Insurance State Supervision Service of Georgia

Methodological Recommendation N3

On Money Laundering and Terrorism Financing Risk Assessment by the Obliged Entity Supervised by the Insurance State Supervision Service of Georgia

May 17, 2022

Tbilisi

Legal Entity of Public Law Insurance State Supervision Service of Georgia taking into consideration the Georgian law "On Insurance", Article 9, Paragraph 7, Article 20, Paragraph 1, Article 21, sub-paragraphs "b" and "k", Georgian Law "On Facilitating Suppression of Money Laundering and Terrorism Financing," Article 4, sub-paragraph "f", Article 8, Article 10 and Article 38, Paragraph 5, "Statement of the LEPL Insurance State Supervision Service of Georgia" approved by the Decree 102 of the Government of Georgia on May 2, 2013, Article 3, sub-paragraph "t", and best international practice and experience in the field of prevention of money laundering and terrorism financing, issues the following recommendation on money laundering and terrorism financing risk assessment by the obliged entity supervised by the Insurance State Supervision Service of Georgia and approves it by the attached "Guideline On Money Laundering and Terrorism Financing Risk Assessment by the Obliged Entity Supervised by the Insurance State Supervision Service of Georgia".

Head of LEPL Insurance State Supervision Service of Georgia

David Onoprishvili

Guideline On Money Laundering and Terrorism Financing Risk Assessment by the Obliged Entity Supervised by the Insurance State Supervision Service of Georgia

1. General Provisions

1. The Guideline on money laundering and terrorism financing risk assessment by the obliged entity in the insurance sector is based on the legislation of Georgia, international recommendations and best practices related to the facilitation of the prevention of money laundering and terrorism financing.

2. The purpose of this Guideline is, on the one hand, to assist the obliged entity accountable to the Insurance State Supervision Service of Georgia (hereinafter - Service) in the development and effective implementation of the system for assessing and managing the risks of money laundering and terrorism financing, and on the other hand, to support or facilitate the Service to carry out effective supervision.

3. This is a non-binding guideline, which includes the main principles and standards to be applied by an obliged entity in assessing and managing the risks of money laundering and terrorism financing, and to be followed by the Service in supervision. A key requirement for the risk management system implemented by the obliged entity is to be adequate to preventive measures and able to deal with the money laundering and terrorism financing risks faced by the company. The assessment of these risks is one of the essential attributes of the compliance system implemented by the obliged entity.

4. Obliged entity is required to develop a risk management system. It can adapt this system to the nature, scale, and complexity of its activities.

5. Obliged entity ensures that all clients are assigned a certain level of risk.

6. Obliged entity must be able to justify the level of risk assigned to the client and the adequacy of the preventive measures to the Service.

7. Obliged entity can further identify low-risk factors or risk reduction criteria tailored to the specifics of its business, which should be properly substantiated and prescribed in policies/procedures. If the level of money laundering and terrorism financing assigned to a client is low the obliged entity has the right to apply simplified CDD measures in accordance with the legislation of Georgia; however, the obliged entity must ensure that the level of risk is actually low.

8. If the risk reduction or low-risk criteria is not specified in the policies/procedures and the assignment of low risk or reduction of risk is based on the individual features of the client, the obliged entity shall perform appropriate analysis/justification and document the analysis with indication of the date and the relevant circumstances. Upon request, the obliged entity shall provide above-mentioned information to the Service.

9. In the event of identifying high or higher client risk the obliged entity must apply EDD measures determined by the current legislation on facilitating suppression of money laundering and terrorism financing.

10. With the purpose of effective management and mitigation of the risks of money laundering and terrorism financing, the risk-based approach allows the obliged entity to identify, analyze and assess the risks and to take measures proportionate to the risks identified as well.

11. The risk management system developed by the obliged entity must be approved by the governing body of the company. It is also important for the employees of the company to have a high level of awareness of money laundering and terrorism financing issues and to be involved in continuous process of familiarizing with the relevant international standards and global events.

12. The assessment of money laundering and terrorism financing risk is a product, or a process based on a specific methodology aimed at identifying, analyzing and assessing these risks. A risk can be viewed as a combination of three factors: risk, vulnerability, and impact. Typically, risk event occurs when a threat exploits vulnerability. Therefore, the level of risk can be mitigated by reducing the scale of the threats, vulnerabilities or their impact.

13. Money laundering and terrorism financing risks include criminals/terrorist groups/terrorists; past, present or future money laundering/terrorism financing operations; incomes from criminal operations received within the country (in terms of terrorism financing - income from assets purchased either legally or illegally), or transnational inflow of proceeds from criminal activities outside the country.

14. Vulnerability of the anti-money laundering and terrorism financing prevention system may be related to certain features of the product, services/delivery channels, client base, institutions, systems, or jurisdictions (including ineffective systems and measures of control), which contributes to the risks of money laundering and/or terrorism financing.

15. The impact of money laundering and terrorism financing means the effect or damage that money laundering and terrorism financing can cause. It also implies both short and long-term consequences for financial systems/institutions and the damage to the country's economy and society in general.

16. During the risk assessment process, the personal data/information of the client must be protected in accordance with the legislation.

17. The terms used in this Guideline have the meaning defined by the Law of Georgia “On Facilitating Suppression of Money Laundering and Terrorism Financing” and other normative acts of Georgia unless otherwise provided by this Guideline.

2. Key elements of the risk management system

1. To manage money laundering and terrorism financing risks, the obliged entity will introduce a risk-based approach that involves identifying, understanding, and assessing the money laundering and terrorism financing risks faced by the company, which will be mitigated by proportionate preventive measures.

2. The risk assessment and management approach developed by the obliged entity should typically include the following elements:

   a)Business-wide risk assessments – business-wide risk assessments should help companies understand where they are exposed to money laundering/terrorism financing risk and which areas of their business they should prioritize in the fight against money laundering/terrorism financing.

   b) Customer Due Diligence - obliged entity should use the findings from its business-wide risk assessment to inform its decision on the appropriate level and type of CDD that they will apply to individual business relationships.

   c) Obtaining a holistic view – obliged entity should gather sufficient information to be satisfied that it has identified all relevant risk factors, including, where necessary, by applying additional CDD measures, and assess those risk factors to obtain a holistic view of the risk associated with a particular business relationship.

   d)Monitoring and review - in order to determine whether the risk associated with the business relationship has changed and to confirm that the information held by the obliged entity corresponds to the risk profile of the client, the information on the client must be regularly updated/revised, and the business relationship must be monitored.

3. Business-wide risk assessments

1. Business-wide risk assessment involves identifying, assessing, and managing money laundering and terrorism financing risks related to the core activities of the obliged entity.

2. Business-wide risk assessment should consider the inherent level of risk of the client and the beneficial owner, the nature and location of their business, jurisdiction, products, services and distribution channels, transactions, and other risk factors, the risk mitigation measures implemented in accordance with the compliance control system developed by the obliged entity, and the level of residual risk resulting from such measures.

3. Business-wide risk assessment methodology is approved by the governing body of the obliged entity. This risk assessment methodology should be detailed, clearly defined, and include the frequency of the risk assessments. Obliged entity should consider performing the business-wide

risk assessment annually. However, if according to the obliged entity's reasonable judgement the material circumstances associated with its risk profile have not changed, the risk assessment may be performed every 2-3 years.

4. If the obliged entity is a parent company (organization) registered in Georgia, it provides a business-wide risk assessment at the group level, which includes an assessment of the money laundering and terrorism financing risks of the parent company and group members defined as obliged entities in accordance with the legislation on facilitating suppression of money laundering and terrorism financing.

5. The process of risk assessment performed by the obliged entity and its result must be documented.

6. If requested by the Service, the obliged entity must demonstrate that its risk assessment and associated risk management measures are adequate.

4. Risk assessment methodology

1. The process of assessing the money laundering and terrorism financing risks consists of two distinct, albeit cohesive stages:

   a) Risk identification.

   b) Analysis and assessment of risks.

2. The obliged entity evaluates both the inherent and residual risk associated with the transaction. Inherent risk refers to the level of risk before the obliged entity carries preventive measures, while residual risk refers to the level of risk taken because of such measures. In the process of risk assessment, the obliged entity should consider the risk factors associated with the transaction, including the identity of the client, the geographic area they operate in the product/service requested and delivery channels.

3. Where possible, information about these money laundering and terrorism financing risk factors should come from a variety of sources. Obliged entity should determine the type and numbers of sources on a risk-sensitive basis.

4. When assessing the risk, the obliged entity should consider the following sources of information:

a) Money Laundering and Terrorism Financing National Risk Assessment Report and Action Plan;

b) Methodological guidelines/recommendations developed by the supervisory body and the results of the inspection conducted by the same body;

c) Information provided by the Financial Monitoring Service, state executive bodies, and/or law enforcement agencies (reports, alerts typologies, guidelines, methodological documents, etc.);

d) Standards/recommendations developed by competent international organizations, typological studies, and reports;

e) Information obtained as part of the initial CDD process;

f) Information from the civil sector, such as the Corruption Perceptions Index, the Global Terrorism Index, etc.;iInformation from civil society, such as corruption indices and global terrorism index;

g) Money laundering and terrorism financing mutual evaluation reports;

h) Reliable and credible international business bases (World-check, Name Scan, Thomson Reuters, etc.)

i) In the case of legal entities – audit reports;

j) Information from the reliable and reputable media outlets;

k) Analytical studies provided by relevant research organizations;

l) Scientific publications.

5. Money laundering and terrorism financing risk-factors

1. The money laundering and terrorism financing risk factors specified in this guideline are not exhaustive and the obliged entity may take other circumstances into account when identifying the risks.

2. The presence of any particular risk factor does not indicate the final level of risk for the client. As a rule, this is done through reconciliation of the CDD measures carried out by the obliged entity and all the identified risk factors. The obliged entity must assess the risk factors defined in each particular case, including the identity of the client and the beneficial owner, the geographic area of operation, the insurance products requested, delivery channels, etc.

6. Risk factors related to the geographical area

1. In determining geographic risk, the obliged entity should consider risk factors related to the jurisdictions in which the customer and beneficial owner are based (beneficial owner, life insurance beneficiary, pension scheme participant), country/region to which the above-mentioned persons have relevant business or personal links.

2. High-risk factors:

a) High-risk jurisdictions;

b) The country is identified by competent international organizations as a sponsor of terrorism and/or terrorist organizations are operating within this country;

c) Sanctions, embargoes, and/or other similar measures have been imposed on the country by relevant international organizations (including the UN Security Council);

d) The country does not have an adequate legal framework to facilitate the prevention of money laundering and terrorism financing, and this fact is recognized by the relevant international organizations;

e) The level of corruption and/or organized crime in the country is high and this fact is recognized by relevant international organizations;

f) Insurance premium is paid through financial institutions located in a high-risk jurisdiction;

g) The third party/intermediary is registered or operates in a high-risk jurisdiction.

3. Low-risk factors:

a) The country has an adequate legal framework to facilitate the prevention of money laundering and terrorism financing, and this fact is recognized by the relevant international organizations;

b) The level of corruption and/or organized crime in the country is low and this fact is recognized by relevant international organizations.

7. Client-related risk factors

1. To determine the risk level of a client, it is necessary to consider risk factors related to the business or professional activities, reputation, nature, and behavior of the client (its beneficial owner, life insurance beneficiary, participant in the pension scheme).

2. It is internationally recognized that the following risk factors indicate a high-risk level for the client:

a) A client whose organizational structure is so complex that it is impossible to identify the actual beneficial owner and the person exercising control;

b) A client who regularly makes suspicious and unusual transactions (operations);

c) A client who requests an unusually high level of confidentiality;

d) A client who refuses to deliver/provide information about their beneficial owner;

e) A client whose profession or activities are known to be very cash intensive cash services (currency exchange, money transfers), casino, gambling , etc.

f) A client whose business is linked to precious metals, precious stones, and their products, the sale and purchase of real estate and antiques;

g) The transaction (operation) of the client does not correspond to the declared activity; the nature of financial transactions changes dramatically and does not correspond to the usual activities of the client;

h) A client who avoids or delays the submission of standard information;

i) Charity funds or other non-profit organizations that are not subject to state supervision;

j) A client who carries out monetary transactions with a high-risk financial institution(s);

k) Client is a legal entity with nominee shareholders and/or shares in bearer form.

l) Politically exposed persons;

m) High wealth individuals;

n) Negative media reports/assessments about the client (their beneficial owner, life insurance beneficiary, pension scheme participant) (for example, allegations of terrorism or other criminal/illegal activities). In this case, the obliged entity must take into account the degree of reliability of the information and the independence of the source;

o) Any other circumstances that cast doubt in relation to the risk of the client (for example, questionable identity documents, the person's reputation, or his/her previous activities).

3. The following risk factors indicate a low risk level for the client:

   a) Obliged entity that is subject to state supervision in facilitating the prevention of money laundering and terrorism financing in Georgia or in the countries that are not considered high-risk jurisdictions;

   b) Companies listed on a stock exchange determined by the order of the President of the National Bank of Georgia;

   c) Public administrations or public enterprises of Georgia and other low risk countries.

8. Product-related risk factors

1. In identifying product-related risks, the obliged entity should consider the risk factors associated with product complexity and volume.

2. The obliged entity must evaluate its product/service individually, with consideration of the identity of the clients and the nature of the business relationship with them.

3. High-risk insurance products include investment-linked life insurance (including savings and repayable life insurance), and pension schemes.

4. The risk of these high-risk products is further increased when the following factors are present:

   a) Flexibility of the insurance/pension payments system when the payment can be made by an anonymous person(s);

   b) Possibility to pay a large or unlimited amount of insurance premium/pension contributions or additional amounts;

   c) Payments in cash;

   d) Possibility to withdraw the accumulated amount at any time without restrictions, without imposing a fine/penalty or imposing an unusually low fine/penalty;

   e) The product may be used as collateral;

5. The following circumstances are considered low risk factors for the above products:

   a) Transfer of the product in favor of another person is not allowed;

   b) Amount of total investment is limited;

   c) Small insurance premiums/pension contributions;

   d) Only small amounts of regular payments are allowed, no overpayments.;

   e)Corporate insurance policies/pension schemes, when the insurance premium/pension contribution is paid regularly, from the client's salary account;

   f) Insurance policy cannot be terminated in the short or medium term;

   g) It is not allowed to use the product as collateral;

   h) Payments in cash are not allowed.

9. Introducing new technology, product, service, or delivery channels

1. Before introducing new technology (including developing technologies), product, service, delivery channels, or other significant changes in business practices, the obliged entity must assess the money laundering and terrorism financing risks associated with such changes.

2. Above-mentioned process should include assessing the risks associated with the new product, service, supply channel, determining the necessary control measures, risk management processes, risk mitigation measures, and assessing the residual risk level. All relevant structural units of the organization (at least, the person responsible for the operation of the compliance control system,

internal audit, legal service, information technology service, etc.) should be involved in the process of approving the new product.

3. The obliged entity must make sure that there are appropriate business process, infrastructure, and resources available to manage the money laundering and terrorism financing risks arising from the introduction of a new product, and only then introduce it into business practice. It is also important to review/reassess the level of risk in case any features of the product are changed.

10. Risk factors related to delivery channel

1. The risk of product delivery is associated with certain forms of business relations with the client when it is difficult to identify the parties involved in transaction.

2. High-risk circumstances:

   a) Delivery of the product through remote channels without using EDS or electronic databases of the LEPL "Agency for the Development of Public Services";

   b) Delivery of the product through several intermediaries/third parties;

   c)Unusual circumstances of using Intermediary/third party (for example, unreasonable geographical distance).

3. Low-risk circumstances:

   a) Establishing a business relationship with a third party/intermediary who applies CDD measures, is well known to the obliged entity and is subject to existing regulations and supervision in terms of prevention of money laundering and terrorism financing;

   b) Insurance product is delivered in the form of corporate insurance.

4. The risk of product delivery through a third party/intermediary is increased by the fact that in such a case it is almost impossible to reveal unusual behavior of the customer; Apart from that, the third party/intermediary may not be subject to anti-money laundering and anti-terrorism financing control (this particularly applies to international intermediaries).

5. Prior to establishing a business relationship, the obliged entity must review information on money laundering and terrorism financing risks in the jurisdiction of the third party/intermediary. It is prohibited for the obliged entity to rely on a third party/intermediary registered or operating in a high-risk jurisdiction. This prohibition does not apply when the obliged entity relies on a branch or subsidiary operating or registered in a high-risk jurisdiction or if it is a member of the same group, if the group-level compliance control system ensures effective management of money laundering and terrorism financing risks in a high-risk jurisdiction.

6. The obliged entity must assess the following circumstances:

   a) Whether the third party/intermediary is a member of the same financial group and how confident the obliged entity is of the adequacy of the compliance control system effective at the group level;

   b) If the third party/intermediary is not a member of the same financial group:

   b.a) Whether the third party/intermediary takes adequate CDD measures and stores information in accordance with the legislation on facilitating the prevention of money laundering and terrorism financing and with the recommendations of the Financial Action Task Force, and whether it is subject to effective state supervision;

   b.b) Whether the obliged entity will be able to obtain client identification/verification documents and other relevant documentation/information, including copies of these documents, from a third party/intermediary immediately upon request.

11. Risk assessment/weighing

1. At the stage of assessing the risks of money laundering and terrorism financing, the obliged entity must determine the level of risk for each identified risk category (geographical area, client, product/service, delivery, etc.): as low, medium, or high (although different variations of these levels are allowed). To this end, it evaluates all relevant risk factors for each category.

2. When weighting risk factors, firms should make an informed judgement about the relevance of different risk factors in the context of a business relationship, based on a joint analysis of the probability of occurrence of a particular risk and a possible outcome.

3. The obliged entity has the right to assign specific rates (scores) to risk factors depending on their significance, which should be based on a reasonable assessment.

4. When assigning specific rates (scores) to risk factors, the obliged entity must ensure that:

   a) Weighing shall not be unreasonably based on the assessment of only one factor;

   b) Economic or profit considerations of the obliged entity shall not affect the assessment of risks;

   c) Weighing will not lead to the circumstances when it will be impossible for any business relationship to be classified as high risk;

   d) Weighing will not lead to the breach of the requirements set in the current legislation on suppression the prevention of money laundering and terrorism financing;

   e) The assigned risk level shall be overcome, if necessary (such action should be properly substantiated).

5. If the obliged entity uses software purchased from an external provider to manage money laundering and terrorism financing risks (scoring, weighting, calculating final rates (scores) and categorizing of risk levels), the relevant personnel of the obliged entity must understand how the system works and how it combines risk factors to achieve an overall risk rate (score) and how the risk level is categorized to ensure the latter is accurate.

12. General principles of risk management

1. After identifying and analyzing the risks of money laundering and terrorism financing the obliged entity must apply the risk management strategy developed by the company and follow adequate policies and procedures to mitigate the assessed risks.

2. The obliged entity must implement policies and procedures that will enable them to effectively manage the identified risks and direct/reallocate their own resources to the relatively weak fields in terms of prevention of money laundering and terrorism financing.

3. Volume and complexity of control measures taken by the obliged entity at the risk management stage must correspond to the level of the assessed risks.

4. In the process of risk management, it is important to involve different structural divisions/units of the company, which have different competencies and responsibilities. At the same time, it is important that each employee understands their role in implementing the money laundering and terrorism financing risk management strategy.

5. The importance of the active participation of the management must be emphasized, since it is the management that determines the direction and goals of business activity and makes strategic decisions, on which the money laundering and terrorism financing risk management policy is ultimately based.

6. The management of the company should always be aware of the risks identified during the business and ensure the implementation of adequate control mechanisms (including the allocation of resources for appropriate software and staff training). The management should also be open to withdraw from business relationships with the clients about which it does not have adequate information or from offering them its products or services.

7. The effectiveness of the obliged entity in the process of assessing and managing the risks significantly depends on the professional expertise of employees. All employees should be aware of the legal and regulatory framework related to their activities, including anti-money laundering and anti-terrorist financing legislation. To this end, the obliged entity must ensure that appropriate training programs are arranged for the relevant personnel, bearing in mind the principle that each

employee should, within the limits of their competence, participate in the process of facilitating the detection of cases of money laundering and terrorism financing.

8. Risk-based approach allows the obliged entity to decide on the key issues, methods, and intensity of the employee training program itself. As a result of this program, employees should be able to identify and analyze the risk of money laundering pertaining to the clients, their transactions/business, or products.

9. The Management of the company should continuously monitor the effectiveness and adequacy of risk management mechanisms in relation to the assessed risks. To ensure this feature of the risk management system, the obliged entity must constantly monitor the risks of money laundering and terrorism financing and update the information (periodically/as necessary). This may include:

   -Compliance control – to ensure that the essential systems are implemented;

   -Examination of performance – to ensure that the employees are following the company procedures;

   -Independent audit – to ensure that the policy and practice meet the standards.

13. Risk profile update and ongoing monitoring

1. Assigning a risk level to a client is a dynamic process that may require periodic review and reassessment of the level of risk assigned during the business relationship.

2. The most important component of the money laundering and terrorism financing risk management system is ongoing monitoring, the purpose of which is to:

   a) Receive up-to-date information about the purpose and intended nature of the business relationship of the client (and their beneficial owner) and keep records;

   b) Re-assess the risk level of the client in accordance with the latest transactions and the updated information;

   c) Determine the relevance of the insurance products purchased by the clients with the obliged entity's knowledge of the clients and their risk profile;

   d) Identify suspicious and unusual transactions and report to the Financial Monitoring Service of Georgia.

3. Ongoing monitoring is carried out regardless of the risk level assigned to the client, although its frequency depends on the client's risk profile. Hence, to ensure the effectiveness of ongoing monitoring, client-related information (identification data, field of activities, ownership structure,

products purchased, etc.) should be reviewed regularly and changes to the information and risk assessment should be done upon necessity.

4. The obliged entity, in accordance with its own risk management policy, determines the frequency of reviewing the risk level and re-implementing CDD measures, which can be determined on risk sensitive basis as follows:

   a) High risk - annually and/or at the renewal of insurance policy/agreement;

   b) Medium risk – every 2-3 years;

   c) Low risk – every 4-5 years;

5. The obliged entity will document and keep records of client risk assessment measures/actions to substantiate the results of the assessment, if necessary.

6. Establishing business relationship with a client is prohibited if the obliged entity has not carried CDD measures, and/or determined the purpose and intended nature of the business relationship, and/or is not confident in the effective management of risks. And if a business relationship already exists in such conditions, the obliged entity should terminate or suspend the service.