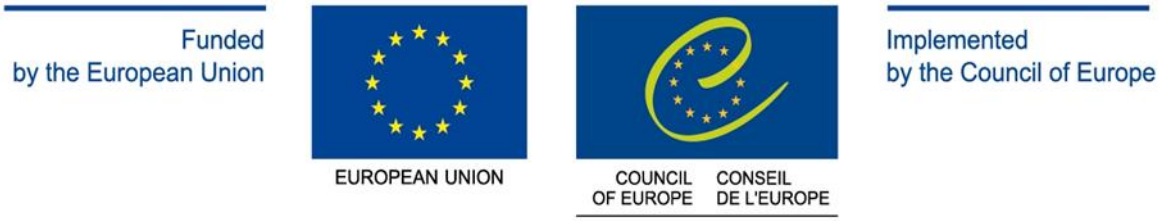


Project against Money Laundering and Terrorist Financing in Serbia

MOLI Serbia

DGI(2013) 6 June 2013

Technical Paper:

Risk Assessment Guidance

Prepared by Council of Europe expert Ms Maud Bokkerink

ECCU-MOLI SERBIA-TP13-2013

June 2013

TABLE OF CONTENTS

This risk assessment guidance paper is intended to assist the obligors under the Serbian AML/CFT law to make an enterprise-wide risk assessment to identify and assess their money laundering and terrorism financing risks for customers, countries or geographic areas, products, services, transactions and delivery channels. It describes in general money laundering and terrorism financing processes, the elements of an adequate system of ML/TF risk management, and the stages of an ML/TF risk assessment.

The supervisory authorities are advised to adapt this guidance paper to their supervised sectors by adding examples that are specific for the ML/TF risks in

RISK ASSESSMENT GUIDANCE

1 INTRODUCTION

Recommendation 1 of the 2012 Financial Action Task Force (FATF) 40 Recommendations and its Interpretive Note require supervisors, financial institutions or designated non-financial businesses and professions to apply some of the FATF Recommendations in a risk-based manner. In order to apply a risk-based manner to the anti-money laundering and combatting the financing of terrorism (AML/CFT) requirements, supervisors and obliged entities should first understand the money laundering and terrorism financing (ML/TF) risks of their business by identifying and assessing possible risks. A risk assessment is a first step an obliged entity should take before developing AML/CFT control measures to ensure that these measures will be appropriate to the nature and size of the business.

Obliged entities should take appropriate steps to identify and assess their money laundering and terrorism financing risks for customers, countries or geographic areas, products, services, transactions and delivery channels. They should document those assessments in writing and keep these assessments up to date. The nature and extent of the ML/TF risk assessment should be appropriate to the nature and size of the business. Obliged entities should always understand their money laundering and terrorism financing risks, but the supervisory agencies may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

Based on the risk assessment obliged entities should have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified. The term 'mitigate' in this context means reducing the seriousness or extent of ML/TF risks. They should monitor the implementation of those controls and enhance them, if necessary. When assessing risk, obliged entities should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. Obliged entities may differentiate the extent of measures, depending on the type and level of risk for the various risk factors.

The objective of this document is to provide guidance for obliged entities on how to perform an overall ML/TF risk assessment with respect to their business operations and which factors can be taken into account. This guidance document applies to all obliged entities referred to in Article 4 of the Law on the Prevention of Money Laundering and Terrorism Financing of the Republic of Serbia ("Official Gazette of RS", No. 20/2009).

This guidance document addresses the following topics:

- ML/TF risks faced by financial institutions and DNFBPs;
- ML/TF risk assessments methodology for business operations;
- ML/TF risk control policies and procedures.

2 MONEY LAUNDERING AND TERRORISM FINANCING

Money laundering and terrorism financing are global issues that can affect the economic, political, security and social structures of a country. The consequences of money laundering and terrorism financing are undermining the stability, transparency and efficiency of a country's financial system, economic disruptions and instability, jeopardising reform programmes, decrease of investment, tarnishing a country's reputation and threatening national security.

ML/TF risks arise also from failure to implement the Law on the Prevention of Money Laundering and Terrorism Financing and related regulations. Failure to regulate money laundering and terrorism financing risk may result in an obliged entity being significantly exposed to reputational risk and the risk of sanctions imposed by a regulatory body.

2.1 DEFINITION OF MONEY LAUNDERING

Money laundering refers to all activities of criminals to conceal and disguise the origin of proceeds generated from criminal activities, in order to create the impression that these were generated in a legal manner. Money laundering allows criminals to use their illegally gained funds without raising a suspicion. The Law on the Prevention of Money Laundering and Terrorism Financing stipulates that money laundering is:

1) Conversion or transfer of assets acquired through the commission of a criminal offence;
2) Concealment or misrepresentation of the true nature, source, location, movement, disposition, ownership of or rights with respect to the assets acquired through the commission of a criminal offence;
3) Acquisition, possession, or use of assets acquired through the commission of a criminal offence.

Money laundering encompasses a wide range of activities that may be involved in disguising the origin of proceeds of crime. The money laundering process may involve a series of transactions conducted in both the informal and formal sectors whereby the proceeds of crime are the input, and assets with an aura of legitimacy are the output. Any provider of a product or service that can be used to store or transfer value can itself be abused as an instrumentality in the laundering process. Money laundering is possible through businesses in the financial sector and businesses operating outside of the financial sector.

2.1.1 Three stages of money laundering

Money laundering is usually described as a three-stage process aimed at concealing the origin of criminal proceeds.

- Placement
- Layering
- Integration

In the initial placement stage proceeds generated from crime are placed into the financial system, for instance by depositing cash into an account. Large cash amounts

are broken up to appear less suspicious and deposited over a certain period of time into the accounts at various financial institutions. Furthermore, illegally gained funds can be invested in securities, insurance contracts, etc. Criminal money can also be mingled with regular operating income or as income from dummy or phantom companies, which actually do no business, but only serve for depositing cash into accounts.

In the second layering stage the funds are transferred from the account into which they were deposited to other accounts in series of transactions to the accounts at different institutions world-wide. Many of these transactions make no economic sense, and they remain unaccounted for in business operations. The main objective of these transactions is to hide the connection between the funds and the criminal activity from which they were generated. The purpose of these transactions is to disguise the money trail and obstruct those trying to investigate the origin of the money.

In the third integration stage the funds are invested in legal business operations, works of art, shares, real estate property, luxury goods. It is very difficult to make a distinction between legal and illegal funds in this stage.

A key step in the money laundering process involves combining proceeds of crime with legitimate business monies to obscure the source of funds. Funds re-enter legal economic flows, by being placed into business operations or otherwise invested, after which they appear as 'legal' money generated from legitimate business activities. Another way is to revive a company facing difficulties by investing large amounts of money in it, after which the company continues with its normal business activity using criminal money, while the money launderers receive dividends and salaries as legal sources of income.

These three stages will not always take place sequentially as sometimes criminals will directly invest their illegally gained funds in luxury goods or real estate. Also, with some crimes, such as investment fraud, the criminal funds will already be in the financial system and as such there is no need any more to place them in the system. Additionally, before illegal money will be placed in the financial systems, the money often also will just be moved, either physically by mail or through couriers, or through money transfer systems.

2.2 DEFINITION OF TERRORISM FINANCING

Terrorism financing is a specific form of financial crime. Essentially, it includes raising, collecting or providing funds to finance terrorism, a terrorist act or terrorist organisation. The basic objective of individuals and organisations involved in terrorism financing is not necessarily to disguise the sources of funds, but primarily to conceal the nature of activity for which the funds are intended. Terrorists use a variety of methods to transfer money for the needs of their organisations and activities, including the financial sector, cash transfers, trade, donations and charity organisations, as well as (informal) money transfer systems.

Funds intended for terrorist organisations and activities may originate from legal sources, such as donations, charity organisations, profit generated from regular business activity, as well as from illegal sources, such as drug trafficking, arms trafficking, gold and diamond smuggling, fraud, kidnapping and extortion.

The Law on the Prevention of Money Laundering and Terrorism Financing stipulates that terrorism financing means the providing or collecting assets, or an attempt to do so, with the intention of using them, or in the knowledge that they may be used, in full or in part:

1) in order to carry out a terrorist act;

2) by terrorists;
3) by terrorist organisations.

For the purpose of the Law, financing of terrorism means inciting and aiding in the provision or collection of assets, regardless of whether a terrorist act was committed or whether the assets were used for the commission of a terrorist act.

2.2.1 Four stages of terrorism financing

There are four stages in the process of terrorism financing:

- Collecting funds from legal business operations or from criminal activities
- Keeping the collected funds
- Transferring the funds to terrorists
- Using the funds

The first stage includes the collection of funds from legal business operations of companies related to, or even led by terrorist organisations or individuals, or from criminal activities such as drug trafficking, kidnapping, extortion, fraud, etc. Donations by individuals supporting terrorist organisations' goals, and charity funds collecting money and channelling it towards terrorist organisations, are also a significant source of these funds.

In the second stage, the collected funds are kept in different manners, including accounts opened by intermediaries, individuals or companies.

The third stage includes the transfer of these funds to terrorist organisation units or individuals for operational use. In this stage, it is typical to use transfer mechanisms, such as international electronic transfers between banks or payees, charity organisations, (informal) money transfer systems or networks. Money can also be transferred via courier and by cross-border smuggling.

The last stage is the use of funds. The criminal intent of these funds becomes manifest when they are used for the activities of terrorist organisations, such as purchasing explosives, arms, telecommunications equipment, supporting regular cell activities, providing hiding places and medical care, financing training camps, propaganda, or political support and refuge.

Reporting entities are not responsible for establishing the commission of a criminal offence or for establishing the intention of terrorist activities; their role is to report suspicious activities, while the Administration for the Prevention of Money Laundering (APML) and investigative bodies should further investigate the case, establishing if there is any connection with terrorism.

2.3 LINK BETWEEN MONEY LAUNDERING AND TERRORISM FINANCING

The techniques and methods used for money laundering and for terrorism financing are similar, but at the same time, there are significant differences between them. In the case of money laundering, the initial funds are always the result of illegal activities, while in the case of terrorism financing the funds may originate from both illegal and legal activities. Terrorists use the same techniques and go through the same stages characteristic of money laundering in order to disguise the identity of their financiers. However, the main objective of persons involved in terrorism financing is not necessarily concealing the source of funds, but disguising the nature of the financed activity. And when terrorists withdraw funds from legal sources, detection and monitoring becomes even more difficult. Financial transactions connected with a

terrorist act mostly involve lower values than those in the case of money laundering; however, the financing of a terrorist organisation can involve large amount.

An efficient system against money laundering and terrorism financing must cover both risks: it must prevent, detect and sanction both the placement of illegal funds into the legal financial system, and the provision of terrorists and terrorist organisations with financial means needed for their activities.

3 MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

FATF Recommendation 1 and its Interpretative Note (paragraph 8) require that obliged entities conduct a business related risk assessment which should include risks related to customers; countries or geographical locations; products and services; transactions and delivery channels. In order for obliged entities to fulfil their obligations under AML/CFT legislation and to implement the FATF Recommendations, they should take measures to execute a money laundering and financing of terrorism risk assessment. A risk assessment enables the entity to focus its AML/CFT efforts and to adopt appropriate measures to optimally allocate the available resources.

The legal basis for implementing actions and measures for the prevention of money laundering and terrorism financing is the Law on the Prevention of Money Laundering and Terrorism Financing. Under Article 7 of the Law, the institution is obliged to draw up an assessment of money laundering and terrorism financing risk in accordance with the guidelines adopted by the supervisory authority. The risk assessment should be done for each group or type of customers, business relationships, product or services offered by the obliged entity within its business.

Each institution, regardless of its size and complexity, is expected to develop an adequate risk management system for money laundering and terrorism financing. This risk management system is to ensure that the ML/TF risks should be continuously and comprehensively identified, assessed, monitored, managed and mitigated.

An adequate system of money laundering and terrorism financing risk management should include:

- A risk assessment of money laundering and terrorism financing risks of the business;
- Policies and procedures to control money laundering and terrorism financing risks;
- An organisational structure to execute these risk management controls; and
- A process to systematically check and assess the adequacy of the control systems.

3.1 RISK ASSESSMENT OF THE BUSINESS

Risk is a function of the likelihood of occurrence of risk events and the impact of risk events. The likelihood of occurrence is a combination of threat and vulnerability, or in other words, risk events occur when a threat exploits vulnerability. Accordingly, the level of risk can be mitigated by reducing the size of the threats, vulnerabilities, or their impact.

In order to establish the obliged entity's exposure to ML/TF and the efficient management of that risk, the entity needs to identify every segment of its business operations where a ML/TF threat may emerge and to assess its vulnerability to that threat. It is necessary that ML/TF risks are continually identified at all management levels - from the operational level to the Executive Board - , and to include all organisational units of the entity. The size and complexity of a business plays an important role in how attractive or susceptible it is for ML/TF. For example, a large organisation is less likely to know a customer personally who thereby can be more anonymous than a customer of a small organisation. And an organisation that provides international services might be more attractive to a money launderer than a domestic organisation.

Upon identifying the risks, the entity needs to adequately assess the money laundering and terrorism financing risk exposure, which would enable it to evaluate the likelihood of adverse effects arising from that risk and the potential impact of that risk on the realisation of business objectives.

The risk identification and analysis needs to be conducted for all existing and new products, activities and processes. An effective process of ML/TF risk identification and analysis serves as a basis for establishing an adequate system of risk management and control, and, consequently, for reaching the ultimate goal – minimising possible adverse effects arising from that risk.

A risk assessment of money laundering and terrorism financing risks proceeds from the assumption that different products and services offered by obliged entities in their business operations, or different transactions executed by them, are not equally vulnerable to misuse by criminals. The purpose of a risk assessment is to apply control measures proportionate to the identified risk. This allows obliged entities to focus on the customers, countries, products, services, transactions and delivery channels that constitute the greatest potential risk.

The process of an ML/TF risk assessment has four stages:

1) identifying the areas of the business operations susceptible to ML/TF;
2) conducting an analysis in order to assess the likelihood and impact of ML/TF;
3) managing the risks; and
4) monitoring and reviewing the risks.

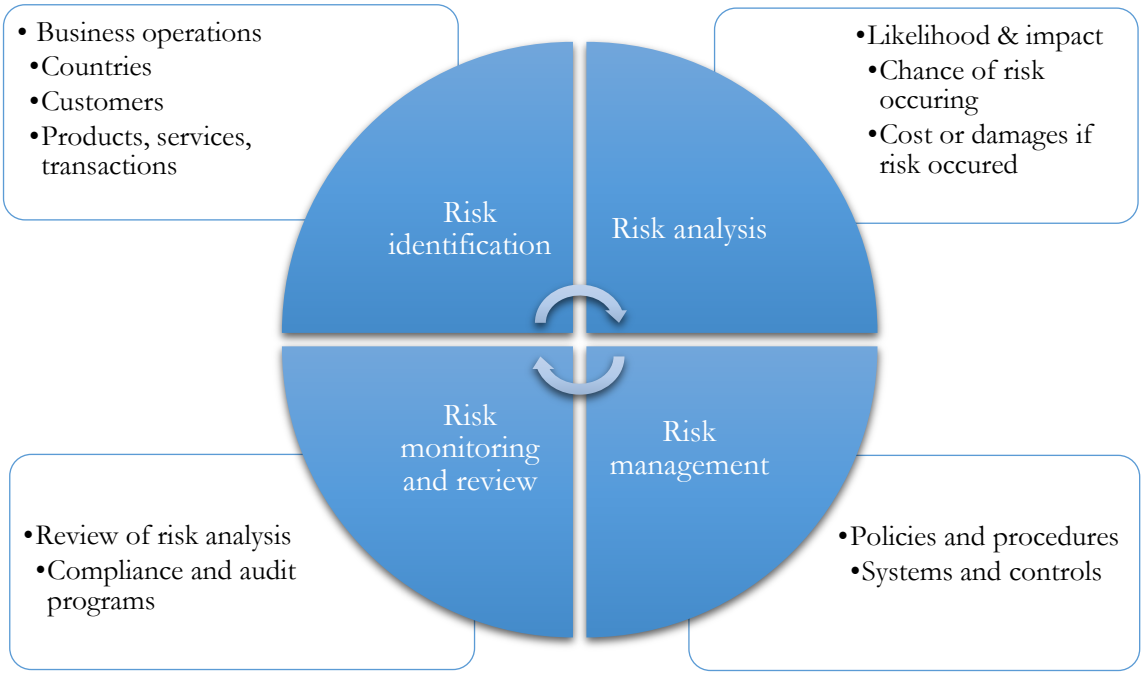
The first stage of the risk assessment is to identify customers, products, services, transactions, and geographical locations specific for the obliged entity. Depending on specific characteristics of and delivery channels for certain customers, products, services and transactions, the threat of and vulnerability to money laundering and terrorism financing varies.

In the second stage, the ML/TF risks that can be encountered in an entity need to be analysed as a combination of likelihood that the risk will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss to the business from the crime or from fines from the authorities. It can also consist of reputational damages to the business or to the whole sector. The analysis of certain risk categories and their combinations is specific for each entity, so that the conclusion on the total risk level must be based on all relevant information.

In the third stage, the entity will, based on the analysis, apply risk management strategies and implement policies and procedures accordingly. To effectively mitigate the risk adequate systems and controls will be implemented.

Finally, in this process the risks and the management of the risks have to be monitored and reviewed. An obliged entity can do this by developing a monitoring regime through its compliance and audit programs. The assessment of money laundering and terrorism financing risks must be revised periodically, based on the extent risks have changed or the obliged entities operations or strategies have changed.

RISK ASSESSMENT METHOD



In view of the fact that the nature of terrorism financing differs from that of money laundering, the risk assessment must include also an analysis of the vulnerabilities of terrorism financing. Since the funds used for terrorism financing may stem from legal sources, the nature of sources may vary. When the sources of terrorism financing originate from criminal activities, the risk assessment related to money laundering are also applicable to terrorism financing risk assessment.

3.2 RISK IDENTIFICATION

The first step in assessing ML/TF risks is to identify certain risk categories, i.e., customers, countries or geographical locations, products, services, transactions and delivery channels specific for the obliged entity. Depending on the specificity of operations of an obliged entity, other categories could be considered in order to identify all segments in which money laundering and terrorism financing risk may emerge. The significance of different risk categories may vary from institution to institution, i.e. the institution may decide that some risk categories are more important to it than others.

3.2.1 Country or geographical risk

Country or geographical risk may arise because of the location of a customer, the origin of destination of transactions of the customer, but also because of the own business activities of an obliged entity, its location and the location of its organisational units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to money laundering and terrorism financing.

There is no general definition based on which particular countries or geographical areas can be categorised as low or high risk. The factors which may define if a specific country or geographical area is more vulnerable to money laundering and terrorism financing, may include different criteria. Factors that may indicate a higher risk are:

- Countries or geographic areas subject to sanctions, embargoes or comparable measures issued, for instance, by the United Nations, the European Union or the United States.
- Countries or geographic areas identified by credible sources (e.g. the FATF, the IMF or the World Bank) as lacking an appropriate system of preventing money laundering and/or terrorism financing. Reference is made to the so-termed 'ICRG process' (International Co-operation Review Group) of the FATF. After each of its meetings (held in February, June and October) the FATF publishes lists of countries which in its opinion lack an adequate system of combating money laundering and terrorism financing.
- Countries or geographic areas identified by credible sources as providing funding for or otherwise supporting terrorist activities.
- Countries or geographic areas identified by credible sources as having a high level of corruption, or other criminal activity.

In addition, the Minister of Finance, acting under the authority stipulated by the Law, should establish the list of states applying international standards in the field of money laundering and terrorism financing, which are, as a minimum, at the level of European Union standards (so-called white list), and the list of states not applying money laundering and terrorism financing standards (so-called blacklist).

3.2.2 Customer risk

For the purpose of the ML/TF risk assessment, the obliged entity should define if a type of customers carries an increased money laundering and terrorism financing risk. Based on its own criteria, an obliged entity will determine whether a customer poses a higher risk. Categories of customers who may indicate a higher risk are:

- Customers who conduct their business relationships or transactions (or who have these conducted) under unusual circumstances, such as an unexplained geographic distance between the entity and the location of the customer, frequent and unexplained transfers of accounts to different institutions and frequent and unexplained movements of funds between accounts in various geographic locations.
- Customers where the structure or characteristics of the entity or relationship make it difficult to identify the true owner or controlling interests, or customer that use nominees, trusts, family members or third parties, etc.
- Cash intensive businesses including (informal) money transfer agencies, bureaux de change, betting houses, gambling halls, etc.

- Charities and other 'not-for-profit' organisations (especially those operating on a 'cross-border' basis) which are not subject to any form of monitoring or supervision.
- Indirect relationships through intermediaries who are not (or not sufficiently) subject to AML/CFT measures or who are not supervised.
- Customers who are Politically Exposed Persons (PEPs).
- Occasional customers that do transactions above a certain threshold.

The delivery channels play a role when assessing the customer risk. The extent to which the obliged entity works with customers directly or through intermediaries or correspondent institutions, or establishes business relationships without customers being physically present are important factors to be considered in assessing the risk of a category of customers.

The obliged entity will describe all types or categories of customers that it provides business to and make an estimate of the likelihood that these types or categories of customers will misuse the entity for money laundering or terrorism financing. This likelihood is for instance high if it can occur several times per year, medium is if can occur once per year and low if it is unlikely, but not impossible. In assessing the impact, the entity can for instance look at the financial damages from the crimes itself or from regulatory sanctions; the reputational damage to the institution or the sector. The impact can vary from minor if there are only short term or low cost consequences to (very) major when there are very costly and long term consequences that affect the proper functioning of the institution.

EXAMPLE ONLY

Description of types of customers

SME business:

The SME business customers usually are domestic companies with simple ownership structure. Most of these businesses deal with cash and multiple persons can be acting on their behalf. The likelihood that funds deposited are from illegitimate source is medium. Because of the large number of SME customers in the institution the impact can be major. The risk assessment is high.

International corporations:

Customers that are international corporations have complex ownership structures with often foreign beneficial ownership. Although there are only few of those customers most are located in offshore locations. The likelihood of ML is high but because of the limited number of customer the impact will be moderate. The risk assessment is medium.

Etc., etc.

These descriptions can result in a table as below:

EXAMPLE ONLY

Type of customer	*Likelihood*	*Impact*	*Risk assessment*
Domestic retail customer	medium	moderate	medium
Private banking customer	high	major	high
SME business	high	major	high
International corporation	high	moderate	medium
Company listed on stock exchange	low	minor	low
PEP	high	major	high
Securities broker	low	high	medium
Incidental customer	high	medium	medium

Above risk analysis is a general one for a types or categories of customers. It is the starting point for the risk classification of an individual customer. Based on the circumstances of the individual customer, such as its background or information provide, the risk classification of the customer can be adjusted. Based on that individual risk classification customer due diligence measures will be applied.

3.2.3 Transaction, product and service risk

A comprehensive ML/TF risk assessment must take into account the potential risks arising from the transactions, products and services that the institution offers to its customers and the way these products and services are delivered to the customer. The institution should pay particular attention to money laundering and terrorism financing risk which may arise from the application of new technologies.

In identifying the risks of transactions, products, and services, the following factors could be considered:

- Services identified by internationally recognised and credible sources as being a higher-risk, such as international correspondent banking services and (international) private banking activities.
- Services involving banknotes and precious metal trading and delivery.
- Services that inherently promote anonymity or can readily cross international borders, such as online banking services, prepaid cards, private investment companies and trusts.
- New or innovative products or services that are not provided directly by the entity but are provided through channels of the entity.
- Products that involve large payment or receipt in cash.
- Purchase of valuable assets or commodities (real estate, race horses, vehicles, gems, precious metals, etc.)
- Gaming activities (horse racing, internet gambling, etc.)
- Non face-to-face transactions or services
- One-off transactions

Specific lease products, life insurance policies with a low annual premium or a low single premium, consumer loans or savings products have a low inherent risk because of the long term to realise benefits. Other products, such as back-to-back loans, trade finance, real estate transactions and other high-quality, complex products may produce a higher risk because of their complexity or lack of transparency.

For the risk assessment, the obliged entity will describe all products and services that it provides and make an estimate of the likelihood that customers will misuse that product for money laundering or the financing of terrorism, and the impact thereof in a similar way as for the customer.

EXAMPLE ONLY

Description of types of products, transactions and services

Life insurance

The life insurance products are simple and premiums tend to be very low. Premiums can only be paid through a bank account and no cash is involved. The life insurance products are only sold to Serbian resident persons. The likelihood that insurance products are used for ML/TF is low as will be the impact if it is. Risk assessment is low.

Prepaid cards

Prepaid cards are a new product of the institution and its usage is not clear yet. Funds tend to be loaded through cash deposits and it is not necessary to have a bank account. The likelihood that prepaid cards are used for ML/TF is high and the impact on the business, seeing that it is a new product, will be very high. Risk assessment is high.

Etc., etc.

This description can result in a table as below:

EXAMPLE ONLY

Type of transaction	***Likelihood***	***Impact***	***Risk assessment***
Betting transaction	high	moderate	medium
Online transactions	high	major	high
Domestic bank transfer	medium	moderate	medium
Prepaid card	high	major	high
Life insurance	low	minor	low
Securities account	low	minor	low
Postal package	medium	minor	low

3.3 RISK ANALYSIS – RISK MATRIX

In assessing the risk of money laundering and terrorism financing, the obliged entity is to establish whether all identified categories of risks pose a low, medium, high or unacceptable risk to the business operations. The institution must review different factors, e.g., number and scope of transactions, geographical location and nature of relationship with the customer. In doing so, the institution must also review the differences in the manner in which the institution establishes a business relationship with a customer (e.g., direct contact or non face-to-face). It is due to the combination of these factors and the variety of their combinations, that the level of money laundering and terrorism financing differs from institution to institution. The geographical risk should be seen in correlation with other risk factors in order to come up with an assessment of the total money laundering and terrorism financing risk. Thus, for example, a low risk product in combination with a customer from a high risk country will combined carry a higher risk.

Institutions can use a risk matrix as a method of assessing risk in order to identify the customers that are in the low-risk zone, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing. In classifying the risk, the obliged entity, taking into account its

specificities, may also define additional levels of money laundering and terrorism financing risk. The development of a risk matrix can include the consideration of a wide range of risk categories, such as the products and services offered by the entity, the customers to whom the products and services are offered, the institution's size and organisational structure, etc. A risk matrix is not static; it changes as the circumstances of the entity change. A risk assessment will assist an obliged entity to recognise that ML/TF risks may vary across customers, products and/or geographic areas and thereby focus its efforts on high-risk areas in its business.

The following is an example of a risk matrix that can be developed based on the risk analysis:

EXAMPLE ONLY

Transaction **Customer**	**Betting transaction**	**Online transaction**	**Domestic transfer**	**Prepaid card**	**Life insurance**	**Securities account**	**Postal package**
Domestic retail customer	medium	medium	medium	medium	low	low	medium
Private banking customer	n/a	high	medium	high	n/a	medium	n/a
SME business customer	High	high	medium	high	medium	medium	medium
International corporation	medium	high	medium	high	medium	medium	medium
Company listed on stock exchange	medium	medium	low	medium	low	low	low
PEP	High	high	medium	high	medium	medium	medium
Securities broker	n/a	medium	medium	n/a	n/a	medium	n/a
Incidental customer	medium	high	medium	high	n/a	n/a	medium

The institution must take care that this risk identification and analysis is properly documented in order to be able to demonstrate it as the basis of the AML/CFT policies and procedures, and to be able to provide the risk assessment information to the supervisory authorities.

3.4 RISK MANAGEMENT

The ML/TF risk of each obliged entity is specific and requires an adequate management approach, corresponding to the level and structure of the risk, and to the size of the entity. The objectives and principles of ML/TF risk management should enable entities to establish adequate policies and procedures, including customer due diligence rules, promoting high ethical and professional standards and preventing entities from being misused, intentionally or unintentionally, for criminal activities.

ML/TF financing risk management requires attention and participation of several business units with different competences and responsibilities. It is important for each business unit to precisely know its role, level of authority and responsibility within the entity's organisational structure and within the structure of ML/TF financing risk management.

It is desirable for managers of different lines of business, responsible for risk management at the level of their organisational unit, to develop ML/TF risk management procedures, corresponding to the specific tasks of the organisational unit in question, which must be harmonised with the objectives and principles of ML/TF risk at the level of the institution as a whole.

Management gives direction to its business activities by formulating objectives and making strategic choices from which subsequently policy principles are derived. Management should be able to determine the ML/TF risks of the business and take these into account in the entity's ultimate goals and strategies. Documentation and communication of strategy, policies and procedures are important for their actual implementation. Tools in this respect are, for instance, mission statements, business principles or strategic views. Management will also give direction to setting up, implementing and monitoring the ML/TF control framework and will be responsible for the strategic choices to be made and decisions to be taken in that respect.

Management should be actively involved in analysing and recognizing ML/TF risks and take adequate control measures (e.g., by allocating sufficient resources to setting up an adequate monitoring system or training). Management will thereby receive support from functions that possess relevant knowledge and experience (compliance function, security function, risk management function, commercial functions, etc.). Management should also guard against the obliged entity accepting customers or providing products and services on whom or which the entity has no knowledge or experience, and should ensure that sufficient account is taken of ML/TF risks in the development and pre-introduction phase of new products and services. It is important in this respect that members of the management team involved in the decision-making process have sufficient authority and powers to take and implement the necessary decisions (or have these implemented).

Management's leadership abilities in and commitment to the prevention of money laundering and terrorism financing are important aspects of implementing the risk-based approach. Management must encourage regulatory compliance and ensure that employees abide by internal procedures, policies, practices and processes aimed at risk mitigation and control. Management should also promote an ethical business culture and ethical behaviour. Ethical behaviour is a professional, individual responsibility, where individuals should be aware of the rights, interests and wishes of other stakeholders and conscientiously take them into account, have an open and transparent mind-set, and be willing to take responsibility and be held accountable for their decisions and actions. An ethical business culture denotes a climate and atmosphere in which an entity, also in a broader sense, behaves or acts in a way it can explain and account for. A culture in which this professional, individual responsibility is stimulated and rewarded, and which not only respects the letter of the law, but also its spirit. The elements underpinning this culture are: balancing of interests, balanced and consistent actions, openness to discussion, leading by example, feasibility, enforcement and transparency.

3.4.1 Policies and procedures

Once the identification and risk analysis processes are completed, the strategy of ML/TF risk management is applied to enable the obliged entity to implement adequate policies and procedures for reducing the risks and bringing it down to an acceptable level, with a view to avoiding reputational risks, operational risks, risks of sanctions imposed by a regulatory body and other forms of risk.

The policies and procedures are approved by management and are applicable to all business units, branches and majority-owned subsidiaries. They should allow for sharing of information between business units, branches and majority-owned subsidiaries, with adequate safeguards on confidentiality and use of information exchanged. By assessing the risks and developing policies and procedures the entity ensures the continuity of ML/TF risk management controls despite any changes in the management or staff composition or structure.

The policies and procedures should enable the obliged entity to effectively manage and mitigate the identified risks and focus its efforts on areas in its business which are more vulnerable to ML/TF misuse. The higher the risk, the more control measures have to be applied.

An obliged entity can implement adequate ML/TF risk controls for higher risk products by setting transaction limits and/or a management approval escalation process. Also, the development and application of risk categories for customers together with customer due diligence and transaction monitoring measures based on those risk categories may be one of the strategies for managing potential ML/TF risks posed by customers. Specific policies and procedures will therefore need to be developed with respect to customer due diligence, transaction monitoring, recordkeeping and reporting to the APML.

3.4.2 Training

It is necessary for the obliged entity to ensure that each employee understands his/her role in the process of ML/TF risk management, in order to provide for adequate risk detection and monitoring. Training programs for the employees who are in direct contact with customers or who execute transactions are therefore essential in the process of ML/TF risk management. Lack of human resources and inadequate training can be a limiting factor in this process. All the employees, from the operational level to top management, must be aware of ML/TF risks.

Under the provisions of the Law, the entity is obliged to ensure regular professional education, training and improvement of the employees who are in charge of detecting and preventing ML/TF. Professional education, training and improvement focus on ML/TF techniques, regulations governing this area, the entity's internal acts, including the list of indicators for recognising customers and transactions suspected of money laundering or terrorism financing.

The best way to ensure proper training is to develop an annual program of employee professional education, training and improvement. The entity must adapt the education program to the powers and responsibilities of the employees dealing with money laundering and terrorism financing, as well as to the needs of new employees, those who are in direct contact with customers or who execute transactions, or are responsible for supervising the implementation of the AML/CFT regulations and internal acts. The entity verifies the knowledge of its employees in this area at least once a year, and keeps the verification results for at least a year.

3.5 RISK MONITORING AND REVIEW

Management should be able to adequately manage ML/TF risks, to verify the level of implementation and functioning of the ML/TF risk controls, and to ascertain that the adopted risk management measures correspond to the entity's risk assessment. The entity should therefore establish an appropriate and continuing process for ML/TF risk monitoring and review. This process will be done by the business control function to

ensure on a regular basis that all processes are implemented; the compliance function that periodically monitors if the policies are adhered to and systems are in place; and the audit function that assesses if the policies and process are conform the Law and are performed in an adequate way.

3.5.1 Monitoring process

Regular reports to management should contain the results of the monitoring process, findings of internal controls, reports of organisational units in charge of compliance and risk management, reports of internal auditing, reports of the person authorised for detecting, monitoring and reporting any suspicious transactions to the APML, as well as the findings contained in the supervisory authorities onsite inspection reports on AML/CFT. Management should be furnished with all important information which will enable it to verify the level money laundering and terrorism financing controls, as well as possible consequences for the institution's business if controls are not functioning properly.

The risk reports should indicate if appropriate control measures are established and adequate and fully implemented for the entity to protect itself from possible ML/TF misuse.

The monitoring and review process should include the appraisal of ML/TF risk exposure for all customers, products and activities, and ensure the implementation of proper control systems, with a view to identifying and indicating problems before any negative consequences for the entity's business occur. This process may also alert the entity to any potential failures, for instance failure to include mandatory legislative components in the policies and procedures, insufficient or inappropriate customer due diligence, or level of risk awareness not aligned with potential exposure to ML/TF risks.

3.5.2 Compliance officer

The institution may have a special organisational unit for ML/TF risk management: the compliance officer. The compliance officer is appointed at management level. The compliance officer has an important task in setting up the risk assessment process and in monitoring and reviewing process. The compliance officer should have the following tasks:

- Development of AML/CFT policies and procedures;
- Coordination of ML/TF risk management activities;
- Training and advising of business units concerning issues related to ML/TF risks;
- Monitoring the implementation of the AML/CFT policies and procedures;
- If necessary, ensure adequate control of the customers, transactions and products more vulnerable to risk;
- Submission of reports to management.

3.5.3 Audit

In addition to the continuing process for ML/TF risk monitoring and review, the obliged entity should also have an internal audit to assess the system of ML/TF risk management in an independent manner. Management should ensure that the scope of internal audits are conform the level of ML/TF risk to which the entity is exposed. The independent verification can be conducted by internal auditors, external auditors, expert consultants or other qualified persons not directly involved in the implementation or functioning of the entity's ML/TF risk management.

3.5.4 Review of the ML/TF risk assessment

The obliged entity must keep the ML/TF risk assessment up to date by setting up and describing the process of periodically reviewing the risk assessment. The entity must therefore also stay up-to-date with ML/TF methods and trends, international developments in the area of AML/CFT, and domestic legislation. Such a review can also include an assessment of the risk management resources such as funding and staff allocation and may also identify any future needs relevant to the nature, size and complexity of the reporting entity's business.

A review should also be conducted when the business strategy or risk appetite of an entity changes or when deficiencies in the effectiveness are detected. When the entity is to introduce a new product or activity, an ML/TF risk assessment of that product is to be conducted before offering that new product or activity to customers.