Funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Project against Money Laundering and Terrorist Financing in Serbia

MOLI Serbia

DGI(2013) 12 June 2013

TECHNICAL PAPER:
Proposal to amend existing sectorial guidelines for obliged institutions to include and/or extend provisions on the risk-based approach

Prepared by Council of Europe Expert Ms Maud Bokkerink

ECCU-MOLI SERBIA-TP14-2013

June 2013

Table of Contents

1. Introduction

The FATF Recommendations on anti-money laundering and combating the financing of terrorism (AML/CFT) set out essential requirements that countries have to have in place to apply preventive measures for the financial sector and other designated sectors. The FATF requirements for preventive measures include among others:

- Assessing risk & applying a risk based approach
- Customer due diligence (CDD), including enhanced due diligence (EDD) and simplified due diligence (SDD)
- Reliance on third parties
- Internal controls, including appointment of compliance officer and training
- Foreign branches and subsidiaries
- Record keeping
- Reporting of suspicious transactions

The FATF Recommendations are implemented in the Law on the Prevention of Money Laundering and the Financing of Terrorism.[1] To allow obliged entities to implement the Law in a risk-based manner, the supervisory authorities will need to provide guidance on the various approaches obligors can adopt to implement the requirements of the Law. The supervisory authorities have already issued guidelines for most obliged entities. Only the AML/CFT guidelines of the Securities Commission (SC) and the Foreign Currency Inspectorate address most of the topics above, however, other guidelines need to be enhanced.

This Technical Paper contains proposals to amend existing sectoral guidelines for obliged institutions to include and/or extend provisions on the risk-based approach, and recommendations to harmonize the guidelines where two or more regulators hold responsibility for the same sector.

2. Existing guidelines for obligors

Based on the Law on the Prevention of Money Laundering and the Financing of Terrorism, the supervisors have already issued guidelines for several of the requirements in the Law. However, the level of detail and topics addressed varies. Annex 1 provides an analysis of the topics addressed in existing AML/CFT guidelines and the extent to which they are addressed. The analysis shows that the guidelines of the SC and the Foreign Currency Inspectorate address most of the AML/CFT requirements. However, other guidelines need to be elaborated with guidance on AML/CFT requirements that are now not yet included, such as CDD measures on beneficial owners, politically-exposed persons (PEPs), monitoring of transactions, introduction by third parties, suspicious transaction reporting, internal controls, training, and compliance.

The table below provides an overview of topics that are currently in the guidelines for obligors and topics that need to be added or enhanced.

[1] For an overview of the FATF Recommendations that are implemented in the AML/CFT Law see "TECHNICAL PAPER: Expert opinion on various AML/CFT laws, bylaws, regulations and guidance papers in the Republic of Serbia and the Proposal of concrete recommendations to bring the laws, bylaws and guidance into conformity with the relevant international standards in the area of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT), in particular with the 40 recommendations under the FATF Standards of February 2012."

Supervisor	Title of guideline for obligors	AML/CFT sections currently in guideline	AML/CFT sections that need to be added or enhanced
Securities Commission (SC)	Guidelines on the Application of the Law on Prevention of Money Laundering and Financing of Terrorism for Persons Supervised by the Securities Commission	○ risk analysis & management ○ CDD, SDD, EDD ○ monitoring ○ reporting and STR indicators ○ compliance officer ○ training ○ internal controls ○ record keeping ○ data protection	○ beneficial owner ○ branches
Foreign Currency Inspectorate	Guidelines for Obligors Providing Factoring and Forfeiting Services and Guidelines for Obligors Providing Money Transfer Services	○ risk analysis & management ○ CDD ○ monitoring ○ reporting and STR indicators ○ compliance officer ○ training ○ internal controls ○ record keeping ○ data protection ○ branches	○ beneficial owner ○ EDD ○ SDD ○ PEP
National Bank of Serbia (NBS)	Decision on the Guidelines for Assessing the Risk of Money Laundering and Terrorism Financing	○ risk analysis & management ○ CDD, EDD (PEP) ○ Training	○ SDD ○ EDD ○ beneficial owner ○ monitoring ○ reporting and STR indicators ○ compliance officer ○ internal controls ○ training ○ record keeping ○ data protection ○ branches
National Bank of Serbia (NBS)	Decision of Minimal Content of the "Know Your Client" Procedure	Requires setting up procedures regarding CDD, monitoring, risk management, training	
Minister of Trade and Telecommunications	Guidelines for Postal Service Providers	○ risk analysis ○ CDD, EDD ○ Training	○ SDD, EDD ○ beneficial owner ○ monitoring ○ reporting and STR indicators ○ compliance officer

			○ internal controls ○ record keeping ○ data protection ○ branches
Minister of Trade and Telecommunications	Guidelines for Real Estate Agents	○ risk analysis ○ CDD, EDD ○ training ○ internal controls	○ SDD, EDD ○ beneficial owner ○ monitoring ○ reporting and STR indicators ○ compliance officer ○ record keeping ○ data protection ○ branches
Administration for the Prevention of Money Laundering (APML)	Guidelines for Accountants and Auditors	○ risk analysis ○ CDD, EDD, SDD ○ reporting and STR indicators	○ SDD, EDD ○ beneficial owner ○ monitoring ○ compliance officer ○ internal controls ○ training ○ record keeping ○ data protection ○ branches

3. Recommended amendments to the guidelines

With the FATF requirements, the Law on the Prevention of Money Laundering and the Financing of Terrorism and the topics that are currently addressed in the existing guidelines as a basis, the topics that all guidelines for obligors should address, are the following:

1. Risk analysis and risk management
    a. Geographical and country risk
    b. Client risk
    c. Transaction risk
    d. Service and Product risk
2. New technologies
3. Customer due diligence measures
    a. Beneficial owner
4. Enhanced due diligence
    a. PEPs
    b. non face-to-face situations
5. Simplified due diligence
6. Unacceptable customers
7. Reliance on third parties
8. Monitoring customer's activity
9. Reporting suspicious transactions to the Administration for the Prevention of Money Laundering
    a. Indicators for suspicious transactions
10. Compliance officer

11. Education and training of employees
12. Internal controls
13. Keeping records, protection and keeping of data from those records
14. Implementation of measures of detecting and preventing money laundering and terrorism financing in branches
15. Cooperation with the Supervisor and the APML

Annex 2 has a template for sectoral guidelines which is a compilation of the existing sectoral guidelines. The supervisory authorities are recommended to take those sections from Annex 2 that are not–adequately- addressed in their guidelines and add them to their current guidelines. The sections in the compilation are mainly taken from the guidelines of the SC and the Foreign Currency Inspectorate as these guidelines address most required topics. On a few topics, additional guidance is added.

4. Additional recommendations

NBS

- The NBS should ensure that their guideline is made applicable to all relevant sectors under supervision of NBS (banking, insurance, pension funds, financial leasing) and that the examples in the guideline are relevant for all of their sectors.
- The NBS could consider adding a guidance section on correspondent banking.

Foreign Currency Inspectorate

- The Foreign Currency Inspectorate should ensure that their guidelines is made applicable to exchange offices and that examples are added for this sector.

Games of Chance Inspectorate

- The Games of Chance Inspectorate has not issued any AML/CFT guidelines. The Inspectorate can take the template as a basis for their guidance and work with the APML on examples of low, normal and high risk situations.

Harmonizing guidelines for SC and NBS

- The SC and the NBS have AML/CFT supervision responsibilities of the same entities (authorized banks and custody banks). Their guidance documents needs to be in line to ensure that there are no discrepancies or conflicting guidance.
- The guidelines of the SC address most topics and only needs to be enhanced on a few topics. If the NBS amends their guidelines in line with the template of Annex 2, any discrepancies or conflicts between the guidelines of these two supervisors will be avoided.

Harmonizing guidelines of APML and Foreign Currency Inspectorate

- The APML and the Foreign Currency Inspectorate both have responsibilities for AML/CFT purposes with respect to money transfer services and factoring & forfeiting.
- The guidelines of the Foreign Currency Inspectorate address most topics. If the APML amends their guidelines along the template of Annex 2, any discrepancies or conflicts will be avoided.

Annex 1- Analysis of topics addressed in existing AML/CFT guidelines

Supervisor / Topic	SC	Foreign Currency Inspectorate	NBS	Min Trade & Telecom (Postal services)	Min Trade & Telecom (Real estate)	APML (Acc & Auditors)
Risk analysis	+	+	+	+	+	+
Risk management	+	+	+	-	-	-
Country risk	+	+	+	+	+	+
Customer risk	+	+	+	+	+	+
Transaction/Service/Product risk	+	+	+	+	+	+
CDD	+	+	+	±	±	±
Beneficial owner	-	-	-	-	-	-
EDD	+	-	±	±	±	±
PEP	+	-	+	-	-	+
Non face to face	+	-	-	-	-	±
SDD	+	-	-	-	-	±
Third party reliance	+	+	-	-	-	-
Unacceptable client / refusing clients	±	±	-	-	-	-
Monitoring customer's activity	+	+	-	-	-	±
Reporting STRs and STR indicators	+	+	-	-	-	+
Internal controls	+	+	±	-	+	-
Compliance officer	+	+	-	-	-	-
Training	+	+	±	+	+	-
Cooperation with FIU/supervisor	+	-	-	-	-	-
Record keeping	+	+	-	-	-	-
Data protection	+	+	-	-	-	-
Branches	-	+	-	-	-	-

+ : addresses this topic
±: addresses this topic to some extent
- : only mentions this topic or does not address this topic

Annex 2 - Template for Guidelines for Obligors

NOTE FOR SUPERVISORY AUTHORITIES
This is a template for sectoral AML/CFT guidelines which is a compilation of the existing sectoral guidelines enhanced with additional examples and guidance on several topics. The supervisory authorities are recommended to take those sections from this template that are not or not adequately addressed in their guidelines and add them to their current guidelines.
Some supervisory authorities might have left out certain topics in their current guidelines because these are already clearly regulated in the AML/CFT Law. Nevertheless, it will assist obligors if these requirements are complemented with additional guidance and examples to provide obligors with further instructions on how to implement the AML/CFT Law.
Some requirements in the AML/CFT Law are not applicable to some obligors. For those cases, clearly the supervisory authorities do not need to add those topics to their guidelines.

Introduction

The guidelines for the prevention of money laundering and terrorism financing are being issued with the aim of eliminating the risk to which obligors are exposed, appropriate assessment of the exposure to the risk of money laundering and terrorism financing, drafting of risk analyses, development of risk recognition and management procedures in order to ensure that provisions of the Law on the Prevention of Money Laundering and the Financing of Terrorism and regulations based on it are applied uniformly by obligors.

During the performance of the activities for which they are registered, obligors are required to act in compliance with obligations prescribed by the Law which regulate the area of detecting and preventing money laundering and terrorism financing, and to ensure observance of the prescribed measures and activities at all levels, making sure that all obligors' business activities are conducted in compliance with the Law.

Actions and measures for the detection and prevention of money laundering and terrorism financing are undertaken before, during and after the execution of a transaction and establishment of a business relationship. They include the following:

- knowing clients and monitoring their business operations (customer due diligence);
- reporting suspicious transactions to the Administration, and drawing up lists of indicators for the identification of persons and transactions for which there exist grounds for suspicion of money laundering or terrorism financing;
- designating persons responsible for applying obligations laid down in the Law (compliance officers) and their deputies, and providing the necessary conditions for their work;
- regular professional education, training and improvement of employees;
- providing regular internal controls of the implementation of obligations laid down in the Law;
- keeping records, protecting and keeping data from those records;
- implementation of measures in obligor branches and majority-owned subsidiaries located in foreign countries;
- cooperation between the supervisor and the Administration.

Risk analysis

Pursuant to the Law, the risk of money laundering and terrorism financing is a risk of a client abusing the obligor for laundering money or financing terrorism, or that a client, transaction, service or business relationship will be indirectly or directly used for laundering money or financing terrorism.

In order to ensure prevention of exposure to the negative consequences of money laundering money and terrorist financing, under the Law obligors are required to make a risk analysis which should contain a risk assessment for each group or type of clients, business relationship, service provided by the obligor within its business, or transactions.

The risk analysis is used to determine the risk of a certain client, business relationship, and service provided by the obligor within its business, or transaction, to a risk of money laundering or terrorism financing, and is the basis for the risk-based approach.

A risk-based approach proceeds from an assumption that different business relationships established by obligors within their business activities can carry a smaller or greater risk of money laundering and terrorism financing. We can also speak about different degrees of risk in respect of clients with whom obligors do business, as well as in respect of the types of services they perform within their business operations, because they are not equally liable to abuses when money laundering and terrorism financing is involved. The risk-based approach allows for better risk management, a focus on real and identified threats, efficient utilisation and distribution of resources and flexibility in adapting to risk, as they change over time. The approach makes possible an achievement of better results with the same degree of invested effort, i.e., it makes it possible for obligors to pay less attention to low-risk clients and more attention to high-risk ones.

Drafting a risk analysis is a precondition for implementing prescribed client analysis measures. Pursuant to the classification of the client, business relationship, service or transaction into a risk category depends the type of client analysis which the obligor is required to perform under the Law (ordinary client analysis, enhanced client analysis, simplified client analysis – low-risk group).

The Minister of Finance has laid down the criteria according to which obligors classify clients, business relationships, services or transactions in a low-risk group for money laundering or terrorism financing, except for the cases listed in the Law, and in accordance with the technical criteria prescribed in recognised international standards, in the Regulation on the Methodology of Performing Activities in Accordance with the Law on the Prevention of Money Laundering and the Financing of Terrorism (*Official Gazette of the RS*, No. 07/2010 dated 19 February 2010).

Risk management

Obligors, i.e., their administrations, may before drafting a risk analysis embrace an appropriate policy of managing the risks of money laundering and terrorism financing. The objective of adopting such a policy is primarily to define at obligor level those areas of business which are more or less critical from the aspect of a risk of abuses for money laundering and terrorism financing, i.e., for the obligor to determine and define on its own the main risks and measures for resolving them.

The risk analysis is a procedure in which the obligor defines the following:

- the probability that its business operations can be abused for money laundering or terrorism financing;
- criteria based on which it will classify a client, business relationship, service or transaction as more or less risky in respect of money laundering or terrorism financing;
- consequences and measures for efficiently managing such risks.

In drafting a risk analysis obligors should also take into account the following criteria:

1. obligors must produce the risk categories from the risk criteria determined in the Law, the Regulation and the Guidelines, based on which in implementing measures of analysing clients they will classify a client, business relationship, service or transaction into a risk category;
2. obligors may, in line with their risk management policies, in determining risk categories, autonomously classify certain clients, business relationships, services or transactions as being in a high-risk category for money laundering or terrorism financing, and perform an enhanced analysis of the client;
3. obligors may not, in determining risk categories of clients, business relationships, services or transactions, classify them autonomously as medium- (normal) or low-risk, if under the Law, Regulation and Guidelines they are defined as high-risk. Neither may obligors in contravention of provisions of the Law, regulations or the Guidelines, autonomously expand the sphere of clients, business relationships, services or transactions which they treat as low-risk.

Within the meaning of these Guidelines, a risk assessment should include at least four main types of risk:

- geographical or country risk;
- client risk;
- transaction risk; and
- product and service risk.

In cases other types of risks are identified, due to the specific nature of the obligor, obligors should also include those risks. The assessment of risk of a client also depends on the location of the obligor or the location of its organizational units, implying different level of risk to obligors located in an area visited by many tourists compared with obligors located in a rural area, where all clients are known personally. Increased risk may occur at border checkpoints, airports, in places with high concentration of foreigners or in cases of transactions involving foreigners (e.g. fairs), in places where embassies or consular offices are situated, in the areas with high risk of corruption and crime, etc.

a. Geographical or country risk

The geographical/country risk is an assessment of the exposure to a risk of money laundering or terrorism financing depending on the region where the country of origin of the client, the country of origin of the majority founder, or of the client's owner or of the persons who otherwise exert a controlling influence on the management of the client and performance of those activities, and the country of origin of the person who executes transactions with the client is located.

The factors based on which it is determined whether certain countries or geographical locations carry a higher risk of money laundering or terrorism financing include the following:

1. states against which the United Nations, the Council of Europe or other international organisations have applied sanctions, an embargo or similar measures;
2. states which credible institutions (the Financial Action Task Force-FATF, the Council of Europe and others) have designated as failing to apply adequate measures to prevent money laundering and terrorism financing;
3. states which have been designated by competent international organisations (e.g., the World Bank, the IMF) as failing to apply appropriate measures for the prevention of money laundering and terrorism financing;
4. states which have been designated by competent international organisations as states with a high incidence of organised crime due to corruption, arms trafficking, white slavery or human rights violations;
5. states which credible institutions have designated as those supporting or financing terrorist activities or organisations;
6. states designated by international organisations (the FATF, the Council of Europe, etc.) as uncooperative countries or jurisdictions (countries or jurisdictions which in the view of the FATF have no adequate legislation in the area of the prevention or detection of money laundering or the financing of terrorism, which have no supervision of financial institutions or poor supervision, where the establishment and activity of financial institutions is possible without authorisation of registration with competent public authorities, where the state encourages the opening of anonymous accounts or other anonymous financial instruments, where the manner of recognising and reporting suspicious transactions is deficient, whose international co-operation is inefficient or non-existent, where the law does not provide for an obligation to establish the identity of the beneficial owner, etc.).

In Article 21 of the Regulation the Minister of Finance lists the states which do not apply standards in the area of the prevention of money laundering and the financing of terrorism (so-called black list), and in Article 22 the states which apply money laundering and terrorism financing prevention standards at the level of European Union standards, or higher, (so-called white list). Obligors use the lists of states for assessing the risk to which they can be exposed by a client on those lists. The risk assessment and rating also depend on the location of the obligor and its organisational units. A low degree of product/service risk neutralises to a certain extent risks caused by the location. Transactions conducted at offshore designations carry a higher risk of money laundering and terrorism financing. Clients in the region can be less risky than those outside it, or those in countries with which we have no business relations.

b. Client risk

Obligors autonomously determine their approach to the client risk, based on generally recognised principles and their own experiences. The classification of clients into risk categories is based on identified indicators that are used to identify potential risks. A number of client characteristics are taken into account in establishing a risk profile, such as the client's background, residence or source of income. Where it is physically possible to verify a client's likeness to documents evidencing identity and obtain information in person, this will also help to satisfy or mitigate the client risk.

The threats posed by different types of clients are mainly attributable to the nature of their economic activity or source of wealth. For example, the risk to an obligor that a salaried employee whose only transactions are those derived from electronic payments made by his employer and daily expenses are going to be much lower than a client whose transactions are cash based with no discernable source for this activity. The country or jurisdiction in which the client created their income also needs to be considered in the overall risk classification.

Corporate structures, trusts and partnerships are recognised internationally as vehicles through which opacity in financial transactions can easily be introduced. This can be used by criminals to add layers between a criminal activity and the final use of the illegal funds. Additionally, structures that add layers of complexity, e.g., nominee shareholdings, trusts, powers of attorney have their place in normal legal structures and tax planning scenarios but are just as attractive to criminals for the same reasons. Obligors must recognise the risks that structures that add complexity or opacity to a legal entity pose to their business and have adequate systems of control to ensure that these risks are properly mitigated. Legal entities may come in a variety of different types but their economic activity will be much more varied. Obligors need to include in their risk classification a recognition of the risk posed by the economic activity being conducted through the legal entity. For example, cash-intensive businesses, professions linked to corruption and bribery, real estate development will warrant higher due diligence.

The activities of the following clients may indicate a greater risk:
[supervisor to add examples relevant for the category of obligors]

c. Transaction risk

Risk elements for transactions lie in the frequency, amounts, source and destination of a transaction. Transactions that obscure the source of the funds or facilitate anonymity will be of higher risk. Some transactions may be innocent enough not to attract a risk to the obligor if conducted as a single transaction. These may be low value transactions. However when made in multiples, these transactions could be seen as a conduit through which criminals could layer or integrate proceeds of criminal activity into the system.

Transactions conducted online removes the human element and thereby entail higher risk. Whereas receiving instructions through face-to-face contact will enable an obligor to address any concerns about a proposed transaction.

Money laundering investigations have shown that criminals make extensive use of electronic payment and message systems. The rapid movement of funds between accounts in different countries and jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer or the ultimate beneficiary is not clearly shown in an electronic payment message instruction.

The transaction risk encompasses the following transactions:
[supervisor to add examples relevant for the category of obligors]

d. Product and Service risk

The product and service risk is the risk posed by the product or service proposition itself. Some products or services are inherently less attractive to criminals than others whilst others are the most favoured. Some lease products, life insurance policies with a low annual premium or a low single premium, pension products, consumer loans or savings products have a low inherent risk because of the long term to realise benefits. Low risk services can for instance be standard services for private customers (savings accounts, salary accounts, etc.) or for small-sized business customers (current account facilities, etc.). 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.

The product and service risk concerns the following risky services:
[supervisor to add examples relevant for the category of obligors]

Besides the criteria listed above, obligors should in determining the degree of risk of clients, business relationships, services or transactions include other types of risk or other criteria, such as the following:

- the size, structure and activity of the obligor, including the volume, structure and complexity of the activities performed by the obligor;
- the status and ownership structure of the client;
- the presence of the client, i.e., if the client is not physically present during the conclusion of the business relationship or implementation of the transaction;
- the source of the funds which are the object of the business relationship or transaction in the case of a client who is according to the criteria defined in the Law a politically exposed person;
- the purpose of the conclusion of the business relationship, service or execution of the transaction;
- knowledge of services and its experience, i.e., knowledge in this area;
- other information which indicates that a client, business relationship, service of transaction carry a higher risk.

New technologies

Obligors are required to pay particular attention to all risks of money laundering and terrorism financing which might be the result of the use of new technologies, and implement appropriate measures to prevent the use of those technologies for money laundering and terrorism financing.

Customer due diligence measures

Customer due diligence measures are key preventive elements in the process of detecting and preventing money laundering and terrorism financing. The purpose of implementing customer due diligence measures is to establish and verify in a credible manner the identity of the client based on documents, data and/or information from reliable, trustworthy and objective sources, to determine the beneficial owner of the client and verify the owner's identity, to obtain information about the purpose of the business relationship or transaction and other data in accordance with the Law, and to regularly monitor business activities and check the conformity of the client's activities with the nature and purpose of the business relationship and the usual scope and type of business being

performed by the client, pursuant to the provisions of Article 8 of the Law.

The extent and detail of the client information must be sufficient to allow the obligor to readily identify variances between actual activity and the stated intended nature of the business relationship and to increase information requirements in order to satisfy itself that money laundering or the financing of terrorism can not take place. By seeking information on the nature or source of the client's income or economic activity an obligor is able to ascertain the risk posed to it in respect of money laundering or the financing of terrorism. The obligor will need information that the client's economic activity is plausible. To determine the plausibility that the funds originate from a legal source, the obligor should identify specific indicators which determine the depth of the review. Especially in high-risk situations, the plausibility of the funds need to be determined and recorded using independent and credible sources. It should be clear to an obligor when a client is providing a source of funds or economic activity that is incompatible with the information it has from other sources.

Obligors apply customer due diligence measures in the following cases:

1. when establishing a business relationship with a client (a business relationship is every business or other contractual relationship which the client establishes or concludes with the obligor and which is linked with the performance of the obligor's activity);
2. when carrying out a transaction whose value is the dinar equivalent of 15 000 EUR or more calculated by the National Bank of Serbia median exchange rate on the date of execution of the transaction, irrespective of whether the transaction is carried out in one or more than one connected operations;
3. when there are doubts about the veracity or credibility of previously obtained data about a client or beneficial owner of the client;
4. always when there are grounds for suspicion in connection with a client or a transaction that money laundering or terrorism financing are involved, irrespective of the transaction's value.

The Law authorises obligors, depending on the level of risk of money laundering and terrorism financing, to categorise clients and business relationships into three basic degrees of risk. Based on an estimated degree of risk obligors implement adequate customer due diligence actions and measures. Risk assessments are performed for the duration of the business relationship, and the degree of risk can change. For example, a certain business relationship with a client can initially be assessed as low-risk, and circumstances can then appear which will increase the risk, and vice versa. This does not relate to cases which are classified by the Law as high-risk, to which enhanced actions and measures must be applied (bank transfers from foreign countries, foreign high officials, establishment of a business relationship without the physical presence of the client).

Money laundering risk may be assessed differently by the obligor than terrorism financing risk. Obligors must pay particular attention to clients whose business operations take place largely with cash money because of a terrorism financing risk. Particular attention in that respect should be paid to the operations of non-profit organisations, because there are numerous possibilities for their abuse for financing terrorism. The geographical risk in relation to the financing of terrorism is pronounced in regions where, according to the data of relevant international organisations such as the United Nations, terrorists are active.

Depending on the degree of risk of money laundering and terrorism financing, international standards and the Law make it possible for obligors to implement three types of customer due diligence measures: general, simplified, and enhanced.

a. Beneficial owner

In case the customer is a legal entity the obligor should identify the beneficial owner. The beneficial owner of a legal entity is a natural person who ultimately owns or controls the legal person. The customer due diligence of the ultimate beneficial owner is a requirement since criminals often use schemes involving (foreign) legal persons as a means to conceal the criminal source of funds.

The obligor can take risk-based and adequate measures to verify identity of the beneficial owner. These verification measures should enable the institution to obtain sufficient information to verify identity and to convince itself of the identity of the beneficial owner. The identity of the ultimate beneficial owner should be verified using independent and reliable documents. The obligor should take into account that the scope of the verification measures is related to the risk of money laundering and terrorist financing, which risk depends in turn on the type of customer, product or transaction.

This requirement to verify the identity of the beneficial owner can be met by checking the original or certified copy of the documentation from an official public register which may not be issued earlier than three months before its submission to the obligor. In case data is missing the obligor can have the customer report who the beneficial owner is, and by obtaining the missing data from a representative, procura holder, or empowered representative of the customer.

If, for objective reasons, the data cannot be obtained as specified in this Article the obligor shall obtain it from a written statement given by a representative, procura holder or empowered representative of the customer. The obligor takes the risk assessment of the customer into account in such a way that obtaining written statements is sufficient in case of low-risk customers, but not for high-risk customers.

The obligor also checks whether the beneficial owner is a politically-exposed person.

Enhanced due diligence

Obligors should implement appropriate risk-based measures and controls to mitigate potential risks of money laundering for certain clients designated as high ML/TF risk. Enhanced customer due diligence measures include additional measures which the obligors undertake in cases prescribed by the Law and other cases when they estimate that owing to the nature of the business relationship, the ownership structure of the client, or other circumstances connected to the client or business relationship – there exists a high level of risk of money laundering and terrorism financing. A high level of risk of money laundering and terrorism financing requires the collection of additional information about the nature of the business relationship, as well as more frequent monitoring of the client's business operations.

The Law stipulates that the following should be considered to entail high money laundering or

terrorism financing risk: business relationships established with a politically exposed person and cases when the identity of a customer was not established and verified in its presence or if the identity of a customer was established and verified by a third person.

If a client has been classified in a high-risk category, irrespective of whether it is stipulated by the Law that he or she be classified in this category or the obligor itself has classified the client as high-risk – enhanced customer due diligence actions and measures are effected.
Which additional measures obligors will undertake when they classify clients in a high-risk category based on their own risk assessment depends on the concrete situation. For example if a client was assessed as high-risk due to its ownership structure, the obligor may by its procedures envisage an obligation of collecting additional data and an obligation to additionally check submitted documentation.

These control measures can include increased awareness of the obligor that there exist high-risk clients and transactions within this economic branch, enhanced monitoring of transactions, enhanced levels of control, and more frequent inspections of relationships.

The Law stipulates in Article 28, paragraph 2 that enhanced due diligence measures referred to in Articles 29-31 can be applied in cases of a high risk customer, business relationship, service or a transaction when an obligor estimates that there might be a high level of ML/FT risk. The following measures are stipulated:

1. Mandatory prior written approval of establishing a business relationship or execution of a transaction by a person in charge;
2. Mandatory application of one of the following measures:
    a. Obtaining documents, information or data on which an obligor may additionally check and verify the veracity of identification documents and information based on which the identity of the customer was established and verified;
    b. Additional scrutiny of obtained information about the customer in public and other available databases;
    c. Acquiring references from relevant institutions the customer has established business relations with;
    d. Additional scrutiny of data and information about the customer with the competent state authorities or other competent institutions in the state of residence of the customer or of its headquarters
    e. Establishing direct contact with a customer by telephone or by a visit of an authorized person of the obligor at home or headquarters of the customer,
3. Mandatory monitoring of transactions or other business activities a customer carries out at the obligor's.

Clients who represent a high risk of money laundering or terrorism financing are the following:

1. persons for whom the Administration has issued an order to the obligor to monitor all transactions or business operations of those persons and to notify the Administration thereof, because there exist grounds for suspicion that money laundering or terrorism financing are involved (Article 57 of the Law);
2. persons for whom the Administration has issued to the obligor an order on temporary suspension of the execution of a transaction (Article 56 of the Law);

3. persons for whom the Administration has extended the term to the obligor of an order for monitoring transactions or the person;
4. persons for whom the obligor has sent data to the Administration, because reasons to suspect money laundering or terrorism financing had existed in connection with that persons or a transaction that person had carried out.

a. Politically-exposed persons

Clients who must be classified as high-risk are politically-exposed persons or foreign high officials, in accordance with the Law. The obligor shall establish the procedure determining whether the client or its beneficial owner is a foreign high official, member of the foreign high official's immediate family or foreign high official's close associate, whereby this procedure shall also be applied to the legal entity in which the foreign high official, member of the foreign high official's immediate family or foreign high official's close associate is a representative, proxy or agent. The procedure can be used to define different approaches towards persons who are residents and domestic citizens from those who are non-residents or foreign nationals, because there is a higher probability of the latter being foreign high officials. But this need not always be the case. For example, a Serbian citizen holding a high office in an international organisation is a foreign high official.

To obtain relevant information for identification of foreign high official, the obligor shall undertake the following activities:

- obtain a written statement from the client that he or she is a foreign high official, a member of the immediate family of a foreign high official, or a close associate of the foreign high official;
- use commercial electronic data bases which contain lists of high officials (e.g., World- Check, Factiva, Lexis Nexis);
- search publicly available data and information via the Internet, the media etc.

If information obtained in relation to the client and other publicly available information indicate that the resident or domestic person is a foreign high official, the obligor shall obtain a signed written statement which the customer must complete before establishing a business relation or execution of a transaction. The written statement shall contain:

1. Full name, permanent residence, date and place of birth of the customer establishing a business relation or ordering a transaction, the number, type and issuer of the valid identity document;
2. A statement whether the person is a politically exposed person – pursuant to the criteria set in the Law;
3. Information about the type of the political exposure (a person which has been in a prominent public position for the last year or longer, or a member of family of a politically exposed person or a close associate;
4. Information about the time period of discharging the function, if the customer is a person which has been in a prominent public position in a foreign country for the last year or longer;
5. Information about the type of the public function a person has been performing for the last year (or longer) such as the president of a state, prime minister, ambassador etc.;

6. Information about family relations, if the customer is a member of the family of a politically exposed person who has been occupying a prominent public position in a foreign state for the last year (or longer);
7. Information about the type and manner of business cooperation, if the customer is a close associate of a person who has been occupying a prominent public position in a foreign state for the last year (or longer);
8. Provision according to which, in order to establish the veracity of information, the customer permits the obligor to check the information about the customer by inspection of public or other available sources of information, i.e. to acquire such information directly from the competent authorities of another state, consular representative office or embassy of the state in the Republic of Serbia or the Ministry of Foreign Affairs of the Republic of Serbia;
9. Personal signature of the customer.

The procedure to determine if a client is a public official shall be undertaken also during business relationship with the client, within regular monitoring of its operations. The following factors may be important here:

- foreign high official's country of origin (risk related to dealing with the foreign high official is higher if the official comes from the country with a high degree of corruption and crime);
- foreign high official's title, responsibility and authorisations (higher degree of title or a higher degree of responsibilities indicate a higher risk given a greater possibility of use and allocation of government funds);
- volume and complexity of the business relationship (higher degree and greater complexity of the established business relationship between the foreign high official and the financial institution are indicative of the higher degree of risk regarding this person);
- type of product or service offered to the foreign high official (some categories of services imply higher risk - e.g. private banking);
- third parties doing business with the foreign high official (foreign high officials often rely on off-shore companies and banks, i.e. on entities located in areas or countries not applying adequate AML/CFT measures and standards).

If the client's beneficial owner is a foreign high official, member of the foreign high official's immediate family or foreign high official's close associate, or if these persons manage the client, the obligor shall undertake against this client enhanced due diligence measures. Such measures are undertaken by the beneficiary even when the physical person stops his/her public function over as much time as necessary to conclude that this person did not abuse his/her former position.

Enhanced due diligence, in addition to the due diligence measures referred to in Article 8, paragraph 1 of the Law implies application of additional measures referred to in Article 30 of the Law, as follows:

1. Obtaining the information about the origin of funds and property that is the subject of business relation or transaction from documents submitted by the customer. If it is not possible to obtain the information as described, the obligor shall take a statement of origin directly from its customer;
2. Mandatory written consent from the supervisor in charge, prior to establishing a business relation with such customer;
3. Special and meticulous monitoring of transactions and other business activities of a

politically exposed person after establishing a business relationship.

If it is determined during the business relationship that the client has become a foreign high official, the obligor is required to ask for the consent of the highest management for continuing the business relationship. The data and documentation obtained shall be kept in the client's file.

b. Non face-to-face

Another situation where the obligor is required to classify a client as high-risk is when the business relationship is being established without the physical presence of the client. In that case the obligor is required, besides identifying the client, also to collect additional information about the client's identity (for example additional personal documentation, business documentation, authorisations signed by responsible officers, etc.).

It is recognised that where a client makes face-to-face contact with an obligor, this may be perceived to lower the risk to the obligor. Not only does this present an opportunity for the obligor to verify that the likeness of the person in front of them physically matches that of the documents being presented to support this but is also an opportunity for staff to identify any inconsistencies.

Any mechanism through which the client interacts with an obligor in a non-direct manner increases the exposure to risk. Not only does this allow for third parties to have access to funds or assets through impersonation but also disguise the true owner of those assets by, for example, provision of false identification documentation.

Obligors must put into place control systems that appropriately address the risks posed by non face-to-face contact for clients either at the opening of the business relationship or through the monitoring of that relationship.

In the course of establishing a business relation in customer's absence, when the identification and verification of identity was carried out by a third person, obligors shall ensure that the third person who was delegated to apply enhanced customer due diligence measures, has established and verified the identity of the customer in its presence.

When establishing a business relation in the absence of a customer, pursuant to the Law, an obligor shall apply measures prior to the execution of a transaction, ensuring that the customer has made the first payment from an account opened by the customer in its own name or by its legal representative on behalf of the customer, with a bank headquartered in the Republic of Serbia licensed by the National Bank of Serbia to carry out banking activities.

Simplified due diligence

The Law provides that an obligor can conduct simplified due diligence measures in cases referred to in Article 9 paragraph 1 and 2 of the Law and in cases when the risk of money laundering and terrorism financing is inconsiderable, when the information about the customer – a legal person or its beneficial owner are transparent and readily available or when there is adequate government supervision of the entity. Examples of low-risk can be the following: establishing a business

relationship with a public authority, with a joint stock company whose securities are traded on the securities market in Serbia, etc., unless in connection with the client or the circumstances there exist grounds for suspicion that money laundering or terrorism financing are involved.

An obligor identifies and verifies the identity of its customer, but the procedure is reduced and less complex than with the general customer due diligence measures or enhanced customer due diligence measures. In cases when it is lawful to apply simplified due diligence, the obligor must determine whether the customer really meets the conditions and in accordance with the Guidelines it poses inconsiderable risk of money laundering and terrorism financing. An obligor must not establish a business relationship or execute a transaction prior to establishing all the facts required to determine whether it is the case of simplified customer due diligence. Simplified customer due diligence is not allowed when there is suspicion of money laundering and terrorism financing regarding a customer or a transaction, i.e. if a customer has been placed in the high risk category (Article 9, paragraph 1, item 3) and 4) of the Law).

An obligor may apply simplified customer due diligence measures only exceptionally in cases and under the conditions stipulated by Article 32 and 33 of the Law. Obligors must comply with the exceptions referred to in Article 32 of the Law, if there are reasons to suspect money laundering or terrorism financing with respect to a customer or a transaction.

Unacceptable customers

Based on the risk assessment, the obligor determines if the client poses an unacceptable risk. This may relate to circumstances or characteristics that result from initial due diligence during the customer acceptance process or from transaction monitoring or the periodic reviews of the client's risk profile. If there is indeed an unacceptable risk, the institution will not enter into a business relationship with the client or it will terminate the existing relationship. This is often described in a "customer exit policy", which describes under which circumstances and according to which procedures the institution will terminate its relationship with the client. Examples of potentially unacceptable risks are:

- problems in verifying the client's identity;
- clients who wish to remain anonymous or who provide fictitious identity details;
- shell banks (banks incorporated in a jurisdiction where they have no physical presence);
- the client's name corresponds to a name on the UN or EU terrorist lists;
- clients with respect to whom it appears, based on further information, that the combination of client and products to be used entails unacceptable risks;
- clients who will not provide information or who provide insufficient information (or submit inadequate documentation for verification purposes) about their nature and background, in particular the source of their funds;
- an investigation revealed that, given the client's activities, the corporate structure is complex, non-transparent or obscure, without such being underpinned by a logical explanation in terms of business management;

- professional counterparties who lack the required authorization ('illegal financial undertakings').

Reliance on third parties

In the establishment of a business relationship the obligor may, under conditions laid down by the Law, entrust the performance of certain customer due diligence actions and measures to a third party, in which process the obligor is required to verify that the third party meets the requirements stipulated by the Law. By entrusting certain customer due diligence actions and measures to a third party the obligor is not released from the responsibility for the correct performance of customer due diligence actions and measures in accordance with the Law.

The third party is required to submit to the obligor data collected about the client which the obligor requires in order to establish a business relationship, and, acting on a request of the obligor, deliver without delay copies of identity papers and other documentation based on which the third party applied the customer due diligence actions and measures and obtained the requested data about the client. The obligor is required to keep the obtained copies of the identity papers and documentation in accordance with the Law. If the obligor has doubts about the credibility of the customer due diligence actions and measures performed, or of the identification documentation, or of the veracity of data obtained about a client, it is required to request from the third party to submit a written statement about the credibility of the customer due diligence actions and measures performed and the veracity of the data collected about the client.

The third party who conducted the analysis of the client instead of the obligor is responsible for the fulfilment of obligations laid down by the Law, including the obligation of reporting suspicious transactions and the obligation of keeping data and documentation.

Although the obtaining of the data and documentation (analysis of the client) was conducted by a third party instead of the obligor, the obligor is still responsible for the customer due diligence actions and measures performed.

Monitoring customer's activities

Regular monitoring of customer business transactions represents a key element in establishing the efficiency of implementation of stipulated measures for detecting and preventing money laundering and terrorism financing. The purpose of monitoring customer business transactions is to detect possible money laundering or terrorism financing by checking transactions conformity with the intended nature and purpose of a business relationship of a customer and its normal scope of business.

Monitoring the business activities of the client encompasses four segments of the client's business, as follows:

1. Monitoring and verifying the conformity of the client's business with the envisaged nature and purpose of the business relationship;
2. Monitoring and verifying the conformity of the client's source of funds with the envisaged source of funds that the client listed in the process of establishing the business relationship;
3. Monitoring and verifying the conformity of the client's business with the client's usual volume

of business;
4. Monitoring and recording collected documents and data on the client.

Obligors should also have procedures to deal with clients who have not had contact with the obligor for some time, in circumstances where regular contact might be expected, and with dormant accounts or business relationships, to be able to identify future reactivation and unauthorised use.

The Law proceeds from a basic assumption that certain clients, business relationships, services and transactions carry or smaller or greater risk and threat of money laundering or terrorism financing. For that reason the Law introduces, besides regular analyses of the client (general customer due diligence action and measures), two other different manners of analysis of the client: enhanced analyses for clients with a major risk of money laundering and terrorism financing, and simplified client analyses, which are permitted where there is a negligible risk of money laundering and terrorism financing.

How often and to what extent a customer's activities will be monitored depends on the level of risk a customer entails, i.e. its risk category appraisal. The appropriate level of business activities of a customer understands stipulated measures for monitoring business activities of a customer in a continuous manner and considering services and transactions that the obligor provides and executes for the customer.

In accordance with its ML/FT risk management policy, an obligor may opt for more frequent monitoring of business activities of certain categories of customers and adopt additional scope of measures for the monitoring of customer business activities and determining compliance of its operations.

Monitoring may take place at various levels, depending on the risk and size of activities. The higher the risk, the more intensive (in terms of frequency and depth) the monitoring effort should be. Examples of monitoring methods are:

- Spot checks: targeted checks of accounts and transactions, e.g. of specific groups of customers, or of accounts and transactions earlier deemed to pose an enhanced risk on the basis of reports to the APML or otherwise.
- Manual monitoring: the account manager knows his/her customers and their financial behaviour. Deviations from the customer's normal behaviour will immediately be spotted by the account manager. Key factors in this type of monitoring are an effective and realistic span of control as well as the expertise and competence of the persons carrying out the control operations.
- Periodic management surveys/reports: this type of monitoring is used in case of fairly manageable numbers of customers and transactions. A daily, weekly or monthly printout of turnover, balance, exceeding of limits, fees charged and so forth may give an indication which accounts require closer scrutiny.
- Monitoring by hard indicators: this method is used for an initial filtering on the basis of turnover, maximum balance, transaction amounts, countries of origin or destination, risk sectors and so forth.
- Intelligent transaction monitoring: this type of monitoring is often based on the profiling of each account or customer. Such profile can be made up of turnovers, transaction amounts,

contra accounts, transaction frequency, transaction particulars and so forth. Each element of the profile can be assigned a particular weight. Each new transaction will be checked against the profile, with the transaction that differs the most from the profile getting the highest risk grade. For all transactions that exceed a chosen risk grade, further investigation is called for. Only then can it be determined whether a transaction should be considered suspicious or unusual.

In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the customer, country and product risk. Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction logical for the customer's business or activities?
- Has the pattern of transactions conducted by the customer changed?
- Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

Several types of monitoring can be combined. For instance, monitoring combined with the profiling of accounts with relatively low turnovers and balances will not be very interesting from a cost-versus-risk viewpoint. In contrast, hard indicators (turnover, maximum balance, transactions to and from specific countries and so forth) enable the institution to determine whether such an account should be reclassified from low risk to normal risk or even enhanced risk, after which intelligent monitoring could be applied.

One or other of these approaches may suit most obligors. For obligors that have major issues of volume, a more sophisticated automated system may be necessary. The effectiveness of a monitoring system in identifying unusual activity will depend on the quality of the parameters which determine what alerts it makes, and the ability of staff to assess and act as appropriate on these outputs. The needs of each obligor will therefore be different, and each system will vary in its capabilities according to the scale, nature and complexity of the business. It is important that the balance is right in setting the level at which an alert is generated; it is not enough to fix it so that the system generates just enough output for the existing staff complement to deal with. But equally, the system should not generate large numbers of 'false positives', which require excessive resources to investigate.

Reporting suspicious transactions to the Administration for the Prevention of Money Laundering

Suspicious transactions are defined as transactions which in the opinion of obligors, in respect of the transaction itself or the person executing it, create reasons for suspicion of money laundering or terrorism financing, or that the transaction involves funds derived from illegal activities. It proceeds from the provisions of the Law that suspicious transactions are all transactions which are by their nature, volume, complexity, value or linkage unusual, i.e., have no clearly visible economic or legal basis, or are in disproportion with the usual or expected operations of the client, and other circumstances linked with the status or other characteristics of the client.

As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is subjective and there is not always proof based on firm evidence. An obligor would not be expected to know the exact nature of the criminal offence or that the particular funds definitely arose from crime. However, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition is knowing enough about the customer's business to recognise that a transaction, or series of transactions, is unusual.

Obligors are required to submit data to the Administration always when there exist grounds for suspicion in connection with a transaction or a client that money laundering or terrorism financing are involved, before the execution of the transaction, specifying in the report the deadline for the execution of the transaction. In urgent cases notification may also be effected by telephone, with written notification following no later than the next workday. A reporting obligation also exists for planned transactions, irrespective of whether it has been executed.

If due to the nature of the transaction, because the transaction was not executed, or for other justified reasons, the obligor cannot submit data to the Administration, it is required to submit the data as soon as it becomes possible, and no later than immediately after it learns about the grounds for suspicion that money laundering or terrorism financing is involved, and to substantiate in writing why it had failed to act in the prescribed manner.

Obligors' employees who determine the existence of reasons for suspicion that money laundering or terrorism financing are involved are required to notify immediately the compliance officer for the prevention of money laundering, or the officer's deputy. The obligor is required to organise the procedure of reporting suspicious transactions between all organisational units and compliance officers, i.e., pursuant to the following instructions, to:

- determine in detail the manner of reporting data (by telephone, by fax, by safe electronic mail, etc.);
- determine the type of data which are reported (data about the client, transaction, reasons for suspicion of money laundering, etc.);
- determine the manner of co-operation of organisational units with the compliance officer;
- determine the way of acting towards the client in case the execution of a transaction is suspended by the Administration;
- determine the role of the compliance officer when a suspicious transaction is reported;
- prohibit employees from disclosing information that data, information or documentation are to be submitted to the Administration;
- determine measures in connection with continuing doing business with the client (temporary suspension, termination of business relationship, enhanced customer due diligence actions and measures, monitoring the client's future business operations, etc.).

Several obligors are also required to notify the Administration about all cash transactions of a value of at least 15,000 EUR in dinar counter-value immediately after they are carried out, or no later than three days after the transaction.

The Minister of Finance has laid down the manner of submitting data to the Administration, and conditions under which for certain clients obligors are not required to report to the Administration cash transactions of a value of 15,000 EUR or more in dinar counter-value, in the Regulation on the Methodology of Performing Activities in Accordance with the Law on the Prevention of Money Laundering and the Financing of Terrorism.

a. Indicators for suspicious transactions

The assessment of the suspiciousness of a transaction is based on criteria of suspiciousness specified in the list of indicators for recognising the client and the transaction for which there are reasons for suspicion of money laundering and terrorism financing. A list of indicators is the starting point for employees/compliance officers in recognising suspicious circumstances linked with a given client and/or transaction conducted by that client, for which reason obligors' employees must be informed about indicators so they can use them in their work. In the process of assessing suspicious transactions, compliance officers are required to provide professional assistance to employees.

Obligors are required to draft lists of indicators for recognising suspicious transactions or clients among which they will include indicators published on the Administration's website. In the procedure of determining the existence of elements for qualifying a certain transaction or person as suspicious, one should always keep in mind indicators for recognising the grounds for suspicion. However, if a transaction fulfils the criteria of one indicator, it does not mean that a suspicious transaction is involved and that the data should be forwarded to the Administration immediately. The broader framework should be viewed, in accordance with the principles that the obligor knows its client best, and it should be assessed whether a transaction is outside the bounds of the usual, or expected operations of the client. Conversely, a transaction may be suspicious without fulfilling any of the indicators.

Under the Law, all transactions which are by their nature, size, complexity, value or linkage unusual, or have no clearly visible economic or legal basis, or are disproportionate to the usual or expected operations of the client, as well as other circumstances linked with the status or other characteristics of the client, may be treated as suspicious transactions.

Certain transactions, clients and services, but also business relations, may be treated as suspicious. The rating of the suspiciousness of a certain client, transaction or business relationship is based on the criteria of suspiciousness defined in the list of indicators, but they may be suspicious even if they do not trigger any indicator.

Lists of indicators form the starting point for employees/compliance officers in recognising suspicious circumstances linked with a certain client, a transaction being performed by a client, or a business relationship being concluded by that client, which means that obligors' employees must be informed about indicators so they can use them in their work. In the process of assessing suspicious transactions, compliance officers are required to provide professional assistance to employees.

Obligors are required to develop a list of indicators for recognising persons and transactions for which there exist grounds for suspicion that money laundering or terrorism financing is involved,

taking into account the complexity and extent of the executed transactions, an unusual transaction execution patterns, the value or links of transactions with no economically or legally justified purpose, or transaction which are inconsistent or disproportionate to the usual and expected operations of the client, as well as other circumstances linked with the status or other characteristics of the client.

Obligors are required in drafting the list of indicators referred to in Article 50 paragraph 1 of the Law to include indicators from the List of Indicators posted on the Administration's internet site:
[supervisor to add examples that are relevant for their sectors]

It is especially important that all employees are informed about the indicators and that they use them during their work.

Compliance officer

Obligors are required to appoint compliance officers and deputy compliance officers for the performance of certain actions and measures for the prevention and detection of money laundering and terrorism financing, and to submit to the Administration data about the names and job titles of the compliance officer and deputy compliance officer, and all changes in those data, no later than 15 days from the dates of appointment.

Obligors are required to ensure that the jobs of compliance officer and deputy compliance officer are performed by persons meeting conditions laid down in Article 40 of the Law, and to provide for them the following conditions laid down in Article 42 of the Law:

- unrestricted access to data, information and documentation required for the performance of their tasks;
- appropriate human, material, IT and other work resources;
- adequate office space and technical conditions for an appropriate level of protection of confidential data at the disposal of the compliance officer;
- ongoing professional training;
- replacements during absences;
- protection with respect to the disclosure of data about the compliance officer to unauthorised persons, and protection from other actions which may affect unhindered performance of the compliance officer's duties.

Internal organisational units, including the highest management in the obligor, are required to provide assistance and support to the compliance officer in the performance of his tasks, and to notify the officer regularly about facts which are, or which may be, linked with money launder or terrorism financing.

Obligors are required to define in writing the manner of co-operation between the compliance officer and other organisational units.
In the performance of tasks laid down by the Law, compliance officers are required to:

- provide professional assistance to employees in the operational implementation of measures in the area of preventing and detecting money laundering and terrorism financing;
- advise the obligor's management in the formation of the management policy about money

laundering and terrorism financing risks;
- keep the obligor's management constantly informed about activities in connection with the detection and prevention of money laundering and terrorism financing;
- take part with other obligors in the development of an integrated policy of detecting and preventing money laundering and terrorism financing.

Regular professional education and training of employees

Obligors are required to provide regular professional education, training and improvement for all employees involved in activities of preventing and detecting money laundering and terrorism financing, as well as all those performing certain activities at their jobs which are or could be indirectly or directly exposed to a money laundering and terrorism financing risk, and all associate staff entrusted by contact with the performance of tasks, unless they are independent obligors for the implementation of measures of detecting and preventing money laundering and terrorism financing.

Obligors are required to draft annual professional education, training and improvement programmes for employees in the area of prevention and detection of money laundering and terrorism financing for each calendar year, no later than March for the current year. The programme should specify the following: the content and scope of the educational programme, the aim of the educational programme, the manner of implementing the educational programme (lectures, presentations etc.), the groups of employees for whom the educational programme is intended, the duration of the educational programme.

Obligors are required to pay special attention to the following:
- the level of training of employees, to ensure that they are capable of timely recognition of the risk of money laundering and terrorism financing,
- the level of awareness of employees of the risks to which the obligor could be exposed due to their omission,
- determination of the level of responsibility in the implementation of internal regulations regulating the area of the prevention of money laundering and terrorism financing.

Obligors are required to include in the procedure of employee professional education, training and improvement all new employees, and to organise for them a special programme of professional education, training and improvement in the area of preventing and detecting money laundering and terrorism financing. The programme should contain at least provisions on the obligation to analyse clients, assessment of the money laundering and terrorism financing risk, manner of forwarding prescribed data to the Administration for the Prevention of Money Laundering, indicators for recognising clients and transactions for which there exist reasons to suspect money laundering or terrorism financing, requirements with respect to the security and keeping of data, and procedures which the obligor itself has developed (internal regulations and instructions) for the purpose of implementing the Law, the Regulation and the Guidelines.

Regular professional education, training and improvement may be conducted by the compliance officer, the deputy compliance officer, or other duly professionally trained person appointed by the obligor's management on a proposal by the compliance officer.

Internal controls

Obligors are required to establish regular and systematic internal controls of the execution of tasks of preventing and detecting money laundering and terrorism financing. The purpose of the internal controls is to detect and eliminate deficiencies in the implementation of prescribed measures for the prevention and detection of money laundering and terrorism financing, and to improve the system of detecting transaction and clients for whom there exist reasons to suspect money laundering or terrorism financing. Controls of the correctness and efficiency of the prescribed measures of preventing and detecting money laundering and terrorism financing should be effected by obligors by means of regular or extraordinary supervisions, in the procedure of implementing internal controls pursuant to the Law, the Regulation and the Guidelines.

In the event of changes in the business process (e.g., organisational changes, changes of operating procedures, introduction of new services), obligors are required as part of internal controls to check and adjust their procedures in order to make then adequate for implementing obligations laid down by the Law. Obligors are required to conduct annual checks of how their systems and procedures are adjusted for implementation of the Law, and of the application of those procedures, as well as every time a change in the business process takes place, no later than the date when the change is introduced in the obligor's offer.

Obligors and their managements are responsible for securing and organising internal controls of jobs performed in the obligors in accordance with the Law**.** Obligors are required to define by internal regulation the powers and responsibilities of the management, organisational units, compliance officers and other entities in the obligor performing internal controls, and the manner and schedule of performing internal controls.

In respect of the size of the obligor, the framework of internal controls should:

- secure regular examination of the risk-management and risk-assessment process, taking into consideration the environment in which the obligors do business and activities on the market;
- provide an enhanced focus on the actions of obligors which are more liable to abuses by persons who launder money and other criminals;
- secure compliance with measures for the prevention of money laundering and terrorism financing and assess the programme;
- inform the managerial staff about initiatives on compliance, identified shortcomings in the compliance, corrective actions undertaken, and reports of suspicious transactions submitted;
- ensure continuity of the programme, notwithstanding changes in the managerial staff or the employee structure;
- focus on keeping prescribed records and the submission of requested reports, recommend compliance with measures for the suppression of money laundering and terrorism financing, and secure updating in accordance with regulations;
- implement customer due diligence policy, procedures and processes;
- make possible timely identification of transactions which are to be reported and ensure accurate drafting and submission of reports;
- secure appropriate monitoring of employees who manage money transactions to compile reports, monitor suspicious activities, or get involved in any activity aimed at actions for the

suppression of money laundering and terrorism financing;
- ensure that possible training be provided to all relevant employees.

Obligors are required to draft an annual report about performed internal controls and measures undertaken after those controls no later than 15 March of the current year for the preceding year and to deliver the report to the Administration and the Foreign Currency Inspectorate at their request, within three days after the request is submitted.

The Minister of Finance has laid down the manner of performing internal controls in the Regulation on the Methodology of Performing Activities in Accordance with the Law on the Prevention of Money Laundering and the Financing of Terrorism.

Keeping records, protection and keeping of data in those records

Obligors are required to keep records:
- about clients, as well as business relationships and transactions referred to in Article 9 of the Law;
- furnished to the Administration in accordance with Article 37 of the Law.

The content of the records about clients, business relationships and transactions is prescribed by Article 81 of the Law. Obligors are required to treat data they get as business secrets and to treat them in accordance with the Law, the law which regulates the confidentiality of data and the Administration's Regulation. All employees, as well as all other persons who have access to the data in any form, are required to maintain confidentiality of data.

The following are also deemed business secrets or confidential data according to the law (the obligor may not divulge them to a client or third party):
- data that reasons for suspecting money laundering or terrorism financing have been determined in connection with a party or transaction, and forwarded to the Administration;
- data about suspension of the execution of a transaction, and details in connection with the same;
- data about the order of the Administration for permanent monitoring of the operations of a client;
- data that in connection with a client or a third party an investigation in connection with money laundering or terrorism financing has been opened or could be instituted.

The obligation to preserve confidentiality of data does not exist if the data are needed for evidence in judicial proceedings, if the delivery of the data is requested in writing or ordered by the competent court, or if the data are requested from the obligor by the Supervisor, for the purpose of supervision of the application of the Law.

An exception from the principle of maintaining the confidentiality of data also exists when the obligor is under the Law required to submit the data to the Administration for the Prevention of Money Laundering, in which process the obligor's employees shall not be held liable for any damage to clients and third parties if they complied with the requests of the Administration, i.e., in cases listed in Article 75 of the Law.

Access to data, classified as business secrets or as secrets, must be restricted. Obligors must specify in an internal regulation in detail the conditions and manner of accessing the data, in which process the obligor must take into account the following instructions:

1. data and documentation should be stored in a manner and form preventing unauthorised persons from accessing them and learning their content (in appropriate technically or physically safe rooms for storage, in locked cabinets, etc.);
2. the right of insight into data on clients and transactions for which there exist reasons for suspicion of money laundering or terrorism financing, or knowledge about their content, is held by members of the management and supervisory boards of the obligor, the compliance officer for the prevention of money laundering and terrorism financing and his deputies, managers of the obligor's branches and other persons designated by the obligor's management;
3. it is prohibited to photocopy, copy, process, publish or in any other manner reproduce documentation containing the aforementioned data before a prior written authorisation of a responsible officer;
4. in case documentation is photocopied, the obligor must ensure that it is visible from the copy from which documentation or part of documentation the copy was made, specify in a visible spot that it is a photocopy and the number of photocopies made, the date when the photocopies were made, and the signature of the person who made them;
5. obligor's employees are required to conduct a short procedure of logging in and logging out their personal passwords at the start and the end of the processing of data, in order to prevent by the use of the passwords unauthorised access to documents;
6. a system of monitoring access to data and documentation and their processing must be established;
7. data may be transmitted only in a form which makes it impossible for unauthorised persons to learn about the data, either using the obligor's own courier service or sending in a sealed envelope by registered mail with confirmation of receipt, etc., and in case data are transmitted electronically, by using a secure electronic business system (data encryption, etc.);
8. obligor's employees are required to observe laws which regulate the security of personal data and laws which regulate confidentiality of data.

Obligors are required to keep data and documentation in connection with a client, established business relationship with a client and executed transaction, obtained in accordance with the Law, for a minimum of ten years from the date of the execution of the transaction, and data and documentation about the compliance officer, deputy compliance officer, professional training of employees and performed internal controls for at least five years from the date of the termination of duty of the compliance officer, the performance of the professional training or of the internal control.

Implementation of measures of detecting and preventing money laundering and terrorism financing in obligor branches and majority-owned subsidiaries located in foreign countries

The obligor is required to set up a system of conducting a uniform policy of detecting and preventing money laundering and terrorism financing in all obligor branches and majority-owned subsidiaries in foreign countries. To that end the obligor is required to ensure that the measures prescribed by the Law of detecting and preventing money laundering and terrorism financing in connection with customer due diligence actions and measures (client analysis), notification about suspicious transactions, keeping of records, internal controls, keeping of data and other important circumstances are implemented in the same measure in its branches and majority-owned subsidiaries abroad, except if it explicitly contravenes the regulations of that state, about which it is required to notify the management and to adopt appropriate measures for the elimination of the risk of money laundering and terrorism financing (Article 38 of the Law).

The obligor's management must ensure that:

- all the obligor's branches and majority-owned subsidiaries located in foreign countries are informed about the policy of detecting and preventing money laundering and terrorism financing;
- they build into their operational processes internal procedures of detecting and preventing money laundering and terrorism financing, adopted based on the Law, the Regulation and the Guidelines, through the managers of branches and majority-owned subsidiaries in foreign countries;
- they conduct constant supervision and ensure the efficiency of the measures of detecting and preventing money laundering and terrorism financing in all the branches and majority-owned subsidiaries in foreign countries.

Cooperation with the Supervisor and the Administration for the Prevention of Money Laundering

Within their legal obligations, obligors are required to ensure full co-operation with the supervisory authorities. Co-operation between obligors and the supervisory authorities is mandatory, especially in the case of submission of documentation, requested data and information relating to clients or transactions for which their exist reasons to suspect money laundering or terrorism financing. Co-operation is also necessary in the event of notification about any activity of circumstances which could be linked with money laundering or the financing of terrorism.