Pursuant to Article 7, paragraph 2, subparagraph 7, Article 9, paragraph 1, subparagraph 2 of the Law on Insurance Companies (Official Gazette of the Republic of Srpska, Nos. 17/05, 01/06, 64/06, 74/10, 47/17, and 58/19), Article 93, paragraph 1, points (c) and (d), in connection with Article 10, paragraph 5 of the Law on the Prevention of Money Laundering and Financing of Terrorist Activities (Official Gazette of Bosnia and Herzegovina, No. 13/24), and Article 18, paragraph 1, point 2 of the Articles of Association of the Insurance Agency of the Republic of Srpska (Official Gazette of the Republic of Srpska, Nos. 2/15, 76/16, 89/19, and 35/21), the Board of Directors of the Insurance Agency of the Republic of Srpska, at its session held on 25 December 2024, adopted the

REGULATIONS
on the procedure for assessing the risk of money laundering and financing of terrorist activities

I. GENERAL PROVISIONS

Subject of the Regulations
Article 1

These regulations prescribe the procedure for assessing the risk of money laundering and financing of terrorist activities, the risk factors that an obliged entity must consider when assessing the risk of money laundering and terrorist financing associated with individual business relationships and transactions, as well as the manner of implementing simplified and enhanced customer due diligence measures. Specifically, the regulations prescribe:

1) the minimum activities of the obliged entity for the prevention of money laundering and financing of terrorist activities;
2) rules on organization, management, and responsibility of governing bodies, functions, and other employees within the obliged entity;
3) the manner of implementing identification and monitoring measures for customer transactions and activities;
4) the procedure for assessing the overall business risk and individual risk assessments; and
5) the management of specific or exceptional risks characteristic of the obliged entity's business model, products, or services.

Use of Terms and Abbreviations
Article 2

(1) The terms used in these regulations shall have the meanings as defined in the Law on the Prevention of Money Laundering and Financing of Terrorist Activities and the subordinate regulations adopted based on it.

(2) Certain terms and abbreviations used in these regulations, which are not covered by the provisions referred to in paragraph 1 of this Article, shall have the following meanings:

1) **Agency** - the Insurance Agency of the Republic of Srpska;
2) **Bodies of the obliged entity** - the Board of Directors and the senior management of the obliged entity;

3) **Board of Directors** - the governing body of the obliged entity in accordance with the Law on Companies of the Republic of Srpska;
4) **Senior Management** - the persons who lead and organize the business of the obliged entity and are responsible for the legality of its operations;
5) **ML/TF Law** - the Law on the Prevention of Money Laundering and Financing of Terrorist Activities (Official Gazette of Bosnia and Herzegovina, no. 13/24);
6) **FID** - State Investigation and Protection Agency, Financial Intelligence Department;
7) **ML/TF** - Money Laundering and Financing of Terrorist Activities;
8) **Policyholder** - a person who enters into or concludes insurance in their own name or for the benefit of another person and undertakes to pay the insurance premium to the insurer (insurance company);
9) **Beneficiary** - a natural or legal person entitled to receive compensation under the insurance;
10) **Insured** - a person whose life is insured, or a person on whose survival or death the payment of the insured sum depends;
11) **Customer of a voluntary pension fund** - a natural or legal person who concludes a membership agreement with the fund, i.e., a pension plan contract, as well as the contributor of pension contributions on behalf of a fund member;
12) **Business relationship** - a business, professional, or commercial relationship connected with the professional activities of the obliged entity, which is expected at the time of its establishment to contain an element of permanence.
13) **Customer of the obliged entity** - a person (policyholder, beneficiary, insured, or customer of a voluntary pension fund) who establishes or already has an established business relationship with the obliged entity or conducts a transaction; a person on whose behalf or for whose benefit a business relationship is established or an occasional transaction is conducted; and a person who conducts transactions through various types of intermediaries.
14) **Risk** - the likelihood and potential severity of money laundering, terrorist financing, and the proliferation of weapons of mass destruction, referring to the level of risk that exists prior to the application of risk mitigation measures.
15) **Risk-based approach** - an approach in which the bodies of the obliged entity and the obliged entity itself identify, assess, and understand the risks of money laundering and terrorist financing to which the obliged entity is exposed, and take measures to prevent money laundering and terrorist financing that are proportional to those risks.
16) **Risk factors** - variables that, alone or in combination, may increase or decrease the risk posed by a specific individual business relationship or occasional transaction.
17) **Inherent risk** - the level of risk prior to risk mitigation.
18) **Residual risk** - the level of risk that remains after risk mitigation.
19) **Emerging risk** - a risk that has never been previously identified or an existing risk that has significantly increased.

20) **Source of funds** - the origin of the funds involved in a business relationship or occasional transaction, which also implies the manner in which these funds were acquired and are used in the business relationship (e.g., personal income, credit funds, gifts, inheritance, savings, etc.).

21) **Source of wealth** - the origin of the customer's total assets.

22) **Risk assessment of money laundering and terrorist financing in Bosnia and Herzegovina** - a comprehensive risk analysis at the state level conducted by the competent authorities.

23) **Risk assessment program** - an internal act through which the obliged entity identifies, assesses, and mitigates the risk of ML/TF, determines the risk level of a client group or individual client, their geographic area of activity, business relationship, transactions, products or services, the manner of providing them to the client, and new technological developments related to potential misuse for money laundering and terrorist financing, and which includes policies and procedures for effective risk management.

24) **Occasional transaction** - a transaction that is not conducted within an established business relationship.

25) **Complex and unusual transaction** - a transaction that is larger than expected by the obliged entity based on knowledge of the client, business relationship, or category to which the client belongs, or that has an unusual or unexpected pattern compared to the client's normal activity or transaction pattern associated with similar clients, products, or services.

Entities Subject to Application

Article 3

(1) The entities subject to the application of the provisions of this Rulebook are:

1) an insurance company holding a licence to conduct life insurance business;

2) an insurance broker and insurance agent engaged in intermediation or representation in insurance in the conclusion of life insurance contracts and other investment-related insurance, except for an insurance agent engaged in life insurance representation in the name and on behalf of an insurance company; and

3) a company managing voluntary pension funds.

(2) In conducting life insurance, other investment-related insurance and voluntary pension insurance activities, the entity subject to application shall act in accordance with the Law on AML/CFT and by-laws adopted thereunder, this Rulebook and other regulations governing this field, and shall ensure that its entire operations are carried out in compliance therewith.

(3) The provisions of this Rulebook shall apply to all entities referred to in paragraph (1) of this Article, while the guidelines for risk analysis and assessment in the application of this Rulebook (hereinafter: the Guidelines) shall be applied by the entity to which the relevant part of the Guidelines relates, taking into account the specific circumstances relating to customer risk, product, service or transaction risk, geographic risk, and the risk related to the manner of establishing and conducting the business relationship.

II. ORGANISATION, MANAGEMENT AND RESPONSIBILITY

Organisation, Management and Responsibility of the Governing Bodies of the Obliged Entity

Article 4

(1) The governing bodies of the obliged entity shall establish adequate mechanisms for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction in all organisational units and across all business lines of the obliged entity.

(2) The governing bodies of the obliged entity shall promote the integrity of the authorised person and a high level of corporate governance standards in communication with the employees of the obliged entity.

(3) The governing bodies of the obliged entity shall ensure the establishment and implementation of an internal control system that guarantees the full practical implementation of the programme referred to in Article 11 of this Rulebook, and shall regularly monitor and assess the applicability and effectiveness of the established comprehensive controls.

(4) The obliged entity's procedures shall be effective and shall include regular processes for appropriate and efficient oversight by the senior management of the obliged entity, internal control systems, internal audit, segregation of duties and responsibilities, employee training, and other components closely related to the specific characteristics of the obliged entity.

(5) For the implementation of the obliged entity's policies and procedures, the programme of the obliged entity shall clearly define the authorities and responsibilities of activity holders, organisational units or functions, senior management, other management, and other employees of the obliged entity.

(6) Where the obliged entity is a member of a financial or other group, the governing bodies of the obliged entity, in addition to being responsible for ensuring that the prescribed risk management policies and procedures comply with the law and implementing regulations, shall also be responsible for monitoring compliance with policies and procedures adopted at the group level.

Authorised Persons

Article 5

(1) The governing body of the obliged entity, or where applicable, the director, shall appoint at management level an authorised person and one or more deputies of the authorised person. The authorised persons shall meet the requirements for appointment prescribed by the Law on AML/CFT.

(2) The obliged entity referred to in Article 3 of this Rulebook shall, in proportion to the size, nature, scope and complexity of the activities it performs, assess the number of employees required to carry out anti-money laundering and counter-terrorist financing tasks, and shall ensure the necessary conditions and resources for performing these tasks.

(3) The obliged entity shall ensure that the authorised person is provided with:

1) the authority to issue instructions to all employees for the implementation of measures, actions and procedures under the Law on AML/CFT, regulations and the programme, and to report thereon to the governing bodies of the obliged entity;
2) full and direct access to data, information and documentation necessary for performing tasks within his/her competence;
3) direct communication with the governing bodies of the obliged entity; and
4) timely receipt of reports on significant, unusual and suspicious transactions and client activities.

(4) For an obliged entity with four or fewer employees, if no authorised person has been appointed, the authorised legal representative shall be deemed to be the authorised person.

(5) The obliged entity referred to in Article 3 of this Rulebook shall ensure the presence of the authorised person during on-site supervision and shall ensure that the authorised person provides information necessary for the unobstructed conduct of both indirect and direct supervision.

Duties and Responsibilities of Authorised Persons

Article 6

(1) The authorised person shall be responsible for performing the following tasks:

1) ensuring, monitoring and coordinating the activities of the obliged entity in order to ensure compliance of its operations with the provisions of the Law on AML/CFT and implementing regulations;
2) assessing the adequacy of the programme, policies and procedures and conducting a risk assessment at least once a year, and submitting proposals to the governing bodies of the obliged entity for their updating or improvement;
3) submitting semi-annual reports to the governing bodies of the obliged entity on the obliged entity's actions and compliance with AML/CFT requirements, as well as on activities undertaken against identified suspicious clients;
4) ensuring the proper and timely functioning of reporting lines;
5) participating in the definition and amendment of operational procedures and in the preparation of internal provisions relating to the prevention and detection of money laundering and terrorist financing;
6) participating in the preparation of guidelines for conducting controls related to the detection and prevention of money laundering and terrorist financing;
7) participating in the establishment and development of IT support related to activities concerning the detection and prevention of money laundering and terrorist financing of the obliged entity;
8) including in his/her activities elements for internal review of the accountability of employees who have neglected their duties in this area;
9) preparing for the governing bodies of the obliged entity proposals for improving the system for detecting and preventing money laundering and terrorist financing, and proposing measures to eliminate identified weaknesses and deficiencies;
10) providing support in activities carried out by the internal audit of the obliged entity; and
11) participating in the preparation of professional training and training programmes for employees in the field of prevention and detection of money laundering and terrorist financing.

(2) The deputy authorised person shall perform all tasks referred to in paragraph (1) of this Article in the absence of the authorised person, and shall also perform any other tasks prescribed by the Law on AML/CFT and implementing regulations.

Training of Employees of the Obliged Entity

Article 7

(1) The obliged entity referred to in Article 3 of this Rulebook shall ensure continuous annual training for all employees covered by the programme for the prevention of money laundering and terrorist financing. The content of this training shall include at least the following topics within the scope of this Rulebook:

1) statutory obligations of the obliged entity and obligations arising from other regulations;
2) the programme, policies and procedures of the obliged entity;
3) detailed elements of the "Know Your Customer" (KYC) policy;
4) threats and typologies of money laundering, as well as risks to the obliged entity and the personal responsibilities of employees;
5) capabilities and weaknesses of financial institutions in preventing money laundering, terrorist financing and the proliferation of weapons of mass destruction;
6) the responsibilities and authorities of the authorised person and the deputy authorised person of the obliged entity; and
7) the internal control system.

(2) The frequency and topics of the training referred to in paragraph (1) of this Article shall be adapted by the obliged entity to the actual needs of its specific organisational units, functions and/or employees. For the purpose of timely alignment with new requirements, awareness of emerging trends, and maintaining the already acquired knowledge and experience of its employees, the obliged entity shall establish a programme of regular training.

(3) In determining the needs, type and scope of the training referred to in paragraphs (1) and (2) of this Article, the obliged entity shall adjust the extent and content of the training depending on whether it concerns new employees who have direct contact with clients, employees working with new clients, or employees responsible for monitoring compliance of the obliged entity's operations with the requirements of the Law on AML/CFT and other regulations.

(4) Through the training programme, the obliged entity shall ensure that all relevant employees fully understand the importance and necessity of the effective implementation of the "Know Your Customer" (KYC) policy, and that such understanding is key to its successful implementation.

(5) The annual training plan referred to in Article 54(3) of the Law on AML/CFT shall be submitted by the obliged entity to the Agency no later than 15 April of the current year.

Reporting Lines

Article 8

(1) The obliged entity referred to in Article 3 of this Rulebook shall establish procedures for internal reporting to the competent authorities regarding prescribed transactions, suspicious funds, and suspicious clients. Reporting lines within the organisation of the obliged entity must be clearly defined.

(2) The reporting system must enable adequate communication, information exchange, and cooperation at all organisational levels, and must ensure timely, accurate, and sufficiently detailed information necessary for effective risk management.

(3) The established reporting system of the obliged entity, in addition to regular reporting, must also enable the timely notification of the governing bodies of the obliged entity about identified deficiencies in the system for preventing money laundering and terrorist financing, the corrective measures taken, and the deadlines set for their elimination.

(4) Information and data on suspicious transactions, funds, and client activities provided by the obliged entity to the State Investigation and Protection Agency's Financial Intelligence Department must be accurate, complete, timely, concise, and sufficient for further action.

Internal Control and Audit

Article 9

(1) The obliged entity referred to in Article 3 of this Rulebook shall, within its regular activities undertaken for the effective management of the risk of money laundering, terrorist financing, and proliferation of weapons of mass destruction, establish internal controls throughout its entire organisational structure, at all levels, across all functions and business lines, proportionate to the size and nature of its operations, and shall adapt them to changes in the organisation and business environment.

(2) The obliged entity referred to in Article 3, paragraph 1, points 1) and 3) of this Rulebook shall, at least once a year, ensure an independent internal audit of the assessment of the system for preventing money laundering, terrorist financing, and proliferation of weapons of mass destruction, proportionate to the size and nature of its operations.

(3) The obliged entity referred to in Article 3, paragraph 1, point 2) of this Rulebook shall ensure an independent internal audit of the assessment of the system for preventing money laundering, terrorist financing, and proliferation of weapons of mass destruction when its law or implementing regulations require the establishment of an internal audit function, or when the obliged entity or its supervisory authority determines that, considering the size and nature of the operations, it is necessary.

(4) Compliance of the obliged entity's operations with the requirements of the Law on AML/CFT and regulations shall be subject to independent assessment by the internal audit function of the obliged entity, which includes evaluating the adequacy of the entity's policies, procedures, measures, actions, and processes.

(5) The internal audit of the obliged entity shall conduct regular assessments of the processes and risk management system in the operations of the obliged entity to ensure that such risks are appropriately identified, measured or assessed, monitored, analysed, and controlled, that adequate reporting is performed, and that appropriate measures are taken to mitigate and manage such risks.

External Audit

Article 10

(1) The obliged entity referred to in Article 3, paragraph 1, points 1) and 3) of this Rulebook shall contract with an independent auditing firm to perform an audit for the assessment of compliance of its operations with the requirements for the prevention of money laundering, terrorist financing, and proliferation of weapons of mass destruction.

(2) In order to fulfil its tasks and obligations, the independent auditor, with respect to the prevention of money laundering, terrorist financing, and proliferation of weapons of mass destruction, shall provide an assessment of:

1) the implementation of the statutory and other prescribed obligations of the obliged entity;
2) the implementation of the programme, policies, and procedures;
3) adherence to risk management rules;
4) the adequacy of the performance of control functions;
5) the adequacy of the information system;

6) timeliness, correctness, accuracy, and completeness of reporting to the competent authorities; and
7) the adequacy and effectiveness of the internal control system in relation to risk management.

(3) The audit of compliance with the requirements for the prevention of money laundering, terrorist financing, and proliferation of weapons of mass destruction may be performed by the same independent auditor who conducts the audit of the financial statements.

(4) The contract with the independent auditor shall be concluded in the manner and within the deadlines defined by the regulations governing the audit of financial statements.

(5) After completing the audit of compliance with the requirements for the prevention of money laundering, terrorist financing, and proliferation of weapons of mass destruction, the independent auditor shall prepare a report on the audit performed. The report shall include findings and assessments of the effectiveness of the obliged entity on all matters referred to in paragraph (2) of this Article.

(6) The report on the audit referred to in paragraph (5) of this Article shall be submitted by the obliged entity to the Agency within the deadline prescribed for submitting reports on financial statement audits.

(7) The independent auditor is obliged to immediately notify the Agency and the governing bodies of the obliged entity in writing about:

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

(8) Providing data to the Agency under paragraph (7) of this Article shall not be considered a violation of the auditor's obligation to maintain confidentiality arising from regulations governing the audit field or from the contract.

(9) The Agency may require additional explanations from the external auditor regarding the audit performed, as well as verification of the audit report by another external auditor if there are reasons to doubt the truthfulness, accuracy, and completeness of the opinion given in that report. The cost of verifying the audit report by another external auditor shall be borne by the obliged entity.

III. INTERNAL ACTS

Programs, Policies, and Procedures

Article 11

(1) The obliged entity referred to in Article 3 of this Rulebook is required to adopt and implement appropriate internal acts and establish control procedures which, for the purpose of effective risk management, will cover all actions and measures for the prevention and detection of money laundering, financing of terrorist activities, and proliferation of weapons of mass destruction, as defined by the Law on Prevention of Money Laundering and Financing of Terrorism (AML/CFT

Law), the subordinate acts adopted pursuant thereto, including the Risk Assessment of Money Laundering and Financing of Terrorist Activities in Bosnia and Herzegovina.

(2) The obliged entity referred to in Article 3 of this Rulebook is required to adopt a program for implementing the activities referred to in Article 1 of this Rulebook, which shall include policies and procedures as its integral components.

(3) The provisions of the program, as well as all policies and procedures, must be fully implemented by the obliged entity in all organizational units and across all business lines.

(4) Through the acts referred to in paragraph 1 of this Article, the obliged entity is required to ensure high ethical and professional standards of responsible employees and to effectively prevent any possibility of their misuse for the purpose of money laundering, financing of terrorist activities, or proliferation of weapons of mass destruction, whether the employees are aware of it or not.

(5) The obliged entity referred to in Article 3 of this Rulebook is required to ensure the application of the acts referred to in paragraph 1 of this Article by establishing appropriate procedures and systems of internal controls.

Content of the Program, Policies, and Procedures

Article 12

(1) A mandatory part of the program referred to in Article 11 of this Rulebook are the policies and procedures regulating the following segments:

1) risk assessment and client acceptability,
2) identification and verification of the client's identity,
3) monitoring of business relationships and transactions, and
4) risk management.

(2) The policies and procedures for implementing the program referred to in Article 11, paragraph 1 of this Rulebook shall be based on risk assessment and the application of the "know your client" principle.

(3) Policies and procedures shall be adopted by the competent body of the obliged entity.

(4) The obliged entity is required, through policies and procedures, to define the objectives, processes, scope, and operation of the system for preventing money laundering, financing of terrorist activities, and proliferation of weapons of mass destruction. In particular, the obliged entity must define through policies and procedures:

1) client acceptability, and prescribe comprehensive procedures for implementing this policy,
2) the methodology for assessing the risk of the client and beneficial owner, their geographic origin, business relationship, and transactions,
3) measures for client identification and monitoring of client activities and transactions in the manner and under the conditions prescribed by the AML/CFT Law,
4) the methodology for assessing the risk of overall business operations,
5) measures and actions to be taken regarding clients with whom no business relationship has been established, but for whom occasional transactions are conducted,
6) measures and actions to be taken to implement targeted financial sanctions (restrictive measures),
7) products or services that the obliged entity will not provide to clients of a certain risk category,

8) taking enhanced measures for risk management and risk mitigation where a high level of risk has been identified,

9) taking simplified measures for risk management and risk mitigation where a low level of risk has been identified,

10) managing isolated or specific risks that are characteristic of the obliged entity's business model, products, or services,

11) appointing the authorized person and their deputies, their position within the organizational structure of the obliged entity, and the powers and responsibilities of the authorized person and their deputies,

12) protection against unauthorized disclosure of information concerning the persons referred to in point 11) of this paragraph and other procedures that may affect the smooth performance of their duties,

13) an appropriate procedure for determining and verifying conditions when establishing employment or engaging persons outside employment with the obliged entity who participate in implementing the AML/CFT Law and the adopted subordinate regulations, as well as a procedure for ongoing verification of these conditions during the employment/engagement period,

14) the powers and responsibilities of all employees of the obliged entity involved in implementing the AML/CFT Law and adopted subordinate regulations,

15) a procedure for anonymous internal reporting of violations of the provisions of the AML/CFT Law and subordinate regulations, including record-keeping and defining the actions the obliged entity will undertake in response to anonymous reports,

16) models for managing the risk of money laundering, financing of terrorist activities, and proliferation of weapons of mass destruction,

17) methods and models for managing compliance of the obliged entity's operations with the provisions of the AML/CFT Law and adopted subordinate regulations,

18) establishing appropriate reporting lines within the obliged entity, as well as reporting lines to the competent authorities,

19) the storage, access, and handling of data, information, and documentation collected in accordance with the AML/CFT Law and subordinate regulations,

20) the manner of keeping and the content of records of collected data,

21) professional training and education of employees of the obliged entity, and

22) conducting internal and external audits of the system for preventing money laundering, financing of terrorist activities, and proliferation of weapons of mass destruction, where appropriate to the size and nature of the obliged entity's operations.

(5) Policies, procedures, and control measures shall be proportionate to the size of the obliged entity, the type, scope, and complexity of the operations it conducts.

IV. IDENTIFICATION AND MONITORING MEASURES

Determination and Verification of Client Identity

Article 13

(1) The entity referred to in Article 3 of this Rulebook is required to implement detailed and comprehensive client identification measures. These measures will depend on the risk category into which individual clients and the products or services they use are classified. Depending on these categories, the entity will apply proportional client identification measures. Identification measures may be: simplified, standard, or enhanced.

(2) The identification procedure is carried out when establishing business relationships. However, to ensure that the documents remain valid and relevant, the entity is required to conduct regular reviews and updates of the collected documents.

(3) The entity shall implement the identification and monitoring measures referred to in paragraphs 1 and 2 of this Article throughout the duration of the business relationship with the client, based on a risk assessment or when relevant circumstances concerning the client change, in all cases where significant transactions are conducted, when there are significant changes in the way the client uses the obliged entity's products or services, when the entity significantly changes the standards for documenting the client's identity or transactions, or when it is required under the provisions of the AML/CFT Law.

(4) When establishing business relationships with new clients, as well as in the cases referred to in paragraphs 2 and 3 of this Article, the obliged entity is required to verify the client's identity using reliable and independent sources of documents, data, or information.

(5) Client identity verification must be completed before establishing a business relationship or executing a transaction. Exceptionally, the obliged entity may carry out verification during the establishment of a business relationship if necessary to avoid disruption of ordinary business operations and where a low risk has been identified. In such cases, these procedures must be completed as soon as possible after the first contact.

(6) Exceptionally from paragraph 5 of this Article, the obliged entity may establish a business relationship provided that appropriate safeguards are in place to ensure that clients or any person acting on their behalf do not conduct transactions until full compliance with the identification and monitoring requirements prescribed by the AML/CFT Law has been achieved.

Obligations Regarding Client Identification

Article 14

(1) The entity referred to in Article 3 of this Rulebook is required to determine and verify the client's identity based on documents, data, or information collected from reliable and independent sources, as well as documents prescribed by other applicable regulations. When carrying out identification measures, the obliged entity must collect all data required by the AML/CFT Law. Special attention must be given to non-resident clients as well as new clients who are not physically present when establishing a business relationship or conducting a transaction.

(2) The entity referred to in Article 3, paragraphs 1 and 2 of this Rulebook is required, except for the policyholder, to determine and verify the identity of the insured person designated as a specifically named natural or legal person, or other persons with a legal interest, as soon as the insured person is identified.

(3) In cases where the obliged entity becomes aware that there is insufficient information about an existing client, it must take urgent measures to collect the necessary information, i.e., it must immediately and as quickly as possible verify the updated identification data.

(4) The obliged entity is required, for client identification and for each individual product, to establish standards regarding the type of necessary documentation and the retention period for such documentation, at a minimum in accordance with the AML/CFT Law.

(5) The obliged entity may not establish a business relationship or conduct business with a client who insists on anonymity, or who uses a false name, provides inaccurate identification data, or submits forged documentation during the identification process. In such cases, the obliged entity is required to make a record of the business contact with the client and submit a report to the FIU in accordance with the AML/CFT Law.

(6) If the implementation of identification and monitoring measures raises the client's suspicion that the obliged entity is taking actions for the purpose of providing data to the FIU, the obliged entity is required to suspend those actions and measures and prepare an official written record, which must be immediately submitted to the FIU without delay.

(7) When carrying out standard and enhanced identification measures, the obliged entity is required to verify the documents, as well as to confirm that the client with whom the business relationship is being established actually exists, is at the registered address, and is genuinely conducting the stated business activities.

(8) Requirements for clients must be defined according to the risk category assigned to the client, so that simplified identification and monitoring procedures are applied for low-risk clients, standard identification and monitoring procedures for medium-risk clients, and enhanced identification and monitoring measures for high-risk clients.

(9) Regular monitoring activities may not be delegated to a third party.

Determination and Verification of the Beneficial Owner's Identity

Article 15

(1) In order to fulfil the obligations prescribed by the Law and subordinate regulations, the obliged entity is required to verify the identity of the client and the beneficial owner of the client based on reliable and independent information and data, in accordance with the AML/CFT Law.

(2) The obliged entity is required to determine and verify the identity of the beneficial owner of the client, who directly or indirectly owns or controls the client as a legal entity, so that at any given time it knows the ownership and management structure of the client and identifies who the beneficial owners are, including taking measures necessary to understand the nature of the client's business, ownership, and control structure when the client is a company, other legal entity, or an equivalent subject.

(3) When verifying the identity of the beneficial owner of a legal entity, the obliged entity shall at a minimum take the following steps:

1) request information about the beneficial owner from the client;
2) document the obtained data and information; and
3) take all measures necessary to verify the obtained data and information in accordance with the AML/CFT Law and subordinate regulations.

(4) The obliged entity is required, through its policies and procedures, to specify which information and data will be considered reliable and independent for the purpose of identifying and monitoring the beneficial owner.

Obligations Regarding the Identification of the Client's Beneficial Owner

Article 16

(1) The obliged entity may use data on beneficial owners by consulting the central register of beneficial owners, a register maintained by the competent authority of the state of establishment, or another public register, to the extent that such access is available, bearing in mind that the use of information from a beneficial ownership register alone does not in itself fully satisfy their obligation to take appropriate risk-based measures to determine and verify the identity of the beneficial owner.

(2) The obliged entity shall take additional steps to identify and verify the beneficial owner, particularly where the risk associated with the business relationship is higher or where the obliged entity is not certain that the persons listed in the register are the ultimate beneficial owners.

(3) The requirement to identify and take all necessary and reasonable measures to verify the identity of the client's beneficial owner applies only to a natural person who is the ultimate owner of the client and/or a natural person who has the right to exercise significant influence over the decision-making of the management body of a company and/or who receives, manages, or distributes assets for a specific purpose. However, in order to comply with the obligations prescribed by the AML/CFT Law, the obliged entity shall also take reasonable measures to understand the client's ownership and control structure.

(4) The measures that the obliged entity is required to take in order to understand the client's ownership and control structure must be sufficient to provide reasonable assurance regarding the risk associated with different levels of ownership and control. In particular, the obliged entity must ensure that the client's ownership and control structure is not unjustifiably complex or non-transparent, or that a complex or non-transparent ownership and control structure has a legitimate legal or economic reason.

(5) In order to fulfil its obligations under the AML/CFT Law, the obliged entity is required to notify the FIU immediately and without delay if, inter alia, it is unable to identify and verify the client's beneficial owner, or if there is suspicion that the client's ownership and control structure gives rise to suspicion and/or if there are grounds to suspect that the funds constitute proceeds of illegal activity or are related to the financing of terrorism.

Verification of the Identity of the Client and the Beneficial Owner

Article 17

(1) Confirmation, i.e. verification, of the collected data and information regarding the client and the client's beneficial owner shall be ensured by the obliged entity through inspection and obtaining documentation containing the data and information on the client and the client's beneficial owner, or in another manner prescribed by the AML/CFT Law.

(2) When identifying the persons referred to in Articles 14 and 15, paragraphs 1 and 2 of this Rulebook, the obliged entity is required to obtain the original or a certified copy of the documentation containing the collected data and information on the client and the client's beneficial owner, or to make a copy thereof by inspecting the original or certified copy, which shall also include an electronic document.

(3) If the person referred to in Article 14, paragraph 2 of this Rulebook is not designated by name or title, the obliged entity is required to obtain such scope of information as will be sufficient to establish their identity, i.e. the identity of the beneficial owner of that beneficiary, no later than at

the time of payment of the insured amount or the exercise of rights arising from surrender, advance payment, or pledging of the insurance policy.

(4) If the obliged entity has made a copy of an identification document during the implementation of identification measures, it is required to ensure that the copy, whether in paper or electronic form, includes the date and time when the identification was carried out, as well as the name, surname, and signature of the employee who performed the identification.

Regular Identification and Monitoring Measures

Article 18

(1) Regular identification and monitoring measures include determining and verifying the identity of the client and the client's beneficial owner, obtaining and assessing information regarding the purpose and intended nature of the client's business relationship or transaction, as well as regularly monitoring their business, in cases and in the manner prescribed by the AML/CFT Law.

(2) When carrying out the measures referred to in paragraph 1 of this Article, the obliged entity is required to 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 AML/CFT Law and this Rulebook, determine and verify that person's identity.

(3) Regular identification and monitoring measures apply to medium-risk clients or occasional transactions that the obliged entity assesses as representing a medium risk.

Simplified Identification and Monitoring Measures

Article 19

(1) The obliged entity may apply simplified identification measures in cases where a business relationship is established with clients who have been identified as lower-risk levels in accordance with the conducted risk assessment.

(2) The obliged entity may apply simplified identification and monitoring measures to long-term life insurance policies or voluntary pension insurance contracts that are assessed as representing low risk, taking into account the results of the Money Laundering and Terrorist Financing Risk Assessment in Bosnia and Herzegovina.

(3) The obliged entity is required to collect sufficient information to determine whether the client meets the conditions for applying simplified identification and monitoring measures, and to carry out regular monitoring measures to detect unusual or suspicious activities or transactions that clients may attempt to conduct.

(4) If there is suspicion that the activity involves money laundering, terrorist financing, or the proliferation of weapons of mass destruction in connection with the client, transaction, or service to which simplified measures were applied, the obliged entity is required to conduct an additional assessment and apply enhanced identification and monitoring measures.

(5) In accordance with the provisions of the AML/CFT Law, the obliged entity is required to collect and verify the prescribed data and information about the client by inspecting the original or certified copy of valid documents or documentation containing the client's data and information, such as: personal identification document, extract from the relevant register, and other documentation prescribed by the AML/CFT Law, taking into account the conducted risk assessment.

Enhanced Identification and Monitoring Measures

Article 20

(1) The obliged entity is required to apply enhanced identification and monitoring measures to a specific business relationship or transaction that is determined to pose a high risk under the AML/CFT Law, the Money Laundering and Terrorist Financing Risk Assessment in Bosnia and Herzegovina, or the obliged entity's own risk assessment.

(2) Enhanced identification and monitoring measures shall also be applied in cases of a business relationship or transaction when the client: terminates the contractual relationship shortly after its conclusion, particularly if it involves a high premium or contribution amount; makes large and frequent premium or pension contribution payments; or makes amendments to the contract for unusually large increases in premiums or contributions that lack an apparent economic or lawful purpose.

(3) In addition to regular measures, enhanced identification and monitoring measures include additional steps that the obliged entity must take in the cases referred to in paragraph 1 of this Article, as well as in other cases where it assesses that, due to the nature of the business relationship, the manner of the transaction, the type of transaction, the client's ownership structure, or other circumstances related to the client or transaction, there exists or could exist a high risk of money laundering, terrorist financing, or proliferation of weapons of mass destruction.

(4) The obliged entity is required to define in its internal act which enhanced measures will be taken and the extent to which additional data will be obtained and additional verification of collected documentation will be performed in each specific case. The type of additional measures to be undertaken must be based on the risk factors by which the client, business relationship, transaction, service, or distribution channel has been assessed as high risk.

Application of the Proportionality Principle

Article 21

(1) When determining requirements for clients in the process of implementing identification and monitoring measures of client activities and transactions, the obliged entity is required to apply the principle of proportionality. By applying the principle of proportionality, the obliged entity shall ensure that the measures taken are sufficient and adequate to achieve the intended objective.

(2) In the process of determining the requirements referred to in paragraph 1 of this Article, the obliged entity shall ensure that the application of the principle of proportionality does not affect the achievement of the objectives of the legal requirements and the requirements of this Rulebook regarding the comprehensiveness, reliability, and effectiveness of the risk management system for money laundering and terrorist financing.

Application of the "Know Your Customer" Principle

Article 22

(1) In daily business operations and client relationships, the obliged entity shall learn about and become familiar with the client's activities, understand their business, be aware of financial habits, business relationships, sources of funds used in the contractual relationship, and obtain relevant information and documentation regarding the client's business activities. The obliged entity is required to:

1) monitor whether the client's activities are consistent with the purpose and intended nature of the business relationship established between the client and the obliged entity; in the case of legal entities, become familiar with the ownership structure of the legal entity (beneficial owner), the authorized legal representative, and all persons authorized to act on behalf of the legal entity.
2) to require its clients to timely provide information and documentation regarding expected and intended changes in the form and conduct of their business activities;
3) to ensure that the documentation, data, and information collected within the processes of identification, verification, and monitoring are up to date and relevant, and to review existing records, particularly for categories of high-risk clients; and
4) to pay special attention to well-known clients, politically exposed persons, and public figures, and to ensure that any potential unlawful or suspicious activities on their part do not jeopardize the reputation of the reporting entity.

(2) The reporting entity may not delegate regular monitoring activities to a third party.

Unusual Transactions

Article 23

(1) The reporting entity shall establish comprehensive controls, i.e. conduct due diligence of clients and transactions, taking into account: complexity, unusually high amounts, unusually linked transactions, unusual or seemingly disadvantageous early surrender or request for payment of contributions, any unusual method of payment lacking a clearly evident economic or legal purpose, or transactions that are inconsistent with or disproportionate to the client's usual, expected business activities.

(2) The reporting entity shall require clients to provide an explanation for any observed significant change in behaviour.

(3) Where clients are unable to provide an explanation, or provide an unconvincing and unsubstantiated explanation, the reporting entity shall treat such behaviour as suspicious and implement additional measures for a more detailed examination, including submitting a suspicious activity report on the client to the FIU.

(4) In relation to clients and transactions or funds referred to in paragraph (1) of this Article, the reporting entity shall at a minimum verify information concerning the source of funds, the client's business activity, and the intended nature of the business relationship with the client. If it determines that the transaction is not suspicious, it shall make an official written or electronic note to that effect and retain it so that it is available upon request of the FIU and the Agency.

(5) Unusual and atypical behaviours giving rise to suspicion shall include, inter alia:

1) an unexpected change in the client's financial behaviour that cannot be explained by business or financial motives;
2) the unexpected emergence of a new person, business and/or geographical area deviating from the previously known manner and type of business operations, and the client's business and financial network known to the reporting entity;
3) unusual or seemingly disadvantageous early surrender of insurance, or a requested payment of contributions;
4) a specific feature of a transaction that does not fit into the client's usual practice;
5) where payment is made before the application has been processed and the risk accepted.

6) unusual engagement of an intermediary in the course of a routine transaction or financial activity (e.g. payment of an unusually high commission to an intermediary that has not been contractually agreed);
7) the client's explanation of a transaction is unconvincing and appears false;
8) frequent repetition of transactions in amounts slightly below the threshold prescribed by the AML/CFT Law for reporting and notification to the FIU;
9) where employees of the reporting entity do not have clear evidence of unlawful activities but have a suspicion that such a possibility exists; and
10) any involvement of a person subject to international sanctions.

(6) If, in relation to transactions or funds referred to in paragraph (1) of this Article, the reporting entity, following an analysis, determines that there are grounds for suspicion of money laundering or terrorist financing, it shall inform the FIU in the manner and within the time limits prescribed by the AML/CFT Law.

Monitoring for the Purpose of Preventing Money Laundering

Article 24

(1) The reporting entity shall conduct ongoing monitoring of the client's activities and transactions and shall ensure the implementation of measures, instruments, mechanisms, and comprehensive controls for detecting activities and transactions that are inconsistent with the nature of the client's behaviour, thereby effectively managing and minimizing its risk in business relationships with clients.

(2) The scope to which the reporting entity develops monitoring of client activities and transactions shall be proportionate to the need for adequate risk sensitivity. For all transactions and clients, the reporting entity shall establish a system capable of detecting all unusual, atypical, and suspicious types of transactions and activities.

(3) The reporting entity shall establish comprehensive controls and monitoring of client activities and transactions, taking into account the nature, size, and complexity of its operations, as well as the assessed level of risk to which it is exposed in the course of its business activities.

Monitoring of Client Transactions and Activities

Article 25

In order to ensure the achievement of the objectives referred to in Article 24 of this Rulebook, the reporting entity shall:

1) define the types of activities and transactions that must alert the reporting entity to the possibility that clients are conducting unusual, atypical, or suspicious transactions;
2) define the types of transactions which, by their nature, primarily lack economic or legal justification;
3) determine which client activities are to be monitored in real time and which may be subject to subsequent (ex post) monitoring (including defining the frequency of such subsequent monitoring), and shall also define the circumstances indicating high risk to be applied when determining which transactions are to be monitored in real time;
4) in addition to the obligations referred to in item 3) of this paragraph, the reporting entity referred to in Article 3, paragraphs 1 and 3 of this Rulebook shall regularly, and at least once a year, review executed transactions and paid premiums/contributions in order to verify the reliability and adequacy of the established system for monitoring activities and transactions.

5) establish transaction limits (payment of premiums in full or in instalments, or payment of pension contributions), and examine all transactions that exceed the established limits;

6) prepare an official and as comprehensive as possible list of examples of suspicious activities and transactions, as well as examples and methods of possible forms of money laundering; and

7) establish an adequate system enabling the creation of accounting documentation and records containing all data that satisfactorily describe the business event that has occurred, and which will serve as a sufficient tool for conducting analysis and monitoring account turnover, i.e. all of the client's business activities.

Enhanced Monitoring Measures

Article 26

(1) For business relationships, products, and services that present a high risk, the reporting entity shall apply enhanced monitoring measures.

(2) In order to identify the category of high-risk business relationships, products, and services, the reporting entity shall determine key indicators on the basis of which such business relationships are categorized into this group, taking into account data on the client's history and available knowledge about the client, such as the sources of funds used in the business relationship, the type and nature of the transactions themselves, the client's country of origin, and other relevant factors.

(3) For high-risk business relationships, products, and services, the reporting entity shall:

1) establish an appropriate information management system to ensure that senior management and the employees responsible for monitoring compliance with the requirements prescribed by the AML/CFT Law and other regulations in this field are provided in a timely manner with the necessary information for identification and effective monitoring of client activities, as well as of the products and services used by clients. This system shall include, at a minimum:

– reporting on missing documentation required for full and reliable client identification;
– reporting on unusual, atypical, and suspicious client activities and transactions; and
– reporting comprehensive information on the overall business relationships of clients with the reporting entity.

2) ensure that senior management is well acquainted with the situation of clients presenting high risk, that it collects and assesses information obtainable from other reporting entities, as well as from domestic and international institutions competent in combating money laundering and terrorist financing. Significant transactions of such clients shall be subject to approval by the senior management of the reporting entity.

Implementation of International Targeted Financial Sanctions

Article 27

(1) In accordance with the regulations governing this area, and for the purpose of combating the financing of terrorist activities and the financing of the proliferation of weapons of mass destruction, the reporting entity shall timely implement targeted financial sanctions based on internationally binding decisions of the United Nations and competent domestic institutions, inform the competent authorities, and freeze the financial assets of persons whom the reporting entity knows or suspects to be subject to targeted financial sanctions.

(2) The reporting entity referred to in Article 3 of this Rulebook shall adopt procedures for the implementation of targeted financial sanctions, defining and establishing a comprehensive process for database screening in terms of scope and frequency, data and alert analysis, record-keeping, and the establishment of reporting lines within the reporting entity and towards the competent authorities.

(3) The reporting entity shall pay particular attention to:

1) verifying whether funds from lawful sources or business activities are, in whole or in part, diverted to support terrorist activities and the proliferation of weapons of mass destruction;
2) implementing comprehensive controls to prevent the financing of terrorists, terrorist organizations, and persons associated with them;
3) continuously monitoring updates to lists of persons subject to restrictive measures adopted by the United Nations Security Council and competent domestic institutions;
4) activities aimed at determining the true identity and/or purpose of, in particular, small payments where the purpose of the transfer and/or the sender and/or the recipient are not clearly indicated;
5) cases where premiums or contributions are paid by non-profit and charitable organizations, particularly where the activities conducted are not consistent with their registered activity or where the source of funds is unclear.

(4) Through monitoring client activities and transactions, the reporting entity shall determine whether clients, or persons acting as originators or beneficiaries in transactions carried out without establishing a business relationship, are persons subject to restrictive measures imposed by the United Nations Security Council and competent domestic institutions.

(5) In cases where persons referred to in paragraph (4) of this Article attempt to establish a business relationship with the reporting entity, or where such persons are existing clients, the reporting entity shall provisionally freeze the funds and restrict the use of products and services utilized with the reporting entity, and shall notify the competent authorities thereof.

V. RISK MANAGEMENT AND MANAGEMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISK

Risk Assessment

Article 28

(1) The reporting entity referred to in Article 3 of this Rulebook shall establish a comprehensive risk management process, which includes the identification of risk factors and regular risk assessment.

(2) The reporting entity shall assess:

1) the risk to which it is exposed due to the nature and complexity of its business (overall business risk assessment); and
2) the risk to which it is exposed due to the establishment of a business relationship 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 interconnected steps: the identification of risk factors and the evaluation of risk.

(4) When assessing the overall level of residual risk associated with its business and with individual business relationships or occasional transactions, the reporting entity shall take into account the level of inherent risk, the quality of controls, and other risk mitigation factors.

(5) The reporting entity shall record and document its overall business risk assessment and individual risk assessments, as well as any changes to these risk assessments, in a manner that allows both the entity and the competent authorities to understand how and why the assessments were conducted in a particular way.

(6) The reporting entity shall ensure that the risk assessment reflects its understanding of the risks and shall be able to demonstrate this to the competent authorities.

Updating the Risk Assessment Methodology

Article 29

(1) The reporting entity referred to in Article 3 of this Rulebook shall establish a system of internal controls and regularly review the methodology for assessing overall business risk and individual risk assessments, ensuring that the risk assessment remains up to date and appropriate.

(2) The reporting entity's system of internal controls referred to in paragraph (1) of this Article shall, at a minimum, include:

1) a specified date during the year on which the overall business risk assessment is updated, as well as a date determined based on risk sensitivity for individual risk assessments, to ensure the inclusion of newly emerging risks and risks in development. If the reporting entity becomes aware of a new risk before this date, it shall analyse and incorporate it into individual risk assessments and overall business risk assessments;
2) records of all significant factors that could affect risk assessments, such as internal reports on suspicious transactions, non-compliance, and information obtained from employees who interact directly with clients, among others.

(3) The reporting entity shall establish a system of internal controls to identify emerging risks and assess them, and shall incorporate them into its overall business risk and individual risk assessments in a timely manner, as necessary.

(4) The system of internal controls referred to in paragraph (3) of this Article shall, at a minimum, include:

1) procedures ensuring that internal information, such as information obtained through ongoing monitoring of business relationships and client activities, is regularly reviewed to identify trends and newly emerging issues related to individual business relationships and the reporting entity's overall business;
2) procedures for regularly reviewing significant sources of information; and
3) cooperation with representatives of other competent authorities, and procedures for providing relevant feedback to employees.

(5) The procedures referred to in paragraph (4), item 2) of this Article, concerning overall business risk assessments, shall, at a minimum, include:

1) alerts 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, particularly risks related to new categories of clients, countries or geographic areas, new products, new services, new sales channels, as well as new compliance systems and controls.

(6) The procedures referred to in paragraph (4), point 2) of this Article, with respect to individual risk assessments, shall, at a minimum, include:

1) alerts regarding terrorist threats and targeted financial sanctions regimes, or their amendments, as soon as they are published or communicated, ensuring that they are acted upon; and

2) media reports relevant to the sectors or countries, or geographic areas, in which the reporting entity actively operates.

Overall Business Risk Assessment of the Reporting Entity

Article 30

(1) The overall business risk assessment shall enable the reporting entity to identify areas in which it is exposed to risk and to determine which areas of its business should be prioritized in its efforts to mitigate risk.

(2) The reporting entity referred to in Article 3 of this Rulebook shall identify each segment of its business, including all existing and new products, services, processes, activities, and procedures, in order to assess in which business segments threats of money laundering, terrorist financing, and the proliferation of weapons of mass destruction may arise. The entity shall also adequately assess the potential negative consequences arising from these risk sources and their potential impact on the achievement of the reporting entity's business objectives.

(3) The reporting entity shall ensure that its overall business risk assessment is tailored to its business profile and that all factors and risks specific to the entity's operations are taken into account. If the reporting entity is part of a group that prepares a group-level risk assessment, the reporting entity shall consider whether the group-level risk assessment is sufficiently precise and specific to reflect its own operations and the risks it faces due to the group's connections with countries and geographic areas, and shall, if necessary, supplement the group-level risk assessment.

(4) Based on the assessed likelihood of risk occurrence and the estimated negative consequences, the reporting entity shall determine the level of risk exposure for each segment of its business.

(5) The reporting entity shall base its overall business risk assessment on all relevant information, shall update it at least once a year, and shall submit it to the Agency.

Risk Analysis and Risk Factors of an Individual Business Relationship or Occasional Transaction

Article 31

(1) The reporting entity shall conduct a risk analysis in order to identify, assess, understand, and mitigate the risks to which it is exposed or may be exposed when establishing or maintaining a business relationship or executing a specific occasional transaction. In conducting the risk analysis, the reporting entity shall take into account risk factors relating 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 shall also include other risk factors that the reporting entity is required to identify due to the specific nature of its business. The risk analysis shall be documented and proportionate to the size of the reporting entity, as well as to the nature, scope, and complexity of its operations, and shall be regularly updated, at least once a year.

(3) The risk analysis referred to in paragraph (1) of this Article shall also include the measures, actions, and procedures undertaken by the reporting entity for the purpose of preventing and detecting money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

(4) The reporting entity shall align the risk analysis referred to in paragraph (1) of this Article with rulebooks and decisions, i.e. guidelines issued by the competent authority, and when preparing and updating it, shall also take into account the Risk Assessment of Money Laundering and Terrorist Financing in Bosnia and Herzegovina.

(5) Based on the conducted risk analysis for each group or type of client, business relationship, service provided within the scope of its activities, or transaction, the reporting 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; or
3) high-risk category.

Weighting of Risk Factors

Article 32

(1) The reporting entity shall consider all identified risk factors and activities related to the business relationship or transaction. In the course of the assessment, the reporting entity may assign different weights to risk factors depending on their individual significance within the context of the business relationship or transaction.

(2) The weight assigned to risk factors may vary depending on the specific product, service, or client, as well as depending on the individual reporting entity.

(3) When weighting risk factors, the reporting entity shall ensure that:

1) the weighting is not influenced by only a single risk factor;
2) economic considerations and profit-related considerations of the reporting entity do not influence the risk assessment;
3) the weighting of risk factors does not result in a situation where no business relationship can be classified as high risk;
4) the risk category established by the AML/CFT Law cannot be altered; and
5) where necessary, an automatically generated risk assessment may be adjusted based on a conducted analysis and a written justification by an authorized person of the reporting entity.

(4) If the reporting entity performs the overall risk assessment for the purpose of classifying a business relationship or transaction into a specific risk category through an automated system that is not developed by the reporting entity but is provided by a third party, the reporting entity must understand the functioning of that system, including the manner in which risk factors are combined to arrive at the overall risk rating.

Risk Assessment of an Individual Business Relationship or Occasional Transaction

Article 33

(1) When assessing the risk of an individual business relationship or occasional transaction, the reporting entity shall take into account relevant parameters and risk factors in order to assess the risks associated with that specific business relationship or the execution of an occasional transaction.

(2) The risk parameters referred to in paragraph (1) of this Article shall, at a minimum, include:

1) the purpose and intended nature of the business relationship;
2) the purpose and objective of the transaction;
3) the value of the product/service, the amounts and size of executed transactions; and
4) the frequency or duration of the business relationship.

(3) When preparing the risk assessment referred to in paragraph (1) of this Article, the reporting entity shall take into account factors that may indicate a potentially higher or lower risk, as set out in the guidelines issued by the Agency.

Sources of Information

Article 34

(1) In order to determine risk, the reporting entity shall use information from various reliable sources, which may be accessed individually or through available commercial tools or databases that consolidate information from multiple sources.

(2) The reporting entity shall always take into account the following sources of information:

1) lists 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, as well as explanations of relevant legislation;
3) information from supervisory authorities, such as guidelines and explanations provided when imposing regulatory measures;
4) information from competent authorities, such as threat reports, alerts, and typologies; and
5) information obtained through initial customer identification measures and ongoing monitoring of client activities.

(3) Other sources of information that the reporting entity may take into account include:

1) its own knowledge and experience;

2) information from entities within 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 bodies, such as mutual evaluation reports,
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 obliged entity shall determine the type and number of sources on the basis of its risk assessment, taking into account the nature and complexity of its business, and shall not rely on a single source for the purpose of risk identification.

VI. MANAGEMENT OF IDENTIFIED RISK

Politically Exposed Persons

Article 35

(1) When establishing a business relationship, carrying out occasional transactions, and throughout the duration of the business relationship, the obliged entity shall prescribe procedures enabling it to determine whether the client and/or the beneficiary of insurance and/or the client's beneficial owner is a politically exposed person.

(2) The obliged entity shall be required to obtain data and information on the client's political exposure directly from the client and/or from publicly available registers and databases, and to update such information on an ongoing basis.

(3) For the purpose of determining political exposure, the obliged entity shall undertake the following activities:

1) obtain a written statement from the client as to whether the client is a politically exposed person, a member of the immediate family, 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 information and other relevant sources.

(4) The same identification and monitoring measures shall be applied by the obliged entity in cases where the founders, beneficial owners, persons authorized to represent, and persons authorized to dispose of funds in the accounts of a legal entity client are politically exposed persons.

(5) Where the client and/or the beneficial owner of the client who enters into a business relationship, carries out a transaction, or on whose behalf a business relationship is established or a transaction is conducted, is a politically exposed person, the obliged entity shall, within the framework of enhanced customer due diligence measures, undertake the following additional measures:

1) obtain information necessary to determine the source of wealth and the source of funds that are or will be the subject of the business relationship or transaction, based on documents and other documentation submitted by the client and/or the client's beneficial owner;
2) employees of the obliged entity conducting activities related to the establishment of a business relationship with the client shall secure prior written approval from the obliged entity's senior management before entering into such a type of business relationship; and
3) after establishing the business relationship, the obliged entity shall apply enhanced and ongoing monitoring of the transactions and other business activities of the politically exposed person.

(6) If the obliged entity determines that a client or the client's beneficial owner has become a politically exposed person during the course of the business relationship, it shall apply the actions and measures referred to in paragraph (5) of this Article and shall obtain written approval from senior management of the obliged entity for the continuation of the business relationship with that person.

(7) The measures referred to in this Article shall also apply to immediate family members and close associates of a politically exposed person.

(8) The obliged entity shall pay special attention to monitoring all business activities conducted with it by a politically exposed person and shall notify the authorized person immediately and without delay if it assesses that circumstances relating to the usual business activities of the politically exposed person have changed.

Establishing a Business Relationship without the Client's Physical Presence

Article 36

(1) Where, in the course of establishing a business relationship, the client or the legal representative, or the person authorized to represent a legal entity, is not physically present with the obliged entity, the obliged entity shall apply enhanced identification measures in order to mitigate and properly manage the risk that may arise from establishing a business relationship in this manner.

(2) When implementing the measures referred to in paragraph (1) of this Article, in addition to the regular customer identification and monitoring measures, the obliged entity shall apply additional measures, which include:

1) requesting additional data, documents, and information used to verify the client's identity, which are not required from other clients;
2) certification of the submitted documents;
3) independent contact with the client by the obliged entity;
4) additional verification of the presented documents or further verification of the client's data, independently and/or by engaging a specialized company for client control and assessment;
5) requiring that the first payment (deposit) be made through an account in the client's name held with another obliged entity that is required to apply similar customer due diligence standards, prior to executing other transactions of the client with the obliged entity; and
6) obtaining data and information regarding the reasons for the client's absence.

(3) If the obliged entity does not implement enhanced identification measures, it shall not establish a business relationship with a client who is not physically present at the time of establishing the business relationship.

Third Party
Article 37

(1) In fulfilling the requirements relating to the identification and verification of the client's identity, the obliged entity may rely on a third party; however, the ultimate responsibility for meeting such requirements remains with the obliged entity that relies on the third party.

(2) The obliged entity shall, in advance, verify whether the third party to whom it entrusts the implementation of client identification measures meets the conditions prescribed by the Law on AML/CFT.

(3) The obliged entity may not accept the performance of certain identification measures through a third party if that third party identified and verified the client's identity without the client's presence.

(4) The obliged entity shall ensure that a copy of the documentation containing the identification data and information on the basis of which the third party verified the client's identity is submitted to the obliged entity without delay.

(5) The obliged entity shall retain the documentation relating to the identification and verification of the client's identity conducted by the third party in accordance with the Law on AML/CFT.

(6) The obliged entity shall conclude a contract with the third party defining the identification and verification measures and actions to be undertaken by the third party, as well as specifying the manner and deadlines for submitting the collected identification documents and ensuring the protection of confidential and personal data.

Prevention of the Misuse of Technological Development
Article 38

(1) The obliged entity shall identify and assess the risks that may arise from the application of new business practices and from the sale of existing and new products through new technologies (e.g., internet-based sales).

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

(3) Within its risk management processes, the obliged entity shall establish criteria and procedures relating to new products, which shall, at a minimum, include the following:

1) ensuring the necessary technical, organizational, and human resources required to assess risks prior to the introduction or use of products, practices, or technologies, as well as for the implementation, application, and management of risks arising from new products;
2) defining the authorities and responsibilities for the testing, approval, and verification of new products. Where the risk analysis indicates that adequate resources have not been provided to understand and manage the risks of a new product, the management of the obliged entity shall postpone its introduction until such resources are secured; and
3) establishing procedures for the implementation of risk mitigation measures arising from the development of new technologies.

(4) In the policies and procedures referred to in paragraph (2) of this Article, the obliged entity shall define the specific risks related to the establishment of business relationships and the

execution of transactions by electronic means, via the internet and/or internet-based payment platforms or other interactive computer systems, by telephone, or through other devices and instruments that enable transactions to be conducted without the client's physical presence at the premises of the obliged entity.

(5) As part of managing these risks, the obliged entity shall:

1) when applying new technologies for the delivery of products/services, implement, in addition to regular customer identification and monitoring measures, additional measures aimed at mitigating and managing the risk of money laundering and terrorist financing;
2) ensure that, for the transactions referred to in paragraph (4) of this Article carried out by clients, identification data on the originator and the beneficiary, as well as the purpose of the transfer, are monitored throughout the entire course of the transfer;
3) establish security measures and controls of processes and systems, and ensure that they are regularly reviewed and tested;
4) apply secure and effective authentication measures to confirm the client's identity and authorization; and
5) ensure that client authentication includes a combination of at least two methods of verifying the client's identity.

(6) When establishing business relationships and conducting transactions by electronic means, the obliged entity shall ensure compliance with obligations applicable to all transfers.

(7) In cases where the obliged entity cannot obtain the necessary identification data and information on clients, it shall refuse to provide such types of services.

VII. FINAL PROVISIONS

Retention of Documentation

Article 39

The obliged entity shall retain information, data, and documentation relating to an established business relationship with a client, an executed occasional transaction, and the identification and monitoring measures carried out, as well as information and supporting documentation concerning authorized persons, professional training of employees, and the implementation of internal controls, in the manner and within the time limits prescribed by the Law on AML/CFT.

Transitional and Final Provisions

Article 40

(1) The Director of the Agency is authorized, as necessary, independently or in cooperation with other competent authorities, to issue recommendations, instructions, or guidelines to the obliged entities referred to in Article 3 of this Rulebook for the implementation of the Law on AML/CFT and the regulations adopted on the basis thereof.

(2) On the date of entry into force of this Rulebook, the Guidelines for Risk Assessment and Implementation of the Law on the Prevention of Money Laundering and Financing of Terrorist Activities in the Insurance Sector, No. UO-19/15 of 28 August 2015, and the Guidelines on Amendments to the Guidelines for Risk Assessment and Implementation of the Law on the Prevention of Money Laundering and Financing of Terrorist Activities in the Insurance Sector, No. UO-25/17 of 30 November 2017, shall cease to be effective.

(3) The obliged entities referred to in Article 3 of this Rulebook shall, no later than 90 days from the date of entry into force of this Rulebook, align their operations with the Law on AML/CFT, the subordinate regulations adopted under the Law on AML/CFT, and this Rulebook.

Entry into Force
Article 41

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

Number: UO-36/24
25 December 2024
Banja Luka

Chairman of the
Board of Directors
Goran Račić