Pursuant to Article 5, Paragraph 1, Item b), Article 20, Paragraph 2, Item b) and Article 37 of the Law on the Banking Agency of Republika Srpska ("Official Gazette of Republika Srpska", No. 59/13 and 4/17), Article 6, Paragraph 1, Item b) and Article 19, Paragraph 1, Item b) of the Statute of the Banking Agency of Republika Srpska ("Official Gazette of Republika Srpska", No. 63/17), and pursuant to Articles 93 and 101 of the Law on anti-money laundering and counter-terrorism financing ("Official Gazette of BiH", No. 13/24), the Management Board of the Banking Agency of Republika Srpska, at its 6th session held on 28 February 2024, adopted the

# DECISION
## on managing money laundering and terrorism financing risk

### 1. General provisions

**Article**

**Subject of the Decision**

This Decision shall stipulate:

(1) the minimum scope, form and content of the activities of the reporting entities to prevent money laundering and the financing of terrorist activities,

(2) the rules of organization, management and responsibility of the bodies, functions and other employed reporting entities,

(3) the procedure for assessing the risk of the entire business operations and individual risk assessments,

(4) the method of implementing measures for identifying and monitoring client transactions and activities, and

(5) the management of isolated or special risks that are characteristic of the business model, products or services of the reporting entities.

**Article 2**

**Use of definitions**

(1) Definitions used in this Decision shall have the same meaning as in the Law on anti-money laundering and counter-terrorism financing (hereinafter: the Law on AML/CFT) and other by-laws of the Banking Agency of Republika Srpska in which they are defined.

(2) Particular definitions used in this Decision, which are not covered by the regulations referred to in Paragraph 1 of this Article, shall have the following meaning:

1) **Money laundering and terrorism financing risk** is the risk of the possibility of money laundering and terrorist financing and proliferation of weapons of mass destruction, and refers to the level of risk that exists before the application of risk mitigation measures,
2) **Inherent risk** is the level of risk before risk mitigation,
3) **Residual risk is** the level of risk that remains after risk mitigation,
4) **Emerging risk** is a risk that has never been identified before or an existing risk that has increased significantly,
5) **Risk factors** are variables that, by themselves or in combination, may increase or decrease the risk posed by a particular individual business relation or occasional transaction,
6) **Funding source** is the origin of the funds involved in a business relation or occasional transaction. It also includes the activity that generated the funds used in the business relation (e.g., the client's salary, earnings),
7) **The source of assets** represents the origin of the client's total assets (e.g., gift, inheritance, or savings),
8) **The assessment of money laundering and terrorist financing risk in Bosnia and Herzegovina** is a comprehensive risk analysis carried out by the competent authorities, which

considers the risks of money laundering and terrorist financing and the proliferation of weapons of mass destruction in Bosnia and Herzegovina,

9) **The regulated entity's clients** are persons who/which establish or already have an established business relation with the regulated entity or carry out an occasional transaction, persons in whose name or for whose benefit a business relation is established or a transaction is carried out and persons who/which carry out transactions through various types of intermediaries,
10) **Electronic money** means an electronically (including magnetically) stored monetary value that constitutes a monetary claim against the issuer of that money, and is issued after receiving cash funds for the purpose of carrying out payment transactions and is accepted by a private individual or a legal entity who/which is not the issuer of that money, whereby electronic money does not include a digital record of a currency that it did not issue and whose value is not guaranteed by a central bank or other public sector entity, and which does not have the legal status of money or currency,
11) **An occasional transaction** is a transaction that is not carried out within the framework of an established business relation,
12) **Supervisory / management board** is a body in accordance with the relevant laws, supervising the business operations of the regulated entity and the work of the top management,
13) **Top management** is represented by persons who, in accordance with the relevant laws, manage and organize the business operations of the regulated entity and are responsible for the legality of the work and
14) **Transfer by means of a batch file** is a set of several individual transfers of cash funds combined for the purpose of the transfer,
15) **Dual-use goods** means goods, including software and technology, which can be used for both civilian and military purposes, and goods which can be used for non-explosive purposes, but which can in any way assist in the production of nuclear weapons or other nuclear explosive devices.

**Article 3**

**Regulated entities obliged to apply**

(1) The provisions of this Decision shall apply to the following regulated entities:
1) banks and banking groups,
2) microcredit organizations,
3) leasing providers,
4) electronic money institutions and
5) other financial organizations that are required by law to operate under the supervision of the Banking Agency of Republika Srpska (hereinafter: the Agency).

(2) The provisions of this Decision shall be applied by all regulated entities referred to in Paragraph 1 of this Article, while the Guidelines for the analysis and assessment of risks in the application of the Decision and managing money laundering and terrorism financing risk (hereinafter: the Guidelines) shall be applied by those regulated entities to which that part applies, taking into account the specific circumstances related to client risk, product, service or transaction risk, geographical risk and the risk of the method of establishing and conducting a business relation and which apply only to those regulated entities.

## 2. Organization, management, responsibility

**Article 4**

**Responsibility of the regulated entity authorities**

(1) The supervisory/management board and the top management of the regulated entity (hereinafter: the regulated entity authorities) shall be obliged to establish an adequate system that will ensure the regulated entity's commitment to a high level of corporate governance, which includes the establishment of adequate mechanisms for combating money laundering, the financing of terrorist

activities and the proliferation of weapons of mass destruction, in all organizational units of the regulated entity and in all business lines.

(2) The regulated entity's authorities shall promote the integrity of the authorized person and a high level of corporate governance standards in communication with the regulated entity's employees, all with the aim of quality risk management.

(3) The regulated entity's authorities shall ensure the implementation of comprehensive controls that will ensure that the Program referred to in Article 14 of this Decision is fully implemented in practice, and shall regularly monitor and verify the adequacy and effectiveness of the established comprehensive controls.

(4) The regulated entity's procedures should be efficient and include regular procedures for appropriate and successful supervision by the regulated entity's top management, internal control systems, internal audit, segregation of duties, training of relevant employees and other segments closely related to this area.

(5) For the implementation of the regulated entity's policies and procedures, the regulated entity's Program must clearly define responsibilities and divide them into appropriate holders, i.e. appropriate organizational units or functions, top management, other management and other employees of the regulated entity.

(6) In the case where the regulated entity is a member of a banking/financial group, the regulated entity's Authorities, in addition to the responsibility for the compliance of risk management policies and procedures with legal and regulatory provisions, also have the responsibility for monitoring compliance with policies and procedures adopted at the level of the banking/financial group.

**Article 5**

**Authorized persons**

(1) The supervisory/management body of the regulated entity shall be obliged to appoint an authorized person at the management level who shall meet the conditions for appointment stipulated by the Law on AML/CFT, which may include the appointment of one or more deputies of the authorized person.

(2) The regulated entities shall be obliged to estimate the number of employees required to perform the tasks of preventing money laundering and terrorist financing, in proportion to the size, type, scope and complexity of the tasks they perform, and to ensure the conditions and means for performing these tasks.

(3) The regulated entities shall be obliged to provide the authorized person with:
1) at least two officers, in the case of regulated entities referred to in Article 3, Paragraph 1, Item 1, and in the case of other regulated entities referred to in Article 3 of this Decision, at least one officer. In larger regulated entities, it is necessary to assess the need for the engagement of more officers,
2) the authorities to issue orders to employees to implement measures, actions and procedures referred to in the Law on AML/CFT, regulations and the Program, and to report thereon to the regulated entity's bodies,
3) daily full and direct access to data, information and documentation necessary for the performance of tasks within their competences,
4) direct contact with the regulated entity's bodies and
5) to receive reports on significant, unusual and suspicious transactions and client activities in a timely manner.

(4) For regulated entities with four or fewer employees, if not appointed, the authorized person shall be considered to be the legal representative or other person who manages the regulated entity's operations, or the responsible person of the regulated entity according to legal regulations.

(5) The regulated entities shall ensure the presence of an authorized person during on-site supervision and ensure that the authorized person communicates directly with the Agency's representatives and provides them with all necessary assistance for the unhindered performance of on-site supervision.

**Article 6**

**Obligations and responsibilities of authorized persons**

(1) The authorized person is responsible for performing the following tasks:

1) ensure, monitor and coordinate the activities of the regulated entity in order to ensure compliance of the regulated entities's operations with the provisions of the Law on AML/CFT and by-laws,
2) at least annually assess the adequacy of the Program, policy and procedures, verify the risk assessment and provide the Supervisory/Management Board with proposals for their updating or improvement,
3) at least quarterly submit a report to the regulated entities's bodies on the regulated entity's activities and compliance with the requirements for preventing money laundering and terrorist financing, as well as activities undertaken against detected suspicious clients for regulated entities referred to in Article 3, Paragraph 1, Item 1 of this Decision, and for other regulated entities referred to in Article 3, Paragraph 1 of this Decision at least once every six months,
4) ensure the proper and timely functioning of reporting lines,
5) participate in defining and changes to operational procedures and in the preparation of internal regulations concerning the prevention and detection of money laundering and the financing of terrorist activities,
6) participates in the development of guidelines for the implementation of controls related to the detection and prevention of money laundering and the financing of terrorist activities,
7) participates in the establishment and development of IT support in connection with activities related to the detection and prevention of money laundering and the financing of terrorist activities of the regulated entities,
8) include in its activities elements for an internal investigation into the responsibility of employees who have neglected their duties in this area,
9) prepare proposals for the supervisory/management board of the regulated entity for the improvement of the system for the detection and prevention of money laundering and the financing of terrorist activities of the regulated entity, and provide proposals for the elimination of identified weaknesses and shortcomings in the operations of the regulated entity and proposals for the improvement of the operations of the regulated entity,
10) provides support in activities conducted by the regulated entity's internal audit and
11) participates in the preparation of professional education and training programs for employees in the field of preventing and detecting money laundering and financing of terrorist activities.

(2) Deputies shall be obliged to perform all tasks referred to in Paragraph 1 of this Article in the absence of the authorized person, but also to perform all other tasks stipulated by the Law on AML/CFT and by-laws.

**Article 7**

**Training of regulated entity's employees**

(1) The regulated entities shall be obliged to ensure ongoing training of all employees covered by the program for the prevention of money laundering and the financing of terrorist activities. The content of this training must include at least the following topics from the area subject to this Decision:

1) the legal obligations of the regulated entity and obligations under other regulations,
2) the program, policies and procedures of the regulated entity,
3) detailed elements of the “Know Your Client” policy,
4) danger of money laundering and the risks for the regulated entity and the personal responsibilities of employees,
5) the capabilities and weaknesses of financial institutions in preventing money laundering and the financing of terrorist activities and the proliferation of weapons of mass destruction,
6) the responsibilities and powers of the regulated entity's authorized persons,
7) the internal control system and

8) the internal audit system.

(2) The regulated entities should adapt the frequency and topics of training referred to in the previous Paragraph to the real needs of their specific organizational units, functions and/or employees. In order to timely comply with new requirements and familiarize themselves with new situations, as well as to maintain the knowledge and experience already acquired by their employees, the regulated entities shall be obliged to establish a regular training program.

(3) In deciding on the needs, type and scope of training referred to in Paragraph 2 of this Article, the regulated entities shall be obliged to adjust the focus of training depending on whether they are new employees who have direct contact with clients, employees who work with new clients, employees who control whether the work of the regulated entity is in compliance with the requirements of the Law on AML/CFT and other regulations, other board of directors, management and/or supervisory board, etc.

(4) Through training programs, the regulated entities shall be required to ensure that all relevant employees fully understand the importance and needs for the most successful implementation of the "Know Your Client" policy and that such understanding is the key to success in their implementation.

**Article 8**

**Internal reporting lines**

(1) The regulated entities shall adopt procedures for internal reporting to competent authorities on transactions, suspicious funds and suspicious clients stipulated by the Law on AML/CFT. Reporting lines within the regulated entity's organization must be clearly defined.

(2) The regulated entities shall establish an appropriate reporting system that will enable adequate communication, information exchange and cooperation at all organizational levels and relevant employees at all levels of the regulated entity, and provide timely, accurate and sufficiently detailed information necessary for effective risk management.

(3) The reporting system established by the regulated entity, in addition to regular reporting, should also enable timely informing of all relevant levels about identified deficiencies in the system for preventing money laundering and terrorist financing, corrective measures undertaken and deadlines set for their elimination.

(4) Internal reporting lines must be regular and efficient, accessible to all parts of the regulated entity and entities that have a reporting obligation, in accordance with internally stipulated reporting policies and procedures.

**Article 9**

**External reporting lines**

(1) The regulated entities shall adopt procedures for reporting to competent authorities outside the regulated entity, in accordance with the Law on AML/CFT and regulations adopted on the basis thereof, on all stipulated information and data.

(2) Information and data on suspicious transactions, funds and activities of clients that regulated entities submit to the State Investigation and Protection Agency - Financial Intelligence Unit (hereinafter: FIU) must be accurate, complete, concise and sufficient for further action.

(3) The regulated entities shall be obliged to fully and promptly fulfill their reporting obligations to competent institutions.

**Article 10**

**Internal audit**

(1) The internal audit of the regulated entity shall conduct a regular assessment of the risk management processes and systems in the regulated entity's operations in order to ensure that this risk is appropriately identified, measured, or assessed, monitored, analyzed and controlled, that it is adequately reported, and that appropriate measures are undertaken to limit and mitigate it.

(2) The compliance of the regulated entity's operations with the requirements of the Law on AML/CFT and regulations should be subject to an independent assessment by the internal audit function of the regulated entity, which includes an assessment of the adequacy of the regulated entity's policies, procedures, measures, actions and procedures.

**Article 11**

**Obligations and responsibilities of internal audit**

(1) In order to fulfill its tasks and obligations, the internal audit of the regulated entity shall be obliged to:

1) include in the reports the findings and assessments of the regulated entity's efficiency on all issues stipulated by the Law on AML/CFT and relevant regulations, programs, policies and procedures of the regulated entity that govern the regulated entity's obligations to prevent money laundering and the financing of terrorist activities and the proliferation of weapons of mass destruction in all segments of the regulated entity's business operations, including the adequacy of policies and procedures,
2) assess the implementation of measures for determining client eligibility and classifying clients into risk groups,
3) assess the implementation of client identification measures,
4) assess the implementation of measures for monitoring transactions and client activities, with a focus on distribution channels that allow a higher degree of anonymity,
5) assess the functioning of the internal control system,
6) assess the functioning of internal and external reporting lines,
7) assess the adequacy of the training provided and the application of restrictive measures,
8) prepare reports that should contain all information and reviews of the tested samples on the basis of which the assessment was given and
9) report its findings and assessments regularly, i.e. periodically, at least once a year, to the regulated entity's bodies in accordance with the Law on AML/CFT and other relevant regulations, and provide recommendations to the supervisory/management board and board of directors of the regulated entity for the improvement of the internal control system and operations of the regulated entity.

(2) In addition to the activities listed in Paragraph 1 of this Article, internal audit employees in regulated entities shall be required to pay attention to monitoring the activities that regulated entities are required to undertake based on the findings and assessments provided by internal audit, external audit and competent authorities.

**Article 12**

**Obligation to conduct external audit**

(1) The regulated entities shall be obliged to contract with independent audit firms to perform audits and assess compliance of operations with requirements for preventing money laundering and financing of terrorist activities and proliferation of weapons of mass destruction, with the mandatory use of testing techniques.

(2) In order to fulfill its tasks and obligations, the external auditor shall be obliged to provide an assessment on:

1) implementation of legal and other stipulated obligations of the regulated entity,
2) implementation of Programs, policies and procedures,
3) compliance with risk management rules,
4) adequacy of performance of control function operations,
5) information system adequacy,
6) timeliness, regularity, accuracy and completeness of reporting to competent authorities and
7) adequacy and efficiency of the internal control system regarding risk management.

(3) The contract with the external auditor shall be concluded in the manner and within the time limits defined by the regulations governing the audit of financial statements.

(4) After the audit, the external auditor shall prepare a report on the performed audit in one of the languages in official use in Republika Srpska. The report shall include the findings and assessments of the regulated entity's efficiency on all issues stipulated by the Law on AML/CFT and relevant regulations, programs, policies and procedures of the regulated entities governing the regulated entity's obligations to prevent money laundering and the financing of terrorist activities and the proliferation of weapons of mass destruction.

(5) The external auditor shall be obliged to inform the Agency and the supervisory/management board and the top management of the regulated entity in writing, without delay, on:

1) identified illegalities or facts and circumstances related to the prevention of money laundering and the financing of terrorist activities and the proliferation of weapons of mass destruction, which may in any way jeopardize the further operations of the regulated entity,
2) serious violation of internal acts,
3) significant weakness in the functioning of the internal control system and
4) facts that could lead to non-compliance of the regulated entity's operations with the requirements for the prevention of money laundering and the financing of terrorist activities and the proliferation of weapons of mass destruction.

(6) The provision of data to the Agency referred to in Paragraph 4 of this Article shall not be considered a breach of the auditor's obligation to maintain confidential information arising from the regulations governing the field of audit or from the contract.

(7) The external auditor shall, at the request of the Agency, submit in writing the necessary explanations regarding the audit report and other data required by the Agency for the performance of supervision.

**Article 13**

**Rejecting the audit report and limitations**

(1) If the Agency determines that the external audit of the segment of prevention of money laundering and financing of terrorist activities and proliferation of weapons of mass destruction has not been conducted or that the audit report has not been prepared in accordance with the Law on AML/CFT, by-laws adopted on the basis of the law, regulations governing accounting and auditing and in accordance with the rules of the auditing profession, or if it determines through the supervision of the business operations of the regulated entity or in another manner that the audit assessment is not based on true and objective facts, it may reject the audit report and require the regulated entity to have the audit conducted by authorized auditors of another audit firm or, when it deems it necessary, directly appoint an auditor itself, at the expense of the regulated entity.

(2) The audit firm and the authorized auditor performing the audit of the regulated entity may not be a person whose report on the audit of the prevention of money laundering and financing of terrorist activities and proliferation of weapons of mass destruction for the previous business year was not accepted by the Agency.

## 3. Internal acts

**Article 14**

**Program, policies and procedures**

(1) The regulated entities shall be obliged to adopt and implement appropriate internal acts and establish control procedures that, for the purpose of effective risk management, will include all actions and measures for the prevention and detection of money laundering, financing of terrorist activities and proliferation of weapons of mass destruction, which are defined by the Law on AML/CFT, by-laws adopted on the basis thereof, including the Money Laundering and Financing of Terrorist Activities Risk Assessment in Bosnia and Herzegovina.

(2) The regulated entities shall be obliged to adopt a Program for the implementation of activities referred to in Article 1 of this Decision, an integral part of which are appropriate policies and procedures.

(3) The regulated entities shall be obliged to fully implement the provisions of the Program, as well as all policies and procedures, at their headquarters, in all branches and other organizational units in the country and in all branches or other organizational units they have abroad. The regulated entities shall pay special attention to the activities of their branches and other organizational units abroad.

(4) By the acts referred to in Paragraph 1 of this Article and in their implementation, the regulated entities shall ensure high ethical and professional standards of responsible employees and effective prevention of the possibility of them being misused for the purpose of money laundering or financing of terrorist activities or proliferation of weapons of mass destruction, whether they are aware of it or not.

(5) The regulated entities shall be obliged to ensure the implementation of the acts referred to in Paragraph 1 of this Article by establishing appropriate procedures and internal control systems.

**Article 15**

**Content of the Program, policies and procedures**

(1) The mandatory part of the Program referred to in Article 14 of this Decision are the policies and procedures that regulate the following segments:
   1) risk assessment and client eligibility,
   2) client identification,
   3) monitoring of business relations and transactions and
   4) risk management.

(2) The policies and procedures for implementing the policies referred to in Paragraph 1 of this Article must be based on risk assessment and the application of the "Know Your Client" principle.

(3) The policies referred to in Paragraph 1 of this Article must be approved by the Supervisory/Management Board, and the procedures for implementing these policies must be approved by the top management of the regulated entity.

(4) The regulated entities shall be obliged to define in their policies and procedures the objectives, processes, scope and operation of the system for preventing money laundering and the financing of terrorist activities and the proliferation of weapons of mass destruction. In their policies and procedures, the regulated entities shall be obliged to define in particular:
   1) which and what kind of clients are eligible for the regulated entity, as well as to stipulate comprehensive procedures for the implementation of this policy,
   2) methodology for assessing the risk of the entire business operations,
   3) methodology for assessing the risk of the client, business relation and transaction,
   4) measures for identifying the client and monitoring transactions and client activities in the manner and under the requirements specified in the Law on AML/CFT,
   5) measures and activities to be undertaken towards clients with whom a business relation has not been established, but for whom occasional transactions are executed,
   6) measures and activities to be undertaken in order to implement restrictive measures,
   7) products or services that the regulated entity will not provide to clients of certain risk categories,
   8) undertaking enhanced measures for risk management and risk mitigation where a high risk level is identified,
   9) undertaking simplified risk management measures and eliminating risks where a low risk level is identified,
   10) managing isolated or special risks that are characteristic of the business model, products or services of the regulated entity,
   11) appointing the authorized person and his/her deputies, their position in the organizational structure of the regulated entity, the powers and responsibilities of the authorized person and his/her deputy,
   12) protection against unauthorized disclosure of data about the persons referred to in Item 11 of this Paragraph and other procedures that may affect the unhindered performance of their duties,
   13) an appropriate procedure for determining and verifying the conditions for establishing an employment relation and engaging persons outside the employment relation with the regulated

entity who participate in the implementation of the Law on AML/CFT and the adopted bylaws, as well as the procedure for further verifying those conditions during the employment relation/engagement,

14) the powers and responsibilities of all employees of the regulated entity who participate in the implementation of the Law on AML/CFT and the adopted bylaws,
15) the procedure for anonymous internal reporting of violations of the provisions of the Law on AML/CFT and the adopted bylaws, including keeping records and defining the activities that the regulated entity will undertake upon anonymous reports,
16) models for managing the risk of money laundering and the financing of terrorist activities and the proliferation of weapons of mass destruction,
17) methods and models for managing the compliance of the regulated entity's operations with the provisions of the Law on AML/CFT and the adopted bylaws,
18) establishing appropriate reporting lines within the regulated entity, as well as reporting lines to the competent institutions,
19) storing, accessing and disposing of data, information and documentation collected in accordance with the Law on AML/CFT and the bylaws,
20) the method of keeping and content of records of collected data,
21) professional training and education of the regulated entity's employees and
22) performing internal and external audits of the system for preventing money laundering and the financing of terrorist activities and the proliferation of weapons of mass destruction, when appropriate to the size and nature of the regulated entity's operations.

(5) The policies, procedures and control measures referred to in Paragraph 1 of this Article must be proportionate to the size of the regulated entity, the type, scope and complexity of the operations carried out by the regulated entity.

**Article 16**

**Manual**

In order to improve the professional skills and efficiency of their employees, the regulated entities are required to develop a comprehensive manual that will include laws and regulations governing the prevention of money laundering and the financing of terrorist activities, the regulated entity's program with all policies and procedures, rules of conduct for employees, methods for detecting illegal and suspicious activities, responsibilities and competences of authorized persons, descriptions of the most common examples of misuse, an employee training program, and guidelines from competent authorities.

## 4. Measures for identification, monitoring of transactions and activities of a client

**Article 17**

**Client identification**

(1) The regulated entities shall implement detailed and comprehensive client identification measures. These measures shall depend on the risk category in which individual clients are classified and the products or services that clients will use. Depending on these categories, the regulated entities shall apply proportionate client identification measures. Identification measures may be: simplified, standard and enhanced.

(2) The identification procedure shall be carried out at the beginning of the establishment of business relation. However, in order to ensure that the documents are still valid and relevant, the regulated entities shall be obliged to conduct regular reviews and updates of the collected documents.

(3) The regulated entities shall implement the identification and monitoring measures referred to in Paragraphs 1 and 2 of this Article throughout the duration of the business relation with the client based on a risk assessment, or when relevant circumstances regarding the client change, in all cases where significant transactions are carried out, when significant changes occur in the way the client uses the products and services of the regulated entity, when the regulated entity significantly changes the

standards for documenting the identity or transactions of the client, or when it is obliged to do so based on the provisions of the Law on AML/CFT.

(4) When establishing business relation with new clients, as well as in cases referred to in Paragraphs 2 and 3 of this Article, the regulated entities shall be obliged to verify the client's identity using reliable and independent sources of documents, data or information

(5) Verification of the identity of the client must be completed before establishing a business relation or executing a transaction. Exceptionally, the regulated entity may perform the verification during the establishment of the business relation if necessary, in order to avoid interruption of normal business operations and in cases where a low risk has been identified. In such cases, the aforementioned procedures shall be carried out as soon as possible after the first contact.

(6) By way of exception to Paragraph 5 of this Article, the regulated entities may establish a business relation provided that there are appropriate safeguards in place to ensure that clients or anyone on their behalf does not conduct transactions until full compliance with the requirements for identification and monitoring under the Law on AML/CFT has been achieved.

**Article 18**

**Obligations when implementing client identification measures**

(1) The regulated entities shall be obliged to establish and verify the identity of the client on the basis of documents, data or information collected from reliable and independent sources, as well as documents stipulated by other relevant regulations or by means of electronic identification in accordance with legal regulations. The regulated entities shall pay special attention to non-resident clients as well as new clients who are not physically present when establishing a business relation, or in the process of performing a transaction.

(2) In cases where regulated entities learn that they do not have sufficient information about an existing client, they shall be obliged to take urgent measures and collect information, or they shall be obliged to verify the changed identification data immediately and in the fastest possible manner.

(3) The regulated entities shall be obliged to stipulate standards for the identification of the client and each individual product and the period for which such documentation must be kept, at least in accordance with the relevant regulations for the keeping of documents.

(4) The regulated entities may not establish a business relation or conduct business with a client who insists on his/her anonymity or who, when identifying him/herself, uses a false name, provides incorrect identification data and forged documentation. In such cases, the regulated entities shall be obliged to make a note of the business contact with the client and submit a report to the FIU, in accordance with the Law on AML/CFT.

(5) If the implementation of identification and monitoring measures raises suspicions among the client that the regulated entity is implementing actions and measures for the purpose of submitting data to the FIU, the regulated entities are obliged to suspend the undertaking of those actions and measures and draw up an official note in writing, which should be submitted to the FIU immediately and without delay .

(6) When implementing standard and enhanced identification measures, the regulated entities shall be obliged to check documents, as well as to check whether the client with whom they are establishing a business relation actually exists, whether he/she is at the registered address and whether he/she is actually carrying out the specified business activities.

(7) Requirements for clients should be defined depending on the risk category into which the client is classified, so that a simplified identification procedure is carried out for low-risk clients, a standard identification and monitoring procedure for medium-risk clients, and enhanced identification and monitoring measures for high-risk clients.

**Article 19**

**Simplified measures**

(1) The regulated entities may apply simplified identification measures in cases where they establish a business relation with clients who/which are:

1) state authorities and institutions, regardless of the level of organization of the state structure (state, entities, district, local government units, etc.),
2) public sector entities and institutions founded by state authorities and institutions referred to in Item 1 of this Article
3) entities obliged to implement measures to prevent money laundering and the financing of terrorist activities, over which supervision in connection with the application of the Law on AML/CFT and other regulations relating to the prevention of money laundering and the financing of terrorist activities is carried out by bodies and agencies established in accordance with special laws and
4) other clients, legal entities and private individuals, for whom the regulated entity determines, based on a risk analysis, that they are of a low risk.

(2) The regulated entities may apply simplified client identification and monitoring measures in relation to an occasional transaction that they assess to pose a low risk, taking into account the results of the Money Laundering and Terrorist Financing Risk Assessment in Bosnia and Herzegovina.

(3) The regulated entities shall be obliged to collect sufficient information to determine whether the client meets the conditions for the application of simplified identification and monitoring measures.

(4) When there is a suspicion that money laundering or terrorist financing activities or proliferation of weapons of mass destruction are involved in relation to the client, transaction or service to which simplified measures have been applied, the regulated entities are obliged to conduct an additional assessment and apply enhanced measures.

(5) The regulated entities shall be obliged to collect and verify the data and information about the client stipulated by the Law on AML/CFT by inspecting the original or certified copy of valid documents or documentation containing data and information about the client, such as: personal identification documents, extracts from appropriate registers, other business documentation or in another manner stipulated by the Law on AML/CFT, and taking into account the risk analyses performed.

**Article 20**

**Standard measures**

(1) Standard identification and monitoring measures shall include establishing and verifying the identity of the client and the beneficial owner, obtaining and assessing information on the purpose and intention of the client's business relation or transaction, as well as regular monitoring of its operations, in cases and in the manner stipulated by the Law on AML/CFT.

(2) When implementing the measures referred to in Paragraph 1 of this Article, the regulated entities shall verify whether the person acting or claiming to act on behalf of the client is authorized to do so, and in accordance with the provisions of the Law on AML/CFT and this Decision, establish and verify the identity of the same.

(3) Standard identification and monitoring measures shall be applied to medium-risk clients or occasional transactions for which the regulated entities assess that they represent medium risk.

**Article 21**

**Enhanced measures**

(1) The regulated entities shall be obliged to apply enhanced client identification and monitoring measures in relation to an individual business relation or occasional transaction for which a high level of risk has been determined by the Law on AML/CFT or the Money Laundering and Terrorist Financing Risk Assessment in Bosnia and Herzegovina or by the assessment of the regulated entitiy.

(2) The regulated entities shall also be obliged to apply enhanced client identification and monitoring measures in the case of transactions that are: complex, unusual or unusually large, have an unusual pattern of implementation or do not have an obvious economic or lawful purpose and intention.

(3) Enhanced identification and monitoring measures, in addition to standard measures, also include additional measures that the regulated entities are obliged to undertake in cases referred to in Paragraph 1 of this Article, as well as in other cases when they assess that, due to the nature of the business relation, the manner of conducting the transaction, the type of transaction, the ownership structure of the client, or other circumstances related to the client or transaction, there is or could be a high risk of money laundering or financing of terrorist activities and proliferation of weapons of mass destruction.

(4) The regulated entities shall be obliged to define in their internal act which enhanced measures they will undertake and to what extent they will obtain additional data and perform additional checks of the collected documentation in each specific case. The type of additional measures that the regulated entity will undertake should be based on the risk factors on the basis of which the client, business relation, transaction, service or distribution channel is assessed as high risk.

**Article 22**

**Client identification verification**

(1) The regulated entities shall be obliged to provide confirmation, i.e. verification of the collected data and information about the client and the client's beneficial owner, by inspecting and obtaining documentation containing the collected data and information about the client and the client's beneficial owner, or in another manner stipulated by the Law on AML/CFT.

(2) The regulated entities shall be obliged, in addition to the client, to carry out identification and verification of the identification of persons acting in the name or on behalf of the client.

(3) When identifying persons referred to in Paragraphs 1 and 2 of this Article, the regulated entities shall be obliged to obtain the original or a certified copy of the documentation containing the collected data and information about the client, or to make a copy thereof by inspecting the original or a certified copy, which shall also be considered an electronic document.

(4) If the regulated entity made a copy of the identification document when implementing identification measures, he or she shall provide on the copy, in paper or electronic form, data on the time when the identification was performed, as well as the name, surname and signature of the employee who performed the identification.

**Article 23**

**Application of the proportionality principle**

(1) When determining requirements for clients in the procedure for implementing measures for identifying and monitoring client activities and transactions, the regulated entities shall be obliged to apply the principle of proportionality. By applying the principle of proportionality, the regulated entities should ensure that the measures they will undertake must be sufficient and adequate to achieve the desired goal.

(2) In the procedure for determining the requirements referred to in Paragraph 1 of this Article, the regulated entities shall be obliged to ensure that the application of the proportionality principle does not affect the achievement of the objectives of the legal requirements and the requirements of this Decision in terms of the comprehensiveness, reliability and efficiency of the money laundering and terrorist financing risk management system.

**Article 24**

**The principle of “Know Your Client” and forming clients' profiles**

(1) In everyday business operations and relations with clients, the regulated entities must learn and become familiar with the client's activities, fully understand their business operations, become familiar with the financial and payment habits, the types of business relations that the client has and become familiar with their business contacts, their domestic and international market practices, the usual funding

sources used in the business relation, the use of currencies, the frequency and size, or volume, of transactions, and obtain relevant information and documentation about the client's business connections and cash flows. In particular, the regulated entities shall be obliged to:

1) monitor whether the client's activities are in accordance with the purpose and intention of the business relation established between the client and the regulated entity, in the case of legal entities, learn about the ownership structure of the legal entity, the authorized executive decision-makers and all those authorized to act on their behalf,
2) oblige their clients to provide them with information and documentation on expected and intended changes in the form and performance of their business activities in advance and on time,
3) ensure that the documentation, data and information collected as part of the identification and monitoring process is up-to-date and relevant, and that they review existing records, especially for high-risk client categories, and
4) pay special attention to well-known clients and public figures and ensure that their possible illegal or suspicious business activities do not jeopardize the reputation of the regulated entity.

(2) The regulated entities may not outsource regular monitoring activities to a third party.

(3) Based on the elements referred to in Paragraph 1 of this Article, the regulated entities shall be obliged to establish a profile of their clients. This profile will be contained in a special client profile register, as determined by the regulated entities. The determined client profile will be used by the regulated entities as an indicator in monitoring client operations to determine:

1) regularity and continuity in business relations between the regulated entities and clients and
2) unusual behavior and deviations from the client's profiled behavior in order to initiate appropriate measures.

**Article 25**

**Unusual transactions**

(1) The regulated entities shall establish comprehensive controls to detect complex, unusually large transactions or unusual patterns of transactions that do not have a clearly visible economic or legally justified purpose, i.e. are not in line with or are disproportionate to the usual, expected business of the client.

(2) The regulated entities shall require clients to provide an explanation for any significant change in behavior observed.

(3) In the event that clients cannot provide or provide an unconvincing and unsubstantiated explanation, the regulated entities shall consider such behavior suspicious and activate additional measures for a more detailed investigation, including sending a report on suspicious client activities to the FIU.

(4) In relation to transactions or funds referred to in Paragraph 1 of this Article, the regulated entities shall be obliged to at least determine the basis and purpose of the transactions, verify data on the source of funds and the client's activity and the intended nature of the business relation with the client and, if they do not determine that it is a suspicious transaction, make an official note in written or electronic form, which they keep so that it is available upon request by the FIU and the Agency.

(5) Unusual and uncommon behaviors that give rise to suspicion include, among others:

1) an unexpected change in the financial behavior of the client that cannot be explained by business or financial motives,
2) an unexpected appearance of a new person, business and/or geographical area that deviates from the already known manner and type of operations, business and financial network of the client of which the regulated entity is aware of,
3) a special characteristic of a transaction that does not fit into the usual practice of the client,
4) the use of funds from the client's account for a purpose that is not usual and covered by the arrangement between the regulated entity and the client,
5) the explanation of the transaction by the client is not convincing and appears false,

6) when transactions are frequently repeated in amounts that are slightly below the amount stipulated by the Law on AML/CFT for reporting to and notifying the FIU,
7) when the client closes its account by taking the entire amount in cash or by distributing that amount into several smaller amounts and into several accounts and
8) when employees of the regulated entity do not have clear evidence that illegal activities are involved, but they suspect that such a possibility exists.

(6) If, after conducting an analysis, the regulated entities determine reasons for suspicion of money laundering or financing of terrorist activities in relation to the transactions or funds referred to in Paragraph 1 of this Article, they shall be obliged to inform the FIU thereof in the manner and within the deadlines stipulated by the Law on AML/CFT.

**Article 26**

**Monitoring for the purpose of preventing money laundering**

(1) The regulated entities shall carry out ongoing monitoring of transactions and activities of a client as a fundamental aspect of effective measures for know your client, and shall ensure the means or instruments, methods and comprehensive controls to detect transactions that do not fit into such a nature of conduct and to effectively control and minimize their risk in operations with clients through these activities.

(2) The extent to which the regulated entities develop monitoring clients' transactions and activities must be adapted to the needs of adequate risk sensitivity. For all transactions and clients, the regulated entities shall establish such a system that will enable the detection of all unusual, uncommon and suspicious types of transactions and activities.

(3) The regulated entities shall be obliged to establish comprehensive controls and monitoring of clients' transactions and activities depending on the nature, size and complexity of the regulated entity's operations, as well as on the assessed risk to which the regulated entity is exposed in its business operations.

**Article 27**

**Monitoring of clients' transactions and activities**

(1) In order to ensure the fulfillment of the objectives referred to in Article 26 of this Decision, the regulated entities shall be obliged to:
1) define the types of transactions and activities that must alert the regulated entity that there is a possibility that clients are carrying out some unusual, uncommon or suspicious transactions,
2) define the types of transactions that by their nature do not primarily make economic or legal sense,
3) define which transactions will be monitored in real time, and which may be subject to subsequent monitoring (define the frequency of subsequent monitoring of transactions), whereby the regulated entity is obliged to determine the circumstances indicating high risk, which will be applied when determining the transactions that will be monitored in real time,
4) in addition to the obligations from Item 3) of this Paragraph, the regulated entities shall also be obliged to regularly, at least once a quarter, check the transactions carried out based on a random sample, regardless of whether they were monitored in real time or were subject to subsequent monitoring, in order to ensure the reliability and appropriateness of the established monitoring transaction system,
5) set transaction limits, and check all transactions that exceed the set limits, and
6) compile an official list of examples of suspicious transactions and examples and methods of possible forms of money laundering, which is as comprehensive as possible.

(2) Set an adequate information system that will enable the creation of accounting documentation and records with all data that satisfactorily describe the business event that occurred, which will be a sufficient tool for analyzing and monitoring account turnover, i.e. all client business activities.

**Article 28**

**Enhanced monitoring measures**

(1) For business relations, products and services that pose a high risk, the regulated entities shall be required to apply enhanced monitoring measures.

(2) In order to identify the category of business relation, product and service with a high level of risk, the regulated entities need to establish a set of key indicators according to which business relations will be categorized into this group, taking into account data on the history and information of the client, such as the sources of funds used in the business relation, the type and nature of the transactions themselves, the country of origin of the client, and other.

(3) For business relations, products and services that pose a high risk, the regulated entities shall be obliged to:

1) develop an adequate information management system that will ensure that the top management and employees of the regulated entity responsible for monitoring the compliance of the regulated entity's operations with the requirements stipulated by the Law on AML/CFT and regulations in this area have, in a timely manner, the necessary information for the identification and effective monitoring of the activities of clients, products and services used by clients. This system should include at least:
    1. reporting on documentation that is missing for completely secure identification of clients,
    2. reporting on unusual, uncommon and suspicious transactions and activities of clients and
    3. reporting on comprehensive information on the entire business relations of clients with the the regulated entity.
2) ensure that the top management of the regulated entity is well aware of the situation of high-risk clients, and that it collects and assesses information that can be obtained from other regulated entities, as well as from domestic and international institutions that have competences in combating money laundering and the financing of terrorist activities. Significant transactions of these clients should be approved by the top management of the regulated entity.

**Article 29**

**Application of international restrictive measures**

(1) The regulated entities shall be obliged to, in order to combat the financing of terrorist activities and the financing of the proliferation of weapons of mass destruction, implement restrictive measures in a timely manner based on international legally binding decisions of the United Nations and competent domestic institutions, and inform competent institutions and block the financial assets of persons whom the regulated entities know or suspect to be covered by restrictive measures.

(2) The regulated entities should pay the greatest attention to:

1) checking whether funds from legal sources or transactions are, to a greater or lesser extent, directed towards supporting terrorist activities and the proliferation of weapons of mass destruction
2) the application of comprehensive controls to prevent the financing of terrorists, terrorist organizations and persons associated with them,
3) activities to constantly monitor changes in entries on the lists of persons subject to restrictive measures adopted by the United Nations Security Council and competent domestic institutions,
4) activities to identify the real identity and/or purpose of particularly small transfers when the purpose of the transfer and/or the sender and/or recipient are not clearly stated,
5) cases when an account is unexpectedly emptied by a client's order,
6) cases of money laundering in which money is received or sent electronically, and are accompanied by unusual or uncommon aspects, such as the size amount, country to which the money is being sent, country of origin of the order submitter, type of currency, etc.,
7) non-profit and charitable organizations, especially if the activities are not in accordance with the registered activity, if the source of funds is not clear, and if the organization receives funds from unusual and suspicious sources,

8) monitoring entries on the list of dual-use goods published by competent institutions in the country and abroad and

9) monitoring transactions and activities of clients whose activities include the production and trade of dual-use goods.

(3) By monitoring clients' transactions and activities, the regulated entities must determine whether clients, or persons who are principals or beneficiaries in transactions carried out without establishing a business relation, are persons covered by restrictive measures adopted by the United Nations Security Council and competent domestic institutions.

(4) In cases where persons referred to in Paragraph 3 of this Article attempt to establish a business relation with the regulated entity or when they are existing clients, the regulated entities shall be obliged to temporarily freeze funds and dispose of products and services used at the regulated entity and notify the competent institutions thereof.

## 5. Risk management

### Article 30

### Risk assessment, general provisions

(1) The regulated entities shall establish a comprehensive risk management process that includes the identification of risk factors and regular risk assessments.

(2) The regulated entities shall be obliged to assess:
1) the risk to which they are exposed due to the nature and complexity of their business operations (overall operation risk assessment) and
2) the risk to which they are exposed due to the establishment of a business relation or the execution of an occasional transaction (individual risk assessment).

(3) The risk assessment referred to in Paragraph 1 of this Article shall consist of two related steps, the identification of risk factors and the risk assessment.

(4) When assessing the overall level of residual risk associated with their business and individual business relations or occasional transactions, the regulated entities shall take into account the level of inherent risk and the quality of controls, as well as other risk mitigation factors.

(5) The regulated entities shall record and document their overall business risk assessment and individual risk assessments, as well as any changes to those risk assessments, in a manner that enables the regulated entities and the competent authorities to understand how and why the assessments were conducted in a particular manner.

(6) The regulated entities shall ensure that the risk assessment reflects their understanding of the risks and that they can demonstrate this to the competent authorities.

### Article 31

### Risk assessment updating

(1) The regulated entities shall establish systems and controls to continuously review their business-wide and individual risk assessments and to ensure that their risk assessments are up-to-date and adequate.

(2) The systems and controls of the regulated entities referred to in Paragraph 1 of this Article shall include at least:
1) the date for each calendar year on which the business-wide risk assessment will be updated, and the date determined on the basis of risk sensitivity for the individual risk assessment, in order to ensure that new or emerging risks are included. If the regulated entity becomes aware of the emergence of a new risk before this date, it shall be obliged to analyze it and include it in individual risk assessments and business-wide risk assessments and
2) records of all relevant issues that could affect the risk assessments, such as internal reports on suspicious transactions, non-compliance and information originating from employees who work in direct contact with clients, etc.

(3) The regulated entities shall be obliged to provide systems and controls for identifying emerging risks and assessing those risks, and to include them in their business-wide risk assessments and individual risk assessments in a timely manner, as necessary.

(4) The systems and controls referred to in Paragraph 3 of this Article should, as a minimum, include:

1) procedures to ensure that internal information, such as information obtained as part of the ongoing monitoring of clients' business relations and activities, is regularly reviewed to identify trends and emerging issues related to individual business relations and operations of the regulated entity,
2) procedures to ensure that the regulated entities regularly review relevant sources of information, and
3) cooperation with representatives of other industries and competent authorities (e.g. round tables, conferences and training), and procedures to provide feedback to relevant employees.

(5) The procedures referred to in Paragraph 4, Item 2 of this Article in relation to the business-wide risk assessment should include at least:

1) warnings and reports from competent authorities,
2) thematic reviews and similar publications issued by competent authorities and
3) procedures for collecting and reviewing information on risks, in particular risks associated with new categories of clients, countries or geographical areas, new products, new services, new distribution channels, and new systems and compliance controls.

(6) The procedures referred to in Paragraph 4, Item 2, of this Article in respect of individual risk assessments should include at least:

1) warnings on terrorist threats and financial sanctions regimes, or changes thereto, as soon as they are published or communicated, ensuring that they are acted upon if necessary, and
2) media reports relevant to the sectors or countries or geographical areas in which the regulated entities are actively operating.

(7) The frequency of comprehensive reviews of the risk assessment methodology of the entire business operations and of individual risk assessments shall be conducted by the regulated entities on the basis of risk sensitivity.

**Article 32**

**Regulated entity business-wide risk assessment**

(1) The business-wide risk assessment should help the regulated entities to determine the areas in which they are exposed to risk, and which areas of business operations should be prioritized in their combat against risk.

(2) The regulated entities shall be obliged to identify each segment of their business operations, i.e. the type, volume and complexity of their business operations, all existing and new products, services, processes, activities and procedures in order to assess in which segment of their business operations the threat of money laundering, terrorist financing and proliferation of weapons of mass destruction may arise, as well as to adequately assess the negative consequences that could arise from that source of risk, and their potential impact on the realization of the regulated entity's business objectives.

(3) The regulated entities should ensure that their business-wide risk assessment is tailored to their business profile and that it takes into account factors and risks specific to the regulated entity's business operations. If the regulated entity is part of a group that prepares a group-wide risk assessment, the regulated entities should consider whether the group-wide risk assessment is sufficiently precise and specific to reflect the regulated entity's business operations and the risks to which it is exposed due to the group's connections to countries and geographical areas, and supplement the group-wide risk assessment as necessary.

(4) Based on the assessed probability of risk occurrence and the estimated negative consequences, the regulated entities shall be obliged to determine the level of risk exposure for each segment of their business operations.

(5) The regulated entities shall be obliged to base the business-wide risk assessment on all relevant information, and to update it at least once a year and submit it to the Agency.

**Article 33**

**Risk analysis and risk factors of an individual business relation or occasional transaction**

(1) The regulated entities shall be required to conduct a risk analysis in order to identify, assess, understand and mitigate the risks to which they are exposed or could be exposed when establishing or maintaining a business relation or executing a particular occasional transaction. When conducting a risk analysis, the regulated entities should take into account the risk factors related to:
   1) clients,
   2) products, services or transactions,
   3) countries or geographic areas, and
   4) distribution channels.

(2) The risk analysis referred to in Paragraph 1 of this Article should also include other risk factors that the regulated entities are required to identify due to the specific nature of their business operations. The risk analysis should be documented and proportionate to the size of the regulated entity, the type, scope and complexity of its business operations, and the regulated entities are required to update it regularly, at least once a year.

(3) The risk analysis referred to in Paragraph 1 of this Article must also include measures, actions and procedures that the regulated entities undertake in order to prevent and detect money laundering and the financing of terrorist activities and the proliferation of weapons of mass destruction.

(4) The regulated entities shall be obliged to align the risk analysis referred to in Paragraph 1 of this Article with the regulations and decisions, or guidelines, issued by the competent authority, and when compiling and updating it, they shall also be obliged to take into account the Risk Assessment of Money Laundering and Financing of Terrorist Activities in Bosnia and Herzegovina.

(5) Based on the risk analysis performed for each group or type of client, i.e. business relation, service provided by the regulated entity within the scope of its activity, i.e. transaction, the regulated entity shall classify the client in the client profile register into one of the following risk categories:
   1) low risk category,
   2) medium risk category and
   3) high risk category.

**Article 34**

**Risk factor weighting**

(1) The regulated entities shall comprehensively consider all identified risk factors and activities associated with a business relation or transaction. As part of that assessment, the regulated entities may decide to weight risk factors differently, depending on their individual significance, in the context of the business relation or transaction.

(2) The weight assigned to each risk factor may vary depending on the specific product, service or client, but also depending on individual regulated entities.

(3) When weighting risk factors, the regulated entities shall ensure that:
   1) the weighting is not unduly influenced by a single risk factor,
   2) economic considerations and considerations relating to the regulated entity's profit do not influence the risk assessment,
   3) the weighting of risk factors does not lead to a situation where no business relation can be classified as high risk,
   4) the risk category determined by the Law on AML/CFT cannot be changed, and
   5) if necessary, the automatically generated risk assessment can be changed based on the conducted assessment analysis and written explanation by the regulated entity's authorized person.

(4) If regulated entities perform the overall risk assessment for the purposes of classifying a business relation or transaction into a specific risk category in an automated manner, where the system is not developed by the regulated entity, but is provided by a third party, the regulated entities must

understand the functioning of that system, including the method in which risk factors are combined to achieve an overall risk assessment.

**Article 35**

**Risk assessment of an individual business relation or occasional transaction**

(1) When assessing the risk of an individual business relation or occasional transaction, the regulated entities shall be required to take into account relevant risk parameters and factors in order to assess the risks associated with an individual business relation or the execution of an occasional transaction.

(2) The risk parameters referred to in Paragraph 1 of this Article shall include at least:
1) the purpose and intended nature of the business relation,
2) the purpose and intention of the transaction,
3) the value of the funds deposited by the client, the amount and volume of the transactions carried out and
4) the frequency or duration of the business relation.

(3) When implementing the risk assessment referred to in Paragraph 1 of this Article, the regulated entities shall take into account the factors that may indicate a potentially higher/lower risk, which are listed in the Guidelines.

**Article 36**

**Information sources**

(1) In order to determine risk, the regulated entities should use information from various reliable sources, which can be accessed individually or using available commercial tools or databases that aggregate information from several sources.

(2) The regulated entities should always take into account the following sources of information:
1. the list of high-risk countries compiled by relevant domestic and foreign institutions,
2. information made available by competent authorities, such as risk assessments, policy opinions and warnings, and explanations of relevant legislation,
3. information coming from supervisory authorities, such as guidelines and explanations given when imposing regulatory measures,
4. information from competent authorities, such as threat reports, warnings, typologies, and
5. information obtained as part of initial client identification measures and ongoing monitoring of client's activities.

(3) Other sources of information that the regulated entities should consider include, but are not limited to:
1) own knowledge,
2) information from entities in the same business sector, such as typologies and information on emerging risks,
3) information from civil society, such as corruption indices and country reports,
4) information from international standard-setting bodies, such as joint evaluation reports or non-legally binding blacklists,
5) information from credible and reliable public sources,
6) information from credible and reliable commercial organizations, such as risk reports and intelligence reports, and
7) information from statistical organizations and universities.

(4) The regulated entities should determine the type and number of sources based on a risk assessment, taking into account the nature and complexity of their business operations, and not limiting themselves to just one source for determining risk.

## 6. Managing isolated risks

### Article 37

### Business relations with banks or similar credit institutions headquartered abroad (correspondent business relations)

(1) When establishing a correspondent relation with banks and other similar credit institutions headquartered abroad, the regulated entities shall be obliged to, in addition to activities and measures for identifying and monitoring the client in accordance with the risk assessment, obtain additional data, information and documentation stipulated by the Law on AML/CFT.

(2) The regulated entities may not establish or maintain a correspondent relation with a foreign bank or other financial institution on the basis of which that institution may use an account with the regulated entity by enabling its clients to use that account directly.

(3) The regulated entities may not establish or maintain correspondent relations with shell banks.

(4) The regulated entities may not establish or maintain correspondent relations with a financial institution known to allow accounts to be used by a shell bank.

(5) An employee of the regulated entity who establishes a relation with a correspondent bank or other financial institution headquartered abroad shall implement enhanced identification and monitoring measures and shall obtain written approval from the the regulated entity's senior management prior to entering into such a relation, and if such a relation has been established, it may not continue without the written approval of the the regulated entity's senior management.

### Article 38

### Politically exposed persons

(1) When establishing business relation, performing occasional transactions and during the business relation, the regulated entities shall be obliged to define procedures that will enable the determination of whether the client and/or the beneficial owner of the client is a politically exposed person.

(2) The regulated entities shall be obliged to collect data and information on the client's political exposure directly from the client and/or publicly available registers and databases and to continuously update them.

(3) In order to determine political exposure, the regulated entities shall undertake the following activities:
1) obtain a written statement from the client on whether he or she is a politically exposed person, a close family member or a close associate of a politically exposed person,
2) use reliable and credible electronic databases containing lists of politically exposed persons and
3) search publicly available data and other.

(4) The regulated entities shall apply the same identification and monitoring measures in cases where the founders, beneficial owners, persons authorized to represent and act, and persons authorized to dispose of funds in the accounts of clients of a legal entity are politically exposed persons.

(5) When the client and/or the beneficial owner of the client who enters into a business relation or performs a transaction or on whose behalf the business relation is concluded or performs a transaction is a politically exposed person, the regulated entity shall, as part of the enhanced client identification and monitoring measures, undertake the following additional measures:
1) collect data to determine the source of the assets and the source of funds that are or will be the subject of the business relation or transaction from the documents and other documentation submitted by the client and/or the beneficial owner of the client,
2) employees of the regulated entity who carry out activities to establish a business relation with the client shall secure written approval from the regulated entity's top management before entering into such a type of business relation and
3) after entering into a business relation, the regulated entity shall monitor the transactions or funds and other business activities of the politically exposed person in an enhanced and continuous manner.

(6) If the regulated entity determines that a client or the beneficial owner of a client has become a politically exposed person during the business relation, it shall apply the actions and measures referred to in Paragraph 5 of this Article, and shall obtain the written consent of the regulated entity's top management for the continuation of the business relation with that person.

(7) The measures referred to in this Article shall also be implemented for the closest family members and close associates of a politically exposed person.

(8) The regulated entities shall be obliged to monitor with particular attention all business activities carried out by a politically exposed person with the regulated entity and notify the authorized person immediately and without delay, in the event that they assess that the circumstances in relation to the usual business activities of the politically exposed person have changed.

**Article 39**

**Establishing a business relation without the physical presence of the client**

(1) When establishing business relations, the client or legal representative, or the person authorized to represent the legal entity, is not physically present with the regulated entity, the regulated entity shall be obliged to apply enhanced identification measures in order to reduce and qualitatively manage the risk that may be present due to the establishment of a business relation in this manner.

(2) When implementing the measures referred to in Paragraph 1 of this Article, the regulated entities shall be obliged to, in addition to standard measures for identification and monitoring of the client, apply additional measures, which include:

1) requesting additional data, documents and information on the basis of which the client's identity is verified, which are not requested from other clients,
2) verifying the submitted documents,
3) independently contacting the client by the regulated entity,
4) additional verification of the presented documents or additional verification of client data, independently and/or engaging a specialized firm for client control and assessment,
5) requiring that the first payment (deposit) be made through an account in the client's name with another regulated entity that is obliged to implement similar standards for client control and assessment, and before executing other client transactions with the regulated entity, and
6) obtaining data and information on the reasons for the client's absence.

(3) If the regulated entity does not implement enhanced identification measures, it will not establish a business relation with a client who is not physically present when establishing the business relation.

**Article 40**

**Third party**

(1) In fulfilling the requirements for identification and verification of the client's identity, the regulated entities may rely on a third party, but the ultimate responsibility for fulfilling the conditions lies with the regulated entity relying on the third party.

(2) The regulated entities shall be obliged to check in advance whether the third party to whom they will outsource the implementation of client identification measures meets the conditions stipulated by the Law on AML/CFT.

(3) The regulated entities may not accept the performance of certain actions and measures of client identification through a third party, if that person has established and verified the client's identity without its presence.

(4) The regulated entities must ensure that a copy of the documentation with identification data and information on the basis of which the third party verified the client's identity is delivered to the regulated entity, without delay.

(5) The regulated entities shall keep documentation on the identification and verification of the identity of the client carried out by a third party in accordance with the Law on AML/CFT.

(6) The regulated entities shall conclude a contract with a third party, which shall define the measures and actions of identification and verification of the identity of the client, which the third party shall undertake, define the manner and deadlines for submitting the collected identification documents and the protection of confidential and personal data.

**Article 41**

**Preventing misuse of technological development**

(1) The regulated entities shall identify and assess the risks that may arise in connection with the development of new products and new business practices, including new delivery mechanisms, and the use of new technologies under development or payment methods, for new and existing products before their marketing or use.

(2) The regulated entities shall adopt policies and procedures and implement measures necessary to prevent the misuse of technological developments for the purposes of money laundering and the financing of terrorist activities.

(3) In the risk management processes, the regulated entities must establish criteria and procedures related to new products, which at least include the following:
1) ensuring the necessary technical, organizational and personnel resources necessary for risk assessment before the introduction or use of products, practices or technologies for the introduction, application and management of risks arising from new products,
2) defining the authority and responsibility for testing, approving and verifying new products. If the risk analysis shows that adequate resources are not provided for understanding and managing the risk of a new product, the regulated entity's management is obliged to postpone the introduction of the same until such resources are provided and
3) the regulated entities shall be obliged to create procedures and implement measures to mitigate the risks arising from the development of new technology.

(4) In the policies and procedures referred to in Paragraph 2 of this Article, the regulated entities shall define specific risks related to the establishment of business relations, the execution of transactions electronically, via the internet and/or online payment platforms or other interactive computer systems, by telephone or via other devices and instruments that enable the execution of transactions without the physical presence of the client in the regulated entity's premises, the provision of services related to digital assets, as well as the use of electronic payment cards linked to client accounts for payments, deposits and cash withdrawals.

(5) As part of managing these risks, the regulated entities shall be obliged to:
1) when implementing new technological developments and new products or services, in accordance with the law, in addition to standard measures for identifying and monitoring clients, apply additional measures to mitigate risks and manage the risk of money laundering and financing of terrorist activities,
2) ensure that electronic transfers and transfers made by clients from special terminals via free telecommunications lines (POS of the regulated entity, electronic and internet banking), as well as for other transfers specified in Paragraph 4 of this Article, are accompanied by identification data on the payer and the beneficiary, and the purpose of the transfer, throughout the entire transfer process,
3) establish, regularly review and test security measures and controls of processes and systems,
4) apply secure and efficient authentication measures for identity verification and client authorization and
5) ensure that client authentication includes a combination of at least two methods of verifying the client's identity.

(6) When executing these transfers, the regulated entities shall be obliged to ensure compliance with all these obligations for both domestic and international transfers.

(7) In cases where the regulated entity cannot provide the necessary identification data and information about the clients, it will refuse to provide these types of services.

**Article 42**

**Safe deposit box rental**

(1) The regulated entities shall be obliged to implement comprehensive measures that will enable the identification of private individuals and/or legal entities, their legal representatives or authorized proxies, with whom they establish a business relation based on the rental of a safe. An important element of these measures must be ensuring the possibility of identifying the beneficial owner of the items in the safe.

(2) The regulated entities which carry out the activity of renting safes shall be obliged to, when establishing a business relation with a client, conclude a contract on the use of the safe and implement stipulated measures for the identification of the client, its legal representative or authorized proxy.

(3) The regulated entities shall be obliged to, upon each access of a client to the safe, implement identification and monitoring measures for each private individual who accesses the safe, regardless of whether he/she is the user of the safe under the safe deposit box contract, or his/her legal representative or authorized proxy.

(4) The regulated entities shall be obliged to keep records of each access to the safe, which should contain identification data on each person who accessed the safe and the date and time of access to the safe.

**Article 43**

**Custody accounts**

(1) The regulated entities shall implement comprehensive measures that will enable the identification of the beneficial owner or owner of a custody account.

(2) The regulated entities shall establish the identity and collect satisfactory evidence of the identity of each person (intermediary, custodian and representative), as well as the person they represent, i.e. the beneficial owner or owner of the account.

(3) In cases where a professional intermediary opens an omnibus account for several clients and in cases where sub-accounts of an omnibus account are opened, the regulated entities shall establish the identity of all individual clients.

(4) In the following cases, the regulated entities shall be obliged to refuse the request to open an account:
   1) when the intermediary is not authorized to provide the necessary information on the beneficial owners of the funds, e.g. lawyers bound by a code of professional secrecy and
   2) when the intermediary is not subject to standards of control and assessment that are equivalent to the standards set by regulations in BiH.

**Article 44**

**Electronic transfer of money or other assets**

(1) The regulated entities engaged in electronic transfers of money or other assets, i.e. providers of payment and collection services, shall be obliged to collect accurate and complete, legally stipulated data on the originator and beneficiary of electronic transfers of money and other assets and include them in the form or message accompanying the electronic transfer of funds sent or received, regardless of the currency or type of asset.

(2) Data on the originator and beneficiary must accompany the electronic transfer throughout the payment chain, regardless of the number of intermediaries in the payment chain.

(3) When several individual electronic or bank transfers from one originator are combined into a consolidated file for transfer to beneficiaries, the consolidated file must contain the necessary and accurate information on the originator, as well as complete information on the beneficiary of the electronic transfer.

**Article 45**

**Obligations of intermediaries in the transfer of money or other assets**

(1) The regulated entities which mediate in the transfer of money or other assets shall ensure that all data on the originator and beneficiary of the electronic transfer are stored in the form or message accompanying the electronic transfer.

(2) An intermediary in the transfer of money or other assets shall, using an approach based on risk assessment, develop procedures for action in the event that the electronic message used for the transfer of money or other assets does not contain the legally stipulated data on the originator or beneficiary of the electronic transfer.

(3) If a transfer of money or other assets does not contain complete data on the originator or beneficiary of the electronic transfer, the intermediary in the transfer of money or other assets shall, in accordance with the risk assessment, define in its acts when in such a situation it will:

1) refuse the transfer of money or other assets,
2) suspend the transfer of money or other assets until the receipt of the missing data, which it shall request from another intermediary in that transfer, i.e. from the payer's payment service provider, and
3) carry out a further transfer of money or other assets and simultaneously or subsequently request the missing data from the other intermediary in that transfer, i.e. from the payer's payment service provider.

(4) If the payment service provider fails to provide accurate and complete information on the originator and the beneficiary of the electronic transfer, the intermediary in the transfer of funds shall be obliged to warn it of this and inform it within which period it must comply with the provisions of the Law on AML/CFT. If the payment service provider fails to provide accurate and complete information on the originator and the beneficiary of the electronic transfer even after this warning and the expiry of the period, the intermediary in the transfer of money or other assets shall be obliged to refuse future transfers of money and other assets received from that payment service provider, or to limit or terminate business cooperation with that payment service provider.

(5) In the case referred to in Paragraph 4 of this Article, the intermediary in the transfer of money or other assets is obliged to consider whether the lack of accurate and complete data on the originator or beneficiary of the electronic transfer, together with other circumstances, constitutes grounds for suspicion of money laundering or financing of terrorist activities, of which it shall inform the FIU if it determines that there is a basis for suspicion of money laundering or financing of terrorist activities, and otherwise it shall be obliged to make a written official note, which it shall keep in accordance with the Law on AML/CFT.

**Article 46**

**Documentation keeping**

The regulated entities shall be obliged to keep information, data and documentation related to the established business relation with the client, the occasional transaction carried out, the identification and monitoring measures carried out, as well as information and accompanying documentation on authorized persons, professional training of employees and the implementation of internal control in the manner and within the deadlines stipulated by the Law on AML/CFT.

**Article 47**

**Transitional and final provisions**

(1) The Agency shall, as necessary, independently or in cooperation with other competent authorities, provide recommendations and/or instructions and/or guidelines to the regulated entities in the field of preventing money laundering and the financing of terrorist activities.

(2) On the date of entry into force of this Decision, the following Decisions shall cease to be valid:

1) Decision on minimum standards for the activities of banks in preventing money laundering and financing of terrorist activities ("Official Gazette of Republika Srpska", No. 68/12),

2) Decision on minimum standards for the activities of microcredit organizations in preventing money laundering and financing of terrorist activities (Official Gazette of Republika Srpska", No. 68/12) and
3) Decision on minimum standards for the activities of leasing providers in preventing money laundering and financing of terrorist activities (Official Gazette of Republika Srpska", No. 68/12).

(3) The regulated entities shall be obliged to align the Program, policies and procedures with this Decision within 90 days from the date of entry into force of this Decision.

(4) This Decision shall come into force on the eighth day from the date of its publication in the "Official Gazette of Republika Srpska".

Number: UO-60/24

Date: 28 February 2024

PRESIDENT OF THE MANAGEMENT BOARD
Dejan Kusturić