Pursuant to Article 17 and Article 22(1) of the Law on the Council of Ministers of Bosnia and Herzegovina ("Official Gazette of BiH", Nos. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 and 24/08) and Article 101(1) of the Law on the Prevention of Money Laundering and Financing of Terrorist Activities ("Official Gazette of BiH", No. 13/24), upon the proposal of the Ministry of Security of Bosnia and Herzegovina, the Council of Ministers of Bosnia and Herzegovina, at its 98th session held on 29 December 2025, adopted the following:

RULEBOOK ON THE IMPLEMENTATION OF THE LAW ON THE PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORIST ACTIVITIES

Official Gazette of BiH, No. 8/2026, 3.2.2026

CHAPTER I – GENERAL PROVISIONS

Article 1

(Subject Matter of the Rulebook)

This Rulebook prescribes in more detail:

- the criteria for drafting guidelines for assessing the risk of money laundering, financing of terrorist activities, and financing of the proliferation of weapons of mass destruction;
- the implementation of requirements regarding customer identification and monitoring;
- the manner of applying enhanced customer due diligence measures;
- the manner and conditions for applying simplified customer due diligence measures;
- reporting to the Financial Intelligence Department of the State Investigation and Protection Agency (hereinafter: FID), related cash transactions, and submission of documents and data;
- the manner and parameters for establishing, updating, and publishing the list of indicators for identifying suspicious transactions; further defining the identification and monitoring of related transactions;
- the manner and parameters for establishing, updating, and publishing the list of high-risk countries with strategic deficiencies in the field of preventing money laundering and terrorist financing;
- responsibility for ensuring and organizing internal controls, organizing and conducting employee training for reporting entities, and submitting data on authorized persons.

Article 2

(Gender Usage)

Words used in this regulation in one gender for reasons of clarity shall refer equally to both masculine and feminine genders without discrimination.

Article 3

(Meaning of Certain Terms)

1. Certain terms used in this Rulebook shall have the following meanings:

a) “risk” means the impact and likelihood of the occurrence of money laundering, financing of terrorist activities, and proliferation of weapons of mass destruction. Risk refers to the level of risk existing prior to the application of risk mitigation measures;

b) “inherent risk” means the level of risk before risk reduction;

c) “residual risk” means the level of risk remaining after risk reduction;

d) “public authority,” within the meaning of this Rulebook, means a domestic authority at all levels of government in Bosnia and Herzegovina or a foreign state authority, public enterprise, public agency, public service, public fund, public institution or chamber, as well as any other public institution performing activities of public interest on the basis of domestic regulations, regulations of foreign states and international organizations, or EU legislation.

2. Other terms used in this Rulebook shall have the same meaning as in the Law on the Prevention of Money Laundering and Financing of Terrorist Activities (“Official Gazette of BiH”, No. 13/24) (hereinafter: the Law).

CHAPTER II – GUIDELINES FOR RISK ASSESSMENT OF MONEY LAUNDERING AND FINANCING OF TERRORIST ACTIVITIES

Article 4

(Obligation of Supervisory Authorities to Adopt Guidelines)

1. Supervisory authorities referred to in Article 93 of the Law shall adopt and/or, as necessary, update guidelines for the analysis and assessment of risks relating to customers, business relationships, and transactions for reporting entities referred to in Article 5 of the Law within 90 days from the date of entry into force of this Rulebook.

2. The guidelines referred to in paragraph (1) of this Article shall assist in identifying, monitoring, and mitigating risks across various sectors.
3. In addition to the risk factors prescribed in Article 10(1) of the Law, supervisory authorities shall include in the guidelines other risks specific to individual sectors.
4. In drafting the guidelines, supervisory authorities shall take into account the results of the risk assessment of money laundering, terrorist financing, and proliferation financing in Bosnia and Herzegovina (hereinafter: the risk assessment), the Law, and the provisions of this Rulebook. They shall also consider guidelines of international and regional sectoral associations of supervisors or reporting entities, such as those of the European Banking Authority (EBA), the International Organization of Securities Commissions (IOSCO), and others, and shall cooperate with other competent authorities to harmonize positions and define a unified approach.
5. Supervisory authorities shall publish the guidelines on their websites and immediately deliver them to the reporting entities to which they apply.

Article 5

(Written Internal Risk Assessment Program – Conditions and Content)

1. In accordance with Article 10 of the Law, reporting entities shall adopt a written internal program defining risk levels for groups of customers or individual customers, taking into account the country, geographic area of operation, business relationship, transactions, products or services, distribution channels, and the use of new and developing technologies in connection with possible misuse for money laundering, terrorist financing, or proliferation financing, in accordance with this Rulebook and the guidelines of the competent supervisory authority.
2. The written internal program shall also include a method for:

a) identifying all risk factors to which the entity is exposed when establishing a business relationship or conducting a transaction;
b) assessing risk based on identified factors;
c) mitigating assessed risks;
d) monitoring changes in risk and maintaining records of changes in assessed risk levels for customer groups or individual customers, countries, geographic areas, business relationships, transactions, products or services, distribution channels, and new technologies, including reasons for such assessment and actions taken;

e) assessing the risk of the overall business operations;
f) monitoring the effectiveness and implementation of the program.

3. Reporting entities shall ensure that the internal risk assessment program is included in the internal training of their employees.

Article 6

(Factors Affecting Risk Assessment by Reporting Entities)

1. Reporting entities shall develop comprehensive risk assessment procedures.
2. Risk analysis shall be proportionate to the nature and scope of the entity's business and shall include risks relating to customers, products, services, transactions, countries, geographic areas, and distribution channels.

a) Customer risk includes:

1. the business or professional activity of the customer and beneficial owner;
2. the reputation of the customer and beneficial owner;
3. the nature and behavior of the customer and their transactions.

b) Product, service, or transaction risk includes:

1. the purpose of the business relationship and manner of use of the service;
2. regularity and duration of the business relationship;
3. credit exposure and transaction volume;
4. level of transparency of the product, service, or transaction, especially regarding anonymity and ownership structure;
5. complexity of the product or transaction;
6. value and volume of products or transactions, with focus on cash transactions, large transfers, and high-risk trade sectors.

c) Country and geographic risk includes:

1. location of the customer's and beneficial owner's headquarters and operations;
2. relevant personal, business, or financial ties to high-risk countries;
3. effectiveness of AML/CFT regimes in certain countries;
4. level of transparency and tax discipline.

d) Distribution channel risk includes:

1. non-face-to-face business relationships;
2. internet-based services;
3. use of intermediaries and their regulatory and supervisory status.

3. Reporting entities shall also consider other risk factors specific to their business.

Article 7

(Drafting, Publishing, and Updating the List of Indicators for Identifying Suspicious Transactions)

1. The list of indicators for identifying suspicious transactions, funds, and customers under Article 57(5) of the Law (hereinafter: the List of Indicators) shall be adopted and updated by the FID in cooperation with supervisory authorities for each category of reporting entity separately.
2. In drafting and updating the List, known techniques, methods, and trends of money laundering and terrorist financing domestically and internationally shall be considered.
3. The List shall be published on the websites of the FID and supervisory authorities.
4. The List shall be updated as necessary, and at least once every two years.

Article 8

(Risk-Based Approach by Reporting Entities)

1. Reporting entities shall assess risks for each customer group, business relationship, product/service, and transaction.
2. Customers shall be classified into:
   a) low risk;
   b) medium risk;
   c) high risk.
3. Based on risk assessment, reporting entities shall determine whether enhanced or simplified due diligence measures apply.

Article 9

(Customers That May Be Classified as Low Risk)

1. A low-risk customer may include:

a) a public authority meeting transparency criteria;
b) a publicly listed joint-stock or commercial company subject to disclosure requirements ensuring beneficial ownership transparency;
c) a reporting entity registered or resident in a country assessed by FATF or another relevant body as having an effective AML/CFT system and not listed as high-risk.

2. Foreign customers under points (a) and (b) may be classified as low risk only if the country meets the condition under point (c).

3. Subsidiaries majority-owned by low-risk entities may also qualify under certain legal conditions.

Article 10

(Verification of Conditions)

1. Reporting entities shall verify compliance with Article 9 conditions.

2. A written statement shall be obtained from the customer.

3. Other persons assessed as low risk under the Law may also qualify for simplified measures.

Article 11

(Types of Business Relationships, Services, or Transactions That May Be Classified as Low Risk)

1. The following may be classified as low risk:

a) life insurance policies with low premiums (annual total not exceeding BAM 2,000 or single premium not exceeding BAM 5,000);
b) voluntary pension fund membership contracts with non-transferable rights;
c) employee pension schemes with payroll deductions and non-transferable rights;
d) leasing contracts not exceeding BAM 30,000;
e) credit agreements with annual exposure not exceeding BAM 3,000;
f) short-term receivables purchase agreements not exceeding BAM 30,000;
g) financial products/services assessed as low risk;
h) financial products with built-in risk mitigation mechanisms (e.g., electronic money);
i) digital asset transactions under BAM 300 per transaction (or related transactions), not exceeding BAM 600 monthly and BAM 4,000 annually per customer.

2. The use of a low-risk product does not automatically reduce the customer's overall risk category.

Article 12
(Risk Assessment When Introducing New Products and Services)

Obliged entities are required, prior to introducing new products or making significant changes to existing products and services, to conduct a risk analysis, determining:

a) the potential risk that may arise from the introduction of a new product or service;

b) the impact on the overall risk exposure of the obliged entity;

c) the possibilities for adequately managing the new risk in order to reduce the possibility of misuse of the product or service for the purposes of money laundering, financing of terrorist activities, and financing the proliferation of weapons of mass destruction.

Article 13
(Risk Assessment of Individual Business Relationships and Occasional Transactions)

(1) After conducting a risk assessment, the obliged entity must categorize business relationships and occasional transactions, in accordance with the assessed level of risk, into risk categories.

(2) The risks of misuse of an individual business relationship and occasional transactions for money laundering, terrorist financing, and financing the proliferation of weapons of mass destruction may be classified into one of the following categories:

a) **high risk**: situations or activities that have a significant likelihood of a negative outcome with serious consequences, often associated with a high level of threats or vulnerabilities related to money laundering, terrorist financing and/or proliferation financing, and which require the application of enhanced identification and monitoring measures;

b) **medium risk**: situations or activities that have a moderate likelihood of a negative outcome and may cause moderate consequences related to money laundering, terrorist financing and/or proliferation financing, referring to clients, transactions, or business relationships that do not meet the criteria for high risk, but where attention and regular monitoring are nevertheless required;

c) **low risk**: a level of risk where, based on the assessment, no significant indicators of money laundering, terrorist financing and/or proliferation financing have been

identified. In such cases, the obliged entity applies simplified customer identification and monitoring measures, without the need for additional or enhanced measures, unless circumstances arise during the business relationship indicating a higher level of risk.

(3) In addition to the risk categories referred to in paragraph (2) of this Article, obliged entities are required, based on a documented risk assessment, to identify clients, business relationships, and occasional transactions that are unacceptable to the obliged entity, such as: natural and legal persons subject to sanctions of the UN Security Council and/or persons conducting certain business activities without authorization from a competent authority who seek to establish a business relationship with the obliged entity, as well as other persons assessed as unacceptable due to the inability to adequately manage the risk.

Article 14
(Risk Assessment of the Obliged Entity's Overall Operations)

(1) The obliged entity is required to conduct a risk assessment of its overall operations to which it is exposed across all segments of its business. The risk assessment must be proportionate to the scope and complexity of operations and must accurately reflect the actual risks to which the obliged entity is exposed.

(2) Based on the conducted overall risk assessment, the obliged entity shall assess the level of risk to which it is exposed and determine a risk rating as follows:

a) low-significance risk;
b) moderately significant risk;
c) significant risk;
d) very significant risk.

Article 15
(Updating the Overall Business Risk Assessment of the Obliged Entity)

(1) The obliged entity shall regularly update its risk assessment to ensure that it is current and reflects the actual risk situation. The obliged entity shall update the risk assessment without delay in the event of significant changes in its operations or those of its clients, changes in the regulatory environment, or other events that may affect its risk exposure.

(2) The risk assessment must be reviewed and updated at least once a year, or more frequently if required by the circumstances referred to in paragraph (1) of this Article.

(3) When updating risk assessments, the obliged entity must use relevant internal data and information such as operational, transactional and other data, as well as external documentation and guidelines of competent domestic, regional and international institutions such as: the Financial Action Task Force (FATF), the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) of the Council of Europe, the United Nations Office on Drugs and Crime (UNODC), the International Monetary Fund (IMF), the World Bank (WB), the International Organization of Securities Commissions (IOSCO), the European Banking Authority (EBA), and other relevant institutions.

Article 16
(Grounds for Updating a Client's Risk Level and Reviewing Established Risk Assessment Systems)

(1) The obliged entity is required to establish a system for regular assessment and updating of client risk, determining when it is necessary to change, i.e., increase or decrease, a client's risk level in accordance with the client's actual activities during the business relationship.

(2) Updating client risk must include an assessment of inherent and residual risks at the level of the country, sector, obliged entity, and individual business relationships.

(3) Key factors triggering the updating of client risk levels include:

a) the occurrence of circumstances prescribed by Article 29 of the Law;

b) unusual activities, such as alerts from transaction monitoring systems, case openings, or the submission of suspicious transaction reports;

c) requests or inquiries from competent authorities;

d) transactions that violate targeted financial sanctions;

e) significant changes in the scope or type of the client's activities compared to expected or initially agreed business;

f) negative media information concerning the client.

(4) If, during the update of the risk assessment, a need to change the risk level is established, the obliged entity shall update the client's risk rating, which may include the application of enhanced identification and monitoring measures, which must be documented.

(5) The obliged entity is required to prescribe, in its policies, controls, and procedures, measures to eliminate identified weaknesses in risk assessment systems if a risk is

identified or if errors affecting the efficiency and effectiveness of the risk assessment are established.

(6) The measures referred to in paragraph (5) must include an analysis of inadequately assessed risks of business relationships and, in accordance with the identified risk category, give priority to implementing measures for business relationships carrying potentially higher risk.

(7) Taking into account the results of the analysis referred to in paragraph (6), the obliged entity shall review the established risk assessment system and the effectiveness of the internal control system in the classification of clients into risk groups, and, if necessary, undertake one or more of the following measures:

a) implement additional enhanced identification and monitoring measures prescribed by Article 29 of the Law and by-laws of the competent supervisory authority;

b) refuse to carry out the transaction in accordance with Article 14 of the Law;

c) terminate the business relationship in accordance with Article 14 of the Law;

d) notify the Financial Intelligence Department (FOO) of suspicious transactions, funds, and persons in accordance with Article 42 of the Law.

CHAPTER III – IMPLEMENTATION OF CUSTOMER IDENTIFICATION AND MONITORING REQUIREMENTS

Article 17
(Customer Identification Obligations)

(1) Obliged entities are required to understand the purpose and intended nature of the business relationship and transaction.

(2) If insurance companies determine that a beneficiary of insurance who is a legal person or legal arrangement represents a higher risk, they are required to undertake enhanced measures, including reasonable steps to identify and verify the identity of the beneficial owner of the beneficiary at the time of payout.

(3) In cases where the obliged entity suspects money laundering, terrorist financing, or proliferation financing and reasonably believes that conducting customer identification and monitoring procedures would trigger a disclosure to the client, it shall not continue the procedure and shall submit a suspicious transaction report.

Article 18
(Identification of Legal Arrangements)

(1) Identification of legal arrangements referred to in Article 4, point (oo) of the Law shall be carried out using the following identification data and documents:

a) name of the legal arrangement;
b) date of establishment;
c) official identification number where applicable (e.g., tax identification number or registration number);
d) identification data for all natural persons connected with the legal arrangement, including the beneficial owner, known beneficiaries, persons exercising control, including trustees or other persons with control or authority to direct the client's activities (including protectors, co-trustees, or other third parties), including the settlor where significant powers are retained;
e) postal address of the trustee or other persons exercising control;
f) a copy of the agreement establishing the legal arrangement.

(2) For clients that are legal arrangements, obliged entities must obtain information on the powers governing and binding the legal arrangement, on persons in senior management positions, and on the principal place of business if different from the registered address.

Article 19
(Customer Identification Through Third Parties)

(1) The obliged entity shall implement customer identification and monitoring measures in accordance with the Law, this Rulebook, and supervisory guidelines.

(2) Obliged entities may entrust identification measures only to third parties that apply identification and monitoring measures equivalent to or stricter than those prescribed by the Law and are subject to adequate supervision.

(3) Transaction and customer activity monitoring measures prescribed by the Law and implementing regulations may not be outsourced. Obliged entities must fully carry out such monitoring independently within their regular operations.

(4) If an obliged entity entrusts certain customer identification measures to a third party, it shall not be relieved of responsibility for their proper execution in accordance with the Law and applicable international standards.

CHAPTER IV – ENHANCED CUSTOMER IDENTIFICATION AND MONITORING MEASURES

Article 20
(Enhanced Customer Identification and Monitoring)

(1) The obliged entity must apply enhanced identification and monitoring measures in cases referred to in Article 29 of the Law to manage and mitigate such risks appropriately.

(2) Enhanced measures, including identification of the beneficial owner, authorized representative, and beneficiary of funds involved in the transaction, are applied in addition to regular customer identification and monitoring measures.

Article 21
(Additional Identification Information Required Under Other Regulations)

(1) In addition to the requirements of the Law, this Rulebook, and decisions and guidelines of competent authorities and/or supervisory bodies, the obliged entity may request additional information, data, and documentation to fulfill identification obligations where high risk is assessed.

(2) Other laws and regulations may prescribe stricter identification obligations, in which case those provisions shall apply.

Article 22
(Limitation on Reliance on Client Statements Regarding Politically Exposed Person Status)

(1) The obliged entity must not base the identification of politically exposed persons solely on a client's statement regarding their politically exposed status.

(2) A client's statement may be used as a supplementary source of information but does not constitute sufficient proof of whether the client is or is not a politically exposed person.

(3) Obliged entities must use additional sources to verify the client's status, including but not limited to:

a) publicly available databases and official sources of competent institutions and authorities;
b) commercial databases, subject to prior assessment of their reliability;
c) open sources such as media and official announcements;
d) internal databases and information exchange within a group, where applicable and lawful;
e) asset declaration registers of public officials.

Article 23
(Enhanced Due Diligence and Monitoring Measures Applied to Politically Exposed Persons)

(1) When an obliged entity determines that a client, the beneficial owner of a client, a person authorized to represent and act on behalf of the client, or a person authorized to dispose of funds in the account of a legal entity client is a politically exposed person (PEP), it shall:

a) take appropriate measures to determine the source of assets and the source of funds to be used in the business relationship or occasional transaction, in order to mitigate risk;

b) obtain approval from senior management for establishing or continuing the business relationship;

c) apply enhanced due diligence measures and ongoing monitoring of transactions and risks associated with the business relationship, whereby the frequency of ongoing monitoring shall be aligned with the level of risk associated with the business relationship;

d) identify unusual transactions and continuously review available information to ensure that any new information that could affect the risk assessment is identified in a timely manner.

(2) The scope and intensity of measures for determining the source of assets and source of funds shall depend on the level of risk associated with the business relationship or occasional transaction.

(3) Where the risk associated with a business relationship or occasional transaction with a politically exposed person is particularly high, the obliged entity shall verify the source of assets and source of funds on the basis of reliable and independent data, documentation, or information.

(4) The obliged entity shall prescribe, through internal policies, the procedure for approving the establishment or continuation of a business relationship with a politically exposed person.

(5) When deciding on the establishment or continuation of a business relationship, senior management shall take into account the level of risk to which the obliged entity would be exposed by establishing or continuing that business relationship, as well as the entity's ability to effectively manage that risk.

(6) The obliged entity shall apply all measures referred to in this Article to politically exposed persons, their family members, and known close associates of politically

exposed persons as defined in Article 34 of the Law, and shall adjust the scope and intensity of such measures in accordance with the level of risk.

Article 24
(Monitoring of Politically Exposed Persons)

When implementing enhanced due diligence and monitoring measures in relation to politically exposed persons, obliged entities shall consider additional factors, and shall determine whether the politically exposed person:

a) has business interests related to their public functions, i.e., whether there is a conflict of interest;

b) is involved in public procurement processes;

c) holds multiple related or unrelated prominent public functions that may enable influence over several key decision-making points, particularly in departments responsible for spending and procurement;

d) comes from a country for which the FATF or another relevant body has determined that it has strategic deficiencies in its anti-money laundering or counter-terrorist financing regime, or is known to have a high level of corruption, as well as from a country listed as having strategic deficiencies or a higher likelihood of money laundering and terrorist financing as referred to in Article 37 of this Rulebook;

e) holds a prominent public function in sectors known to be exposed to higher levels of corruption, such as the oil and gas, mining, construction, natural resources, defense industry, sports, games of chance, and gambling sectors;

f) holds a prominent public function that could enable them to negatively influence the effective implementation of FATF recommendations in their country.

Article 25
(List of Functions and Indicators of Political Exposure)

(1) Obliged entities shall use an up-to-date list of functions and public positions indicative of political exposure when assessing whether a client is a politically exposed person.

(2) The list of functions includes, among others:

a) elected and appointed holders of the highest executive, legislative, judicial, and diplomatic functions in Bosnia and Herzegovina and abroad;

b) members of management and supervisory boards and directors of companies majority-owned by Bosnia and Herzegovina, the entities, the district, and municipalities;

c) members of political party leadership bodies;

d) senior military and security officials;

e) family members and close associates of the persons referred to in this paragraph.

(3) Close associates of a politically exposed person referred to in paragraph (2) of this Article shall be considered natural persons known to:

a) have or have had a close business relationship with a politically exposed person, including:

1. joint ownership of a legal entity or legal arrangement;
2. joint management of business projects or investments;
3. formal or informal business cooperation of significant scope;

b) benefit from the same legal arrangements as the politically exposed person, including joint beneficial ownership of a trust, fund, account, company, or other legal entity;

c) have a known personal relationship with the politically exposed person, including:

1. persons who frequently travel, reside, or appear publicly with the politically exposed person;
2. persons performing the function of personal advisor, assistant, asset manager, or other personal trustee.

(4) Obliged entities shall establish and regularly update internal lists and use available sources to ensure timely identification of the political status of their clients.

(5) For the purpose of implementing enhanced due diligence and monitoring measures in relation to politically exposed persons, family members of politically exposed persons shall include:

a) parents and children of the politically exposed person;

b) spouse or common-law partner;

c) brothers and sisters;

d) grandfathers, grandmothers, and grandchildren;

e) father-in-law, mother-in-law, son-in-law, and daughter-in-law;

f) adoptive parents and adopted children;

g) other persons living in the same household as the politically exposed person and related by blood or marriage.

Article 26
(Enhanced Due Diligence and Monitoring Measures Applied to Complex, Unusual, and Atypical Transactions)

(1) The obliged entity shall establish appropriate policies and procedures for detecting complex, unusual, or atypical transactions or patterns of transactions. When, in accordance with such policies and procedures, it detects transactions that are complex, unusual, or atypical and sees no clear economic or legal purpose of the transaction or doubts the accuracy of the information provided, the obliged entity shall apply enhanced due diligence and monitoring measures.

(2) Enhanced due diligence and monitoring measures shall be sufficient to enable the obliged entity to determine whether unusual or atypical transactions give rise to suspicion. In addition to the measures set out in Article 33 of the Law, such measures shall include at least:

a) taking justified and appropriate measures to understand the background and purpose of the transactions, for example by determining the source and destination of funds, collecting additional information about the client's business activities to assess the likelihood of such transactions for that client, collecting additional information about the relationship between the ordering party and the beneficiary, etc.;

b) more frequent monitoring of the business relationship and subsequent transactions and paying greater attention to details. The obliged entity shall decide to monitor individual transactions where proportionate to the identified risk.

Article 27
(Enhanced Due Diligence and Monitoring Measures Applied to Clients from Countries with Strategic Deficiencies and Countries with a Higher Likelihood of Money Laundering, Terrorist Financing, and Other High-Risk Situations)

(1) When a client is from a country with strategic deficiencies or a country with a higher likelihood of money laundering or terrorist financing as referred to in Article 37 of this Rulebook, or when a transaction involves such countries, and in all other high-risk situations, the obliged entity shall, through internal policies, prescribe enhanced due diligence and monitoring measures appropriate for the specific high-risk situation,

taking into account those prescribed in Article 35 of the Law and this Rulebook, and shall apply them consistently.

(2) The appropriate type of enhanced due diligence and monitoring, including the scope of additional information requested and the extent of increased oversight, shall depend on the reason why a particular occasional transaction or business relationship is classified as high-risk.

(3) The obliged entity is not required, in all cases where a client is from a country with strategic deficiencies or a country with a higher likelihood of money laundering or terrorist financing, or in other high-risk situations, to apply all enhanced due diligence and monitoring measures listed below, as in certain high-risk situations it may be sufficient to focus on enhanced ongoing monitoring throughout the business relationship.

(4) When determining enhanced due diligence and monitoring measures in such cases, the obliged entity shall consider:

a) increasing the amount of information collected for identification and monitoring purposes, including:

1. information on the identity of the client and the beneficial owner or the ownership and control structure of the client to ensure a full understanding of the risk associated with the business relationship. This may include gathering and assessing information on the reputation of the client or beneficial owner and evaluating any negative allegations against them, for example:
    1. information about family members and close business partners;
    2. information about past and current business activities of the client or beneficial owner;
    3. media searches for adverse reports;
2. information on the intended nature of the business relationship to determine whether the nature and purpose are legitimate and to create a more complete risk profile of the client, for example:
    1. number, value, or frequency of expected transactions to detect deviations that may raise suspicion, and, where appropriate, request evidence and documentation from the client;
    2. the reason the client requests a specific product or service, especially when it is unclear why the client's needs cannot be better met in another way or in another country;
    3. the destination of funds;

4. the nature of the client's or beneficial owner's business to better understand the business relationship or the purpose of an occasional transaction, including information on the client's connection with the ordering or receiving party.

b) increasing the quality of information collected to verify the identity of the client or beneficial owner, including:

1. requiring the first payment to be made through an account opened in the client's name at a financial institution in Bosnia and Herzegovina or at a credit institution in an EU Member State or a third country that applies measures in accordance with EU directives and regulations;
2. verifying that the client's assets and funds used in the business relationship or for occasional transactions do not originate from criminal activity and that the source of assets and funds is consistent with the obliged entity's knowledge of the client and the nature of the business relationship. In certain cases, where the risk associated with the business relationship or occasional transaction is particularly high, verification of the source of assets and funds may be the only appropriate risk mitigation measure. The source can be verified, for example, by comparing with VAT and profit tax returns, copies of audited reports, payrolls, or public documents issued by competent authorities.

c) increasing the frequency of monitoring to ensure the obliged entity can manage the risk associated with an individual business relationship or occasional transaction, or conclude that the business relationship exceeds the entity's risk appetite, and to identify transactions requiring further review, including:

1. increasing the frequency of monitoring the business relationship and occasional transactions to detect potential changes in the client's risk profile and the entity's ability to continue managing that risk;
2. obtaining approval from senior management for establishing or continuing the business relationship to ensure that senior management is aware of the risk to which the obliged entity is exposed and can make an informed decision about managing that risk;
3. conducting more frequent reviews of the business relationship to ensure any changes in the client's risk profile are identified, assess the entity's ability to manage that risk, and take necessary measures if required;
4. conducting more frequent or detailed transaction monitoring to identify any unusual or atypical transactions that may raise suspicion. Transaction monitoring may include, as needed, determining the destination of funds or the rationale for certain transactions.

CHAPTER V – SIMPLIFIED CLIENT IDENTIFICATION AND MONITORING

Article 28
(Cases Where Simplified Identification and Monitoring Measures May Be Applied)

(1) Obliged entities may apply simplified identification and monitoring measures when establishing a business relationship with clients who are:

a) competent authorities and public administration institutions, regardless of administrative level (state, entity, district, canton, municipality);

b) public enterprises and institutions founded by competent authorities and public administration institutions referred to in point (a);

c) obliged entities implementing anti-money laundering and counter-terrorist financing measures, overseen by competent authorities and agencies established under special laws;

d) other clients, legal or natural persons, for whom the obliged entity determines, based on a risk assessment, that they present low risk.

(2) Obliged entities may apply simplified identification and monitoring measures to an occasional transaction assessed as low-risk, taking into account the results of the assessment.

(3) Obliged entities must collect sufficient information to determine whether the client qualifies for simplified identification and monitoring measures, including assessment results.

(4) If there is suspicion of money laundering, terrorist financing, or financing of proliferation of weapons of mass destruction related to a client, transaction, or service where simplified measures were applied, the obliged entity must conduct an additional assessment and apply enhanced measures.

(5) Obliged entities must collect and verify, by reviewing originals or certified copies of valid documents or records, the legally required client data and information, such as identification documents, registry extracts, other business documentation, or as otherwise prescribed by law, considering completed risk analyses.

(6) When performing simplified identification and monitoring, the obliged entity must establish an adequate level of business monitoring to detect unusual and suspicious transactions.

Article 29
(Measures for Simplified Client Identification and Monitoring)

(1) When implementing simplified identification and monitoring, the obliged entity must carry out all client identification and monitoring measures prescribed in Article 15 of the Law.

(2) If the business relationship or occasional transaction is categorized as low-risk, the obliged entity may adjust the scope, timing, or type of certain or all client identification and monitoring measures in a manner appropriate for that risk category.

(3) Simplified identification and monitoring measures may include, but are not limited to:

a) adjusting the timing of identification and monitoring, e.g., when the requested product or transaction has features that limit its use for money laundering or terrorist financing purposes:

1. verifying the client's and/or beneficial owner's identity when establishing the business relationship;
2. verifying the client's and/or beneficial owner's identity when transactions exceed an internally established threshold or after a reasonable period. In such cases, the obliged entity must ensure:
    1. that this does not result in an exemption from client identification and monitoring;
    2. that the identity of the client and beneficial owner is ultimately verified;
    3. that the threshold or time limit is set at a reasonably low level;
    4. that systems are in place to detect threshold or time limit breaches;
    5. that client identification and monitoring are not delayed when legislation in Bosnia and Herzegovina or EU regulations require collection of such information.

b) adjusting the amount of information collected for identification, verification, or monitoring, e.g., verifying identity based on a single reliable, credible, and independent document or data source, or assuming the nature and purpose of the business relationship when the product is designed for a single purpose;

c) adjusting the quality or source of information collected for identification, verification, or monitoring, e.g.:

1. accepting information provided by the client instead of an independent source when verifying the identity of the beneficial owner if, for objective reasons, it is impossible to obtain independent sources;
2. relying on the source of funds to meet some client identification and monitoring requirements when all aspects of the business relationship present low risk, e.g., budgetary funds.

(4) Information collected under simplified measures must provide reasonable assurance that the low-risk assessment of the business relationship or occasional transaction is justified and provide sufficient information on the nature of the business relationship or transaction to identify unusual or suspicious transactions.

(5) The obliged entity must not apply simplified identification and monitoring measures where there are reasons to suspect money laundering, terrorist financing, or financing of the proliferation of weapons of mass destruction related to the client, transaction, assets, or funds, in which case enhanced measures for high-risk, complex, or unusual transactions under Article 33, paragraph (1) of the Law must be applied.

Article 30
(Use of Copies for Identification)

(1) For all original documents, including identification documents, which cannot be retained by the obliged entity, the entity shall review them and make copies or scans in the manner prescribed by Article 15 of the Law.

(2) In the case of foreign documents, not relying solely on identification documents, which are collected in the process of client identification and for transactions not written in one of the languages used in Bosnia and Herzegovina, the obliged entity shall obtain from the client a translation certified by an authorized court interpreter.

Article 31
(Updating Documentation)

(1) Obliged entities shall ensure the validity and relevance of information, data, and documentation that form the basis for client and transaction identification by conducting regular checks of existing documents during the business relationship. In the case of significant transactions, significant changes in the client's transaction patterns, or other material changes that require re-assessment, new or additional information and documentation for identification must be requested and/or collected.

(2) For clients with whom the obliged entity has previously established a business relationship, conducted client identification and monitoring measures, and provided

the client access to products or services via electronic distribution channels with all applicable protection and authentication elements, the obliged entity may obtain a valid identification document from the client through such a distribution channel during the business relationship if it has expired since the establishment of the relationship, ensuring a record of the date and time the updated document was obtained.

Article 32
(Use of Software for Additional Client Identification and Monitoring)

(1) Financial institutions, for the purpose of implementing legally prescribed measures, risk assessment, client identification and monitoring, and enforcement of UN sanctions and Bosnia and Herzegovina's counter-terrorism measures, must establish information/computer systems that enable efficient application of these measures.

(2) Other obliged entities must also establish information/computer systems referred to in paragraph (1) when the supervisory authority assesses that it is necessary, considering the size and nature of the entity's business.

CHAPTER VI – REPORTING TO FOO, RELATED CASH TRANSACTIONS, SUBMISSION OF DOCUMENTS AND DATA

Article 33
(Exemption from Reporting Cash and Related Cash Transactions)

(1) The obliged entity is not required to provide the FOO with information on every cash or related cash transaction whose total value equals or exceeds BAM 30,000 (or equivalent), in the case of daily deposit of sales proceeds from goods and services of clients referred to in paragraph (2) of this Article, except where there is suspicion of money laundering.

(2) A client performing a transaction under paragraph (1) is:

a) a public enterprise;
b) direct and indirect users of budgetary funds at all levels of government in Bosnia and Herzegovina, including local government units and mandatory social security organizations, which are part of the consolidated treasury account system.

(3) The obliged entity is not required to report to the FOO a cash or related cash transaction whose total value equals or exceeds BAM 30,000 (or foreign currency equivalent) when:

a) transferring money between accounts of the same client at the same obliged entity;
b) exchanging currency within the client's account while the money remains in the

client's account at the obliged entity;
c) re-depositing money within the client's account for the purpose of re-investment at the obliged entity.

Article 34
(Submission of Documents)

(1) In addition to the documents referred to in Article 44 points a) and b) of the Law, notaries, lawyers, and law firms are obliged, under Article 44 point c), to provide the FOO with all documents drawn up for the purpose of transferring rights of management and disposal of assets, including:

a) documents intended to gift money in the amount of BAM 30,000 or more;
b) documents intended to transfer membership shares in companies, regardless of the company's capital;
c) documents intended to transfer rights of management or disposal of company assets.

(2) If there is suspicion of money laundering, terrorist financing, or financing the proliferation of weapons of mass destruction, the notary is obliged to provide the FOO with information and data when notarizing documents involving the transfer or acquisition of ownership or other real rights in real estate, certifying documents, notarizing and/or certifying signatures on loan agreements or transfer of company membership shares, and in all other relevant situations.

Article 35
(Content and Layout of Account Transaction Records Submitted by Banks to FOO and Other Authorities)

(1) The obliged entity under Article 5 paragraph (1) point a) of the Law and other entities authorized to open and maintain accounts for payment operations shall submit client account transaction records, when reporting suspicious transactions and responding to requests from the FOO and competent authorities, in electronic Excel format, organized to allow further analytical processing, containing accurate and complete data arranged in the following column order:

a) transaction date;
b) ordering party;
c) ordering party account number;
d) recipient;
e) recipient account number;
f) debit;

g) credit;
h) balance;
i) transaction description/purpose;
j) indication whether it is a cash or non-cash transaction.

(2) The deadline for implementing the activities referred to in paragraph (1) is six months from the adoption of this Rulebook.

Article 36
(Monitoring of Related Cash Transactions)

(1) To detect transactions conducted in smaller amounts that do not exceed the thresholds set out in Articles 12 and 43 of the Law, intended to circumvent identification and reporting, it is necessary to establish a system capable of recognizing related cash transactions.

(2) The period for monitoring related cash transactions cannot be limited to a specific time frame.

(3) Obliged entities shall, in accordance with risk assessment, client profile, transaction frequency, and transaction amount, define in their internal acts the activities and measures to be taken to monitor related cash transactions.

(4) Exceptionally from paragraph (2), authorized exchangers must monitor occasional transactions under Article 19 paragraph (5) point b) of the Law for a period of 30 days, except when there is suspicion of money laundering or terrorist financing.

CHAPTER VII – COUNTRIES WITH STRATEGIC DEFICIENCIES AND COUNTRIES WITH HIGHER RISK OF MONEY LAUNDERING AND TERRORIST FINANCING

Article 37
(Countries with Strategic Deficiencies and Countries with Higher Risk of Money Laundering and Terrorist Financing)

(1) Countries with strategic deficiencies under Article 86 paragraph (1) point a) of the Law are those listed:

a) in FATF statements on countries with strategic deficiencies in their anti-money laundering and counter-terrorist financing systems that pose a risk to the international financial system;

b) in FATF statements on countries/jurisdictions with strategic deficiencies that, in order to address identified deficiencies, have expressed political commitment at the highest

level, have created an action plan with FATF, and are obliged to report progress on addressing these deficiencies.

(2) Countries with a higher risk of money laundering, terrorist financing, and/or financing of proliferation of weapons of mass destruction under Article 86 paragraph (1) point b) of the Law shall be determined by the Council of Ministers of Bosnia and Herzegovina upon the proposal of the Ministry of Security, in cooperation with the Standing Coordination Body and competent authorities, considering results of risk assessments and other credible sources such as:

a) EU data on high-risk third countries regarding anti-money laundering and terrorist financing, if not already included in paragraph (1);

b) OECD data on countries with insufficient tax transparency;

c) EU data on countries assessed as not fully complying with international tax standards;

d) UNODC data on countries producing raw materials for illegal drug production or with known organized drug trade;

e) credible sources on countries with significant levels of corruption;

f) UN and other credible sources on countries subject to international restrictive measures or linked to terrorism and terrorist financing.

(3) The list of countries under paragraph (1) shall be published by the FOO and competent supervisory authorities on their websites.

(4) The list of countries under paragraph (2) shall be provided to obliged entities under Article 5 of the Law through competent supervisory authorities and shall not be publicly disclosed.

(5) The lists under paragraphs (1) and (2) are mandatory for applying the legally prescribed measures for client identification and reporting transactions to the FOO.

(6) Obliged entities shall, in addition to the countries in paragraphs (1) and (2), apply appropriate identification measures to other countries assessed as high-risk based on their own risk assessment.

CHAPTER VIII – INTERNAL CONTROL AND AUDIT, AUTHORIZED PERSON, AND TRAINING

Article 38
(Purpose of Internal Control and Obligation to Verify Adopted Procedures)

(1) The purpose of internal control under Articles 55 and 56 of the Law is to prevent, timely detect, and eliminate deficiencies in Law implementation and to improve internal systems for detecting persons and transactions suspected of money laundering, terrorist financing, or financing the proliferation of weapons of mass destruction.

(2) The obliged entity must establish an internal control system that ensures regular checks of adopted procedures and the functioning of systems to prevent money laundering, terrorist financing, or financing proliferation of weapons of mass destruction.

Article 39
(Obligation to Align Procedures)

(1) In case of changes in the business process of the obliged entity, such as organizational changes, changes in business procedures, or introduction of new services or products, the entity is obliged to verify and align its procedures within the internal control system to ensure compliance with the Law.

(2) Verification of compliance of systems and procedures for implementing the Law, as well as the application of those procedures, must be conducted at least once a year and whenever there is a significant change under paragraph (1), no later than the day the change is introduced in the business.

Article 40
(Responsibility for Organizing Internal Control and Audit)

(1) The obliged entity and its senior management are responsible for ensuring and organizing internal control and internal audits in accordance with the Law.

(2) The entity, by its act, shall define the authority and responsibilities of governing bodies, organizational units, authorized persons, and other personnel in performing internal control, as well as the manner and schedule of internal control implementation.

Article 41
(Annual Report on Internal Audit and Measures Taken)

(1) An obliged entity required under Article 55 paragraph (2) of the Law to organize internal audits must ensure the preparation of an annual report on the internal audit performed and measures taken after the audit, at least once a year. The interval

between consecutive audits and the adoption of reports by competent bodies shall not exceed 12 months.

(2) The annual report shall include at least:

a) total number of reports to the FOO on suspicious, cash, related cash, and non-cash transactions under Articles 42 and 43 of the Law, and assessment of the quality, timeliness, and compliance of these reports with identified threats in the AML/CFT Risk Assessment in Bosnia and Herzegovina;

b) total number of persons or transactions suspected of money laundering, terrorist financing, or financing proliferation of weapons of mass destruction reported to the authorized person by employees but not reported to FOO;

c) total number of business relationships where client identity was established via qualified electronic certificates for electronic signatures or seals, or via video electronic identification, and total number of relationships established via power of attorney;

d) frequency of use of individual indicators for detecting suspicious transactions reported by employees to the authorized person;

e) evaluation of internal control system functioning;

f) measures taken based on recommendations from internal audits;

g) internal IT audit results regarding: protection of electronically transmitted data and storage of client and transaction data in centralized databases;

h) adequacy of training and evaluation of topics for further employee training and development;

i) measures taken to protect personal and confidential data;

j) total number of business relationships where a third party was entrusted with specific identification measures;

k) total number of persons and transactions subject to international restrictive measures.

(3) The obliged entity must submit the report under paragraph (1) to the authorities supervising the Law, upon request, within three days of the request.

Article 42
(Data and Documentation for Registration of the Authorized Person/Obliged Entity in the AMLS System)

(1) For the purpose of registering an obliged entity in the AMLS system, the obliged entity referred to in Article 5 of the Law shall submit to the FOO a decision on the appointment or change of the authorized person and their deputy, containing the following information:

a) full name of the responsible person – a member of senior management responsible for implementation of the Law;
b) full name of the authorized person and their deputy;
c) contact telephone number and email address of the responsible person, the authorized person, and the deputy authorized person;
d) name, address, and registered seat of the obliged entity;
e) unique identification number (JIB) of the obliged entity.

(2) In addition to the data referred to in paragraph (1), all obliged entities except financial institutions must, upon initial registration, also submit to the FOO copies of the following documentation:

a) current extract from the court register or decision of the competent authority;
b) notification on classification of the business entity by activity;
c) foreign exchange operations agreement, if applicable.

(3) The data and documentation referred to in paragraphs (1) and (2) shall be submitted to the FOO by post or electronically.

Article 43
(Obligation to Conduct Training)

(1) Obliged entities shall ensure continuous and adequate training of their employees regarding the prevention of money laundering, terrorist financing, and financing of the proliferation of weapons of mass destruction, in accordance with relevant legislation and internal policies.

(2) All new employees must undergo initial training on the basic principles of anti-money laundering and counter-terrorist financing within 60 days of assuming their position.

(3) Through training programs, obliged entities must ensure that employees covered by the AML/CFT program fully understand the importance and necessity of effectively implementing the “Know Your Customer” (KYC) policy and apply it in performing their duties.

Article 44
(Content and Frequency of Training)

(1) Training must be tailored to employees' job responsibilities and include at least the following topics:

a) definition and basic concepts of money laundering, terrorist financing, and financing of the proliferation of weapons of mass destruction;
b) legal framework and obligations of obliged entities;
c) risk assessment and application of the risk-based approach;
d) internal policies and procedures, including client identification and transaction monitoring measures;
e) indicators of suspicious transactions and reporting procedures;
f) specific characteristics of products and services offered that may be subject to misuse;
g) internal control system.

(2) Training shall be conducted at least once a year, with additional sessions when required due to regulatory changes, internal or external supervisory findings, or introduction of new products and services.

(3) Obliged entities shall organize specialized training adapted to the actual needs of organizational units, positions, or functions, at a minimum including:

a) newly employed staff;
b) client-facing staff;
c) operational staff;
d) compliance and internal control staff;
e) senior management and top management.

Article 45
(Record-Keeping and Evaluation of Training Effectiveness)

(1) Obliged entities shall maintain records of conducted training sessions, including date, duration, content, list of participants, and description of job positions or functions.

(2) In case of unjustified absence from training, the obliged entity shall take appropriate measures, including disciplinary procedures in accordance with internal rules.

(3) Obliged entities shall periodically assess the effectiveness of training and propose measures for its improvement.

CHAPTER IX – FINAL PROVISIONS

Article 46
(Alignment of Internal Legal Acts)

Obliged entities shall harmonize their internal legal acts with this Rulebook within 90 days from the date of its entry into force.

Article 47
(Repeal)

Upon entry into force of this Rulebook, the Rulebook on Implementation of the Law on Prevention of Money Laundering and Financing of Terrorist Activities ("Official Gazette of BiH", Nos. 41/15 and 24/23) shall cease to apply.

Article 48
(Entry into Force)

This Rulebook shall enter into force on the eighth day following its publication in the "Official Gazette of BiH".