent bank has carried out the due diligence process for those customers who have direct access to accounts of the respondent bank and that respondent bank is able to ensure relevant information of customer identification upon the request of the correspondent bank.
7. Financial institutions shall develop and implement policies and procedures related to the ongoing monitoring of activities carried out through correspondent accounts. Financial institutions shall obtain the approval from the senior management before establishing new correspondent relationships and shall apply enhanced due diligence measures provided for in paragraph (4) of Article 22 of the Law on PML/CFT.

Article 16

Politically exposed persons

1. Article 22 of the Law on PML/CFT and instructions issued by FIU-K require application of reasonable measures from financial institutions, to determine whether their customers are domestic or foreign politically exposed persons. Financial institutions shall ensure to apply adequate measures in such situations, including when a beneficial owner is identified as a person with politically exposed person status.
2. When a person is identified as a domestic or foreign politically exposed person on the occasion of establishment of business relationships, financial institutions shall take the measures set forth in paragraph 5.1 of Article 22 of the Law on PML/CFT.
3. Financial institutions shall apply enhanced due diligence measures for ongoing relationships with an existing customer or beneficial owner who has been identified to be politically exposed person.
4. In taking reasonable measures to identify the origin of assets used in the relationship or transaction in compliance with paragraph 5 of the Article 22 of the Law on PML/CFT, financial institutions shall ensure that such measures will include the scrutiny of the source of wealth and the source of funds of the customer.
5. For purposes of paragraph 4 of this Article, “source of wealth” shall refer to the assets owned by the customer and that may have been accumulated over the years, whereas “source of funds” refers to funds to be applied for the first and following transactions, undertaken by the customer in his/her status as a politically exposed person.
6. Financial institutions shall ensure that “immediate family members” and “persons known as close associates” of the domestic and foreign politically exposed person shall be subject of the same enhanced due diligence measures.
7. Procedures and measures for determining the politically exposed person may include, but not limited to:
 - 7.1. requiring relevant information from the potential customer referring to the paragraph 4 of this Article;

- 7.2. searching in the official domestic and international lists;
- 7.3. referring to available public information; and
- 7.4. access to potential electronic commercial databases for politically exposed persons.

Article 17
Record-keeping and retention

1. Financial institutions shall keep all necessary records of transaction, both domestic and international, for at least five (5) years following completion of the transaction or completion of the last transaction in a series of related transactions (or longer if requested by FIU-K, CBK or other competent body in special cases). This requirement applies regardless of whether the business relationship is ongoing or has been terminated.
2. Transaction records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. Records of such transactions include:
 - 2.1. the name of the customer and the beneficial owner, (and holder of a power of attorney, if applicable) and their addresses or other identifying information as normally recorded by the bank;
 - 2.2. the nature (type) and date of the transaction;
 - 2.3. the type and amount of currency involved in the transaction; and
 - 2.4. the type and identification number of any account involved in the transaction.
3. Financial institutions shall keep all necessary records relating to the customer, beneficial owner, or holder of power of attorney, account files, and business correspondence for at least five (5) years following the termination of business relationships, or in specific cases for a longer period, if requested by FIU-K, CBK or other competent authority. The records shall identify the member of the staff who identified the customer (and beneficiary owner if applicable). Financial institutions shall establish safeguards to protect the records from damage and to prevent unauthorized access.
4. Financial institutions shall keep reports of findings from the analysis of large complex transactions and of business relationships that are subject to specific monitoring as determined in Article 25 of the Law on PML/CFT. Reports of findings shall be kept for a minimum of five (5) years following the completion of the analysis or longer if so required by FIU-K or CBK.
5. In absence of an ongoing business relationship, financial institutions and specifically foreign exchange offices and money transfer operators shall keep a copy of the identification of records and records of transactions for a period of five (5) years following a random transaction or the last transaction in a series of related random transaction.
6. Financial institutions shall make available, upon request by the FIU-K, CBK and any other competent authority all records and available information on a customer, beneficial owner or holder of power of attorney and all requested transaction records, in a form and manner that is complete, timely and comprehensible.
7. If financial institutions are aware of records relating to ongoing investigations, such records should be retained until it is confirmed by the relevant law enforcement agency that the case has been

closed, even if the time period of 5 five years has expired.

8. The electronic data of the financial institutions must be stored in a (backup) copy electronically and must be available in a readable form for the FIU-K, CBK and the competent authorities according to the legislation in force.
9. Collection, processing, use and retention of personal data from financial institutions shall be limited to the data that are necessary for the purpose of action in compliance with the requirements of the Law on PML/CFT and personal data should not be further processed in a manner that is in contradiction with this purpose. In particular, further processing of personal data for commercial purposes shall be prohibited.

Article 18

Enhanced customer due diligence

1. In applying enhanced due diligence, financial institutions should ensure not to engage in illegal discrimination based on race, color, religion or national affiliation.
2. Pursuant to the implementation of mandatory measures of enhanced due diligence in accordance with Article 14 and Article 15 of this Regulation, financial institutions shall conduct enhanced customer due diligence, in addition to standard measures, in accordance with the terms and conditions laid down by this Regulation under the following circumstances, but not limited to:
 - 2.1. When establishing a business relationship with a customer that is a trust or another entity (fund) for holding personal assets and a non-resident customer.
 - 2.2. At each stage of the process of customer due diligence, business relationships or transactions wherein financial institution in accordance with Article 7 of this Regulation has determined that these categories are of higher risk for money laundering and terrorist financing. In this process, financial institutions must make efforts to scrutiny the customer's source of wealth and funds;
 - 2.3. In business relationships and transactions with natural and legal persons, including financial institutions from countries that pose a higher risk of money laundering and terrorist financing. To this purpose, financial institutions should take into account public statements and lists issued by the Financial Action Task Force (FATF) for high-risk and uncooperative jurisdictions.
3. Financial institutions shall apply enhanced measures in monitoring accounts, transactions and business relationships and raise the risk element in in such situations where, as a result of suspicion of money laundering or financing of terrorism, a report has been sent to FIU-K.
4. The measures of customer due diligence that can be applied by financial institutions include but are not limited to:
 - 4.1. additional identification information and documents to verify the identity of the customer and beneficial owner as necessary;
 - 4.2. approval of a senior manager of the reporting entity to establish or continue the business relationship with a higher risk client.
 - 4.3. additional information and clarification on the source of wealth and source of funds;

- 4.4. obtaining and assessment of additional information on the intended nature of the business relationship;
 - 4.5. better understanding of the reasons of an intended or performed transaction by obtaining additional information;
 - 4.6. increasing the monitoring and scrutiny of business relationships, transactions and accounts including the source of funds;
 - 4.7. increasing the frequency for updating the information available for the identification of customers, risk level and business profile;
 - 4.8. increasing the periodic reporting to senior management.
5. For Non-Governmental Organizations established under the Law on Freedom of Association in Non-Governmental Organizations in Kosovo, the reporting entities for the purpose of identifying and verifying the beneficial owner will apply due diligence measures to identify the management structure of the NGO, the head of the assembly of members for the association (or the members of the intermediate body when it is applicable), the members of the management board for foundations and institutes, as well as the senior management officer for the three organizational forms of NGO establishment.
 6. For entities that are non-governmental/nonprofit organizations, based on risk assessment, financial institutions can apply and include these measures of enhanced customer due diligence, but without being limited to:
 - 6.1. identification of the founders through official documents;
 - 6.2. identification of the management structure, board of directors and executive management ;
 - 6.3. information on the main donors of the non-profit organization / NGO;
 - 6.4. annual reports of financial activities, completed and planned projects.

Article 19

Identification and reporting of suspicious activities and transactions

1. Certain types of transactions should signal the financial institutions about the possibility that the customer is conducting suspicious activities and actions. They may include transactions that do not have a clear economic, legal or commercial purpose or that involve large amounts of cash movements that are inconsistent with the customer's normal and expected transactions in accordance with the risk and business profile for that customer. A large volume of activity in the account, inconsistent with the amount of funds usually held in the account, may indicate that funds are being laundered. Examples of specific suspicious banking activities can be very useful to financial institutions and should be included in training activities. A suspicious act or transaction is usually an activity that is inconsistent with the knowledge of the legal business activities or personal activities of the customer or the customer's normal business for that type of financial product.
2. Questions that a bank or other financial institution may consider when determining whether an action or transaction may be suspicious are:
 - 2.1. Is the size of the transaction consistent with the customer's ordinary activities?

- 2.2. Is the transaction rational in the context of the customer's business activities or personal activities?
- 2.3. Has the pattern of transactions performed by the client changed?
- 2.4. When the transaction is of an international nature, does the customer have any apparent reason for doing business with the other country involved?
3. Financial institutions should consider that if a customer prefers to carry out a transaction in cash under the amount limits of 10,000 Euros, it may be supposed that the customer aims to avoid reporting and as such leads or contributes to suspicion about the transaction. Financial institutions should consider that multiple transactions, which are carried out in cash by or on behalf of a person or entity and which appear to be connected, amounting to a total of 10,000 Euros or more over a period time lead or contribute to suspicions about the transactions.
4. Financial institutions should provide sufficient guidance and training to staff to enable them to recognize suspicious acts and transactions. They must ensure that all employees know to which person in the financial institution they should report their suspicion and that there is a clear reporting line, where suspicions are sent to the PML/CFT Function. The reporting line between the person who has raised suspicion and the PML/CFT Function should be as short as possible.
5. The PML/CFT compliance function should confirm receipt of report by the staff and at the same time provide guidance and remind of the obligations to not take any action that could impair investigations, i.e., "tipping off" as explained under Article 26 of the Law on PML/CFT and as required in paragraph 12 of this Article.
6. Once the PML/CFT Function receives this initial report, it will verify and analyze the issue based on internal information. Financial institutions should keep records of such analysis and results. If during the review of the analysis and results, the bank or financial institution concludes that the performed or attempted acts or transactions provide reasonable grounds to suspect money laundering or when a connection is found with a terrorism financing action or transaction, the PML/CFT Function shall promptly report the performed or attempted act or transaction to FIU-K. Financial institutions shall report to FIU-K in situations when available information indicates that a person or entity may be or may have been involved in money laundering, related criminal offenses and/or terrorism financing.
7. All internal enquiries generated in relation to the report and the reasons for deciding whether the report is to be submitted to FIU-K shall be recorded. Records of suspicions raised within the PML/CFT but not sent to FIU-K, shall also be kept for five (5) years from the date of the transaction.
8. Pursuant to Article 26 of the Law on PML/CFT, financial institutions should report to FIU all suspicious activities or transactions within 24 hours after the activity or transaction has been identified as suspicious. Sufficient information that establishes reasonable suspicion to be reported should be disclosed and if a particular offense is suspected, this should be stated. When the financial institution has additional relevant evidence, which can be made available, the nature of such evidence should be indicated clearly and immediately when reported to FIU-K.
9. When a financial institution reports in accordance with paragraph 1.2 of Article 26 of the Law on PML/CFT, but there are doubts that the transaction may involve money laundering or may be related to terrorism financing, it should also submit a suspicious transaction report to FIU-K in

accordance with paragraph 6 of this Article, indicating that the two reports refer to the same transaction, activity or person.

10. If a financial institution decides not to enter into a business relationship due to suspicion of money laundering or terrorism financing, it shall report such a decision immediately to FIU-K as defined by the Law on PML/CFT.
11. Financial institutions shall report to FIU-K every customer or transaction that have reasonable grounds to suspect that they may be related to terrorism financing or individuals that support terrorism. Attention should be paid to monitoring and updating the list of organizations and individuals related to terrorists or terrorism based on information received from FIU-K or other available international sources. Attention should be paid to nonprofit and humanitarian organizations, especially if their activities do not comply with the registered activity, if the source of funds is not clear or if such organizations receive assets from suspicious sources.
12. Reporting entities, directors, officers and temporary or permanent employees of the reporting entity who prepare or submit reports in accordance with this Law shall not disclose facts about any report that is submitted or is in the process of being submitted, shall not provide the report nor communicate any information contained in the report or regarding the report, including when such information is being prepared for reporting or when investigations on money laundering or terrorism financing are being or may be carried out, to any person or entity, including any person or entity involved in the transaction which is included in the report, except FIU-K, unless authorized in writing by FIU-K, the public prosecutor or the court to do so.
13. It is the responsibility of every officer or employee of a bank or other financial institution, who was the first to raise suspicion over an act or transaction or a person that has been involved in or is related to money laundering or terrorism financing to ensure the submission of an internal report on such suspicion to the Head of the PML/CFT Function. According to the Law on PML/CFT, any threat to urge them to refrain from preparing a report or to provide a false statement or fail to state true information to the FIU-K, other investigative agencies or judicial authorities is an offense punishable under the Law on PML/CFT. In such cases, reporting officers or employees should immediately report the issue in accordance with the institution's internal reporting lines and procedures.

Article 20

Staff verification, qualification and training

1. Financial institutions should make staff aware of their personal legal (statutory) obligations and inform them that they will be personally liable if they fail to report information in accordance with internal policies and procedures.
2. Financial institutions shall implement general measures to ensure that their employees, especially the staff that has contact with customers or is involved in the execution of transactions and the staff within the PML/CFT Function do not have a criminal record or are not subject to ongoing criminal prosecution for financial crimes, terrorism or any other serious crime that can raise doubts as to their credibility.
3. Financial institutions shall provide on regular basis, at least once a year, training on PML/CFT for all staff that has contact with customers or are involved in the execution of transactions.

4. Documents on the structure of training programs, their content, and names and signatures of participants shall be maintained in the bank or financial institution for at least five (5) years.

Article 21

Role of internal and external audit

1. The Internal Audit Department of financial institutions shall perform audits at least once a year to ensure that the policies and procedures for PML/CFT are implemented fully and in accordance with all requirements of the Law on PML/CFT and this Regulation.

The Internal Audit Department shall report on annual basis to the Board of Directors and inform the management of financial institutions of its findings and assessments, including an appropriate evaluation of staff training on PML/CFT issues.

2. CBK may require financial institutions to engage their external auditors to assess and report on the quality of implementation of PML/CFT measures, including the implementation of legal and regulatory requirements, policies and procedures, internal control systems, and performance of the internal audit.

CHAPTER III

Article 22

Supervision from the Central Bank of the Republic of Kosovo

1. The CBK shall supervise financial institutions in terms of compliance with the obligations under the Law on PML/CFT and this Regulation.
2. CBK shall supervise and inspect financial institutions. To this purpose, the CBK shall exercise its supervisory competencies concerning the right of access, the right to request information and documents and to obtain necessary copies and related rights granted under the Law on PML/CFT and relevant legislation on financial institutions.

Article 23

Remedial measures

Violations of the provisions of the Law on PML/CFT and this Regulation shall be subject to remedial and punitive measures as defined by the Law on PML/CFT, the Law on the Central Bank of the Republic of Kosovo and relevant legislation on financial institutions.

Article 24

Repeal

With the entry into force of this Regulation, the Regulation on prevention of money laundering and

financing of terrorism, approved by the Board of the Central Bank on 30 January 2020, and any other provisions that may be contrary to this Regulation issued by CBK shall be repealed.

Article 25
Entry into force

This Regulation shall enter into force on 1 August 2024.

Bashkim Nurboja
Chairman of the Board of the Central Bank of the Republic of Kosovo