Republic of Serbia
MINISTRY OF FINANCE
Administration for the Prevention of Money Laundering

No: ON-000120-0001/2018
Belgrade, 7 September 2018

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT GUIDELINES FOR AUDITING COMPANIES, ENTREPRENEURS AND LEGAL ENTITIES PROVIDING ACCOUNTING SERVICES, AND FACTORING COMPANIES

Article 114 of the Law on the Prevention of Money Laundering and Terrorism Financing (Official Gazette of the Republic of Serbia, 113/17 of 17 December 2017 - hereinafter referred to as: AML/CFT Law) provides that supervisors can on their own or in cooperation with other authorities make recommendations, i.e. pass guidelines for the application of the AML/CFT Law.

The amended AML/CFT Law (Official Gazette of the Republic of Serbia, 20/09, 71/09 and 91/10) of 11 December 2010 first entrusted the APML to perform supervisory inspection of the compliance by auditing companies and accounting services providers with the AML/CT Law, whereas the AML/CFT Law of (Official Gazette of the Republic of Serbia, 113/17) of 17 December 2017 extended APML's supervisory powers to factoring companies.

Article 6 para 1 of the AML/CFT Law provides that the obliged entity must develop and regularly update an ML/TF risk analysis according to the Guidelines.

These Guidelines are published on the website of the Administration for the Prevention of Money Laundering (APML).

Obliged entities must align their internal acts with these Guidelines no later than three months from the date of entry into force of the AML/CFT Law.

Background

The 2009 AML/CFT Law align Serbia with international AML/CFT standards passed by the Financial Action Task Force (FATF) and the relevant EU *acquis*. It introduced *risk-based approach* to money laundering and terrorist financing to be applied by obliged entities on every client and business relationship. The 2017 AML/CFT Law has extended the risk assessment to the level of the obliged entity itself.

Countries must develop a national ML/TF risk assessment (NRA) and define measures and activities to mitigate the risks identified.

NRA findings provide useful information about financial institutions and DNFBPs, business organisations and independent professionals and support them in their own risk assessment at the level of the given institution to be performed by the obliged entity itself.

The risk assessment provides an answer to the question of which sectors and practices in a country's system pose a potentially higher risk of money laundering and terrorist financing, and in which ones the risk is lower, so that the state can adequately respond to the identified risks, by applying a range of measures and activities, and to make adequate decisions on the allocation of its resources in line with the assessed risks, with a view to investing more effort and resources into high-risk areas.

Development of national risk assessments of money laundering and terrorist financing, pursuant to the amended and revised FATF recommendations adopted in February 2012, constitutes an international standard.

Serbia developed a National Risk Assessment in 2018, and then a working group was established in 2018 to update the previous NRA.

The task of the Working Group has been to revisit and reassess the risks assessed by the comprehensive 2012 National Risk Assessment, using the World Bank methodology.

The time period taken into account for the 2018 risk assessments is considerably longer than for the previous risk assessment that took into account data for one year only. More specifically, the 2018 assessment collected data for the period from 1 January 2013 to 31 December 2017.

The 2018 NRA was carried out using the World Bank methodology which is divided in four thematically distinct sections:

1. assessment of ML threats;
2. ML vulnerability at the national level;
3. sectoral vulnerability;
4. terrorist financing risk assessment.

ML risk assessment is a result of an assessment of ML threats (which is among other things based on predicate criminal offences) and national ML vulnerability.

Based on the analysis of predicate offenses, a review of threats by sector and cross-border threats, the overall assessment of money laundering threats is "medium" with a "no change" tendency.

The national vulnerability to money laundering has been assessed as "medium" based on the analysis of the country's ability to defend itself against money laundering and on the sectoral vulnerability analysis.

An analysis carried out for the purpose of achieving the above stated objective for the Republic of Serbia has shown that the overall money laundering risk is "medium".

Predicate offenses classified as high-level threats for money laundering include: tax offenses, abuse of the position of the responsible person, abuse of office and illicit production and circulation of narcotic drugs.

The criminal offenses whose commission directly or indirectly generates proceeds were considered: first of all, criminal offenses against property, then crimes against the economy, against official duty, against human health, as well as other relevant criminal offenses. The final list included a total of 89 criminal offenses, potentially appearing as predicate offenses to money laundering.

The predicate offenses of the medium level of money laundering threat include illegal crossing of the state border and human smuggling, aggravated theft, robbery, fraud, extortion, illicit trade, corruption related offenses (taking bribes, giving bribes and trading in influence). These crimes are committed predominantly in order to obtain material gain.

Other offenses can be classified as **criminal offenses with a low level of ML threat**.

The largest number of predicate crimes has been committed in the home jurisdiction, which is why the threat is assessed as high.

Growing threats in terms of money laundering are cybercrimes, especially an e-mail business scam (BEC - Business E-mail Compromise) because they are targeting mostly business companies with significant financial resources, and through their commission high amounts of criminal proceeds are generated. Money flows are difficult to track down, especially if they are converted into crypto currencies, and their prosecution is also more difficult because the previous practice of the Special Prosecutor's Office for Cybercrimes in Serbia shows that more than 95% of these crimes were committed by an unknown perpetrator of a criminal offense that operated from abroad, at the expense of a domestic company, while the money transfer was channelled to a bank account in a third country which is neither the country of potential offense commission, nor the Republic of Serbia.

The **sectors** which are exposed to the money laundering threat the most are the sectors of real estate, the organization of games of chance and banking, followed by the sectors of exchange offices, casinos and accountants.

In the financial segment of the system, the most vulnerable institutions to the threats are banks, exchange offices and payment service providers.

The most vulnerable sectors in the nonfinancial segment of the system include the sectors of real estate, games of chance and accounting agencies.

[1]**Table 1. 1**

[1] Table 1. *Classification of exposure to the ML risk by sector*

Sector	Level of threat
Real Estate	High
Games of chance	High
Banks	High
Currency exchange offices	Medium high
Casinos	Medium high
Accountants	Medium high
Lawyers	Medium
Payment institutions	Medium
Capital market	Medium low
Auditors	Medium low
Leasing	Medium low
Notaries	Low
Factoring	Low
Insurance companies	Low
Pension funds	Low

The sectors exposed to a high level of ML threat are the real estate, games of chance and banking sectors. They are followed by exchange offices, casinos and accountants that are exposed to medium-high level threat. Lawyers and payment institutions are exposed to a medium-level ML risk. Capital market, auditors and leasing sectors are exposed to a medium-low level of exposure. The lowest level of exposure - identified as 'low' characterises the following three sectors notaries, factoring and insurance companies.

In assessing cross-border money laundering threats, 152 countries were analysed. Based on the analyses performed, 8 countries are assessed as those with high-level money laundering threats, 7 countries are classified into the category of medium-level threats, while 12 countries are classified into the category of low-level money laundering threat.

Assessment of AML/CFT system vulnerabilities. Based on the collected data and information, examined in the light of money laundering threats, the national combating ability has been rated as 'medium'.
This ability has been analyzed through the quality of the strategic framework, the comprehensiveness of the normative framework, the effectiveness of law enforcement, capacities, resources, independence and integrity of the key participants in the system for the prevention and repression, the effectiveness of internal and international cooperation, as well as through the level of financial integrity, formalization of the economy in the country and other relevant parameters. A comprehensive analysis of money laundering threats is the first step in assessing the risk of money laundering for the country. In light of the results obtained by this analysis, it is necessary to review and assess the national vulnerability, since risk is a function of threats and vulnerabilities. Thus, the assessment of national vulnerability to money laundering constitutes the next step on the road to the national money laundering risk assessment. The overall assessment of national vulnerability is based on an assessment of the country's ability to defend itself against threats, and sector vulnerabilities.

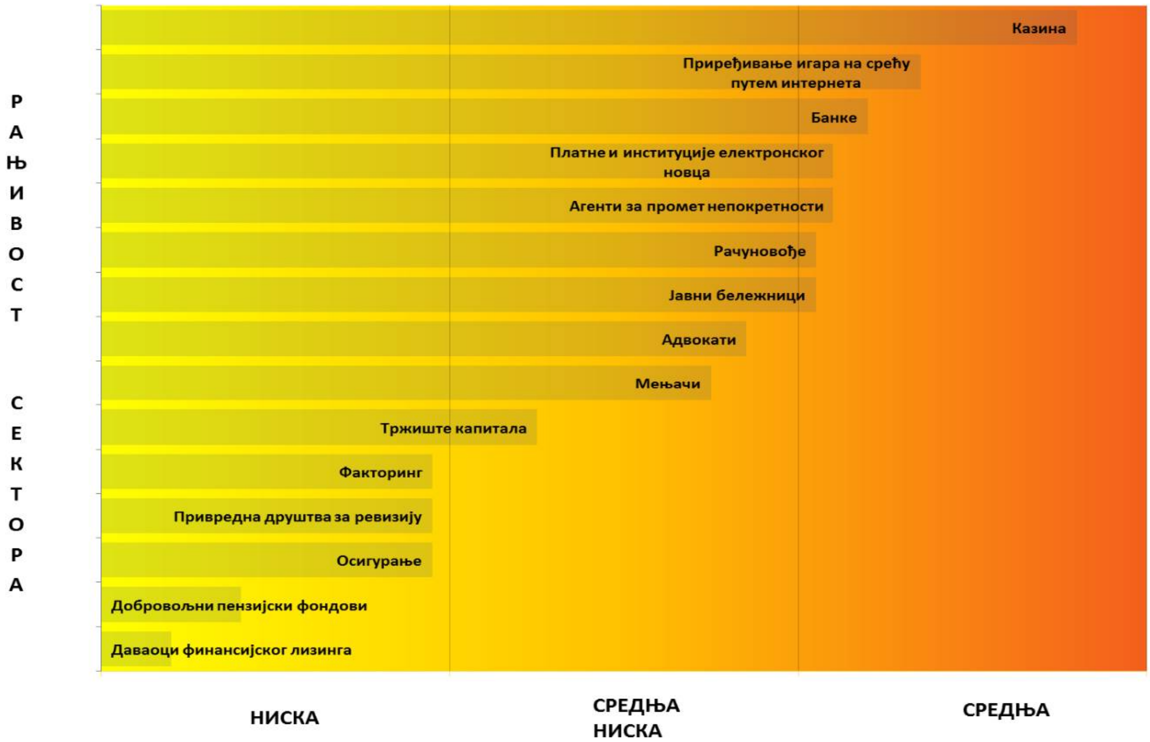
Sectoral vulnerability. As the vulnerability of certain sectors that can be misused for money laundering also affects national vulnerability, as well as the country's combating ability, both the financial and non-financial segments of the AML/CFT system have been analysed.
The sectoral risk analysis was undoubtedly important for the risk assessment. A great deal of attention was focused on data processing and the analysis of both the financial and non-financial systems of the Republic of Serbia. The assessments of vulnerabilities for sectors should not be understood in absolute terms, i.e., that certain sectors are vulnerable or not vulnerable, but in terms of lower or higher vulnerability compared to other sectors. For example, certain indicators and features of the banking system suggest that banks, compared to other sectors, are more vulnerable when it comes to money laundering and financing of terrorism, but that certainly does not mean that the banking sector is vulnerable in absolute terms.

The financial sector of the Republic of Serbia consists of the sectors of banking, insurance, financial leasing providers, voluntary pension funds, other providers of payment services and issuers of electronic money - payment and electronic money institutions, capital markets (broker - dealer companies, authorized banks, investment fund management companies and custody banks), authorized exchange offices and factoring.
The most vulnerable sector in the financial segment of the system is the banking sector, followed by payment service providers and the securities sector.

The DNFBP sector of the Republic of Serbia includes reporting entities under the Law on the Prevention of Money Laundering and Financing of Terrorism, which are intermediaries in real estate sale and lease, organizers of games of chance via the internet, casinos, then the so-called "gatekeepers" that include auditors, accountants, lawyers and notaries public. Also, the DNFBP segment includes developers in the business of building residential and non-residential

buildings, dealers in items made of precious metals, car dealers, which are not reporting entities under this Law.
Compared to other sectors, the real estate sector has been identified as the most vulnerable among the DNFBPs, followed by the games of chance sector and accountants. From the standpoint of money laundering, too, these sectors pose a higher risk.

Vulnerability assessment by sector in tabular form



The sector of accountants is also exposed to a medium-high money laundering threat.
Accountants belong to a sector that is assessed as a medium vulnerability sector compared to other DNFBPs, and whose exposure to money laundering threats, according to the assessment, is medium-high. In this area, progress has been made relative to the 2012 National Risk Assessment, primarily by introducing the obligation for accountants to be registered for this activity in order to be able to perform it (the main business). It is also prescribed that an entrepreneur that has registered the provision of accounting services as a core activity may not be a person who has been convicted by a final and binding judgment of criminal offenses laid down by this Law (including the criminal offenses of money laundering and the financing of terrorism).
In 2012, a unit for supervision of accountants and auditors was established in the Administration for the Prevention of Money Laundering, and supervision is carried out through both off-site and on-site examinations. In most of the on-site examinations of accountants, instances of non-compliance with the Law on the Prevention of Money Laundering and Financing of Terrorism were identified, and afterwards complaints were filed for economic offenses with positive outcomes, in the sense that the Commercial Court found that an

accountant failed to abide by the law and imposed a fine. A large number of training events has also been held in the recent period. The trend is that accountants registered as legal entities have a higher level of awareness about belonging to the anti-money laundering system, than entrepreneurs. Also, recent years have seen a rising trend in the number of accountants. Accountants still perceive certain legal norms, which are derived from international standards, as formalities. Some companies involved in criminal activities used the services of accounting agencies to disguise their criminal actions so that they appear to be legitimate business operations. This is especially true for money laundering cases involving the laundering of proceeds from tax offenses.

Also, there are a number of accountants who continue to question the reporting of any suspicious transaction to the APML. This confirms the opinion that the accountants' awareness of belonging to the AML/CFT system is at an insufficiently high level and that more intensive preventive work is required with accountants.

Auditing companies belong to a sector that is assessed as a low vulnerability sector compared to other DNFBPs, whose exposure to money laundering, according to the assessment, is medium-low. In making the vulnerability assessment for auditors, the following was taken into account: a good licensing regime for the operation of audit firms, the fact that auditors have to have a license to be able to work, and that they may not be convicted of offenses against rights arising from labour, the economy, property, the judiciary, money laundering, financing of terrorism, public order and peace, etc. Auditors have a high level of awareness of belonging to the anti-money laundering and terrorist financing system, and according to the evaluation of the quality of suspicious transaction reports made by the APML, auditors received the highest rating for the quality of suspicious transaction reports in relation to all reporting entities under the Law.

It merits mentioning that based on the analyzed data from the prosecuted cases, in terms of the organizational form, the highest amount of "dirty money" went through business entities having the structure of limited liability companies. The analysis of the prosecuted cases indicates that the most vulnerable are small businesses, and that the threat of money laundering is much higher for them than for other types of organizational structures.

Limited liability companies are rated as a high-level threat, entrepreneurs as a medium-high threat, joint-stock companies are rated as medium-level threats and other forms (limited partnerships and partnerships) as low-level threats. Among these companies there were no trusts as founders, which, also according to the data of the reporting entities (banks), account for less than 5% of the structure of clients’ founders.

The **assessment of the terrorist financing risk** at the national level was made by considering terrorism threats, the impact on the terrorist financing threat, terrorist financing threats, and the vulnerability to terrorist financing, within which, among other things, the NPO sector has been analyzed from the point of view of its terrorist financing vulnerability.

The new TF risk assessment, unlike the previous one, was conducted using the World Bank methodology, it covered the period 2013 -2017, and it is more comprehensive than the previous TF NRA.

By assessing the overall parameters and statistical data used to assess the criteria ‘Terrorism Threat’, ‘Terrorist Financing Threat’ and ‘Terrorist Financing Vulnerability’, the Working Group has made the assessment that the level of the ‘Terrorist Financing Risk’ in the Republic of Serbia is ‘medium’.

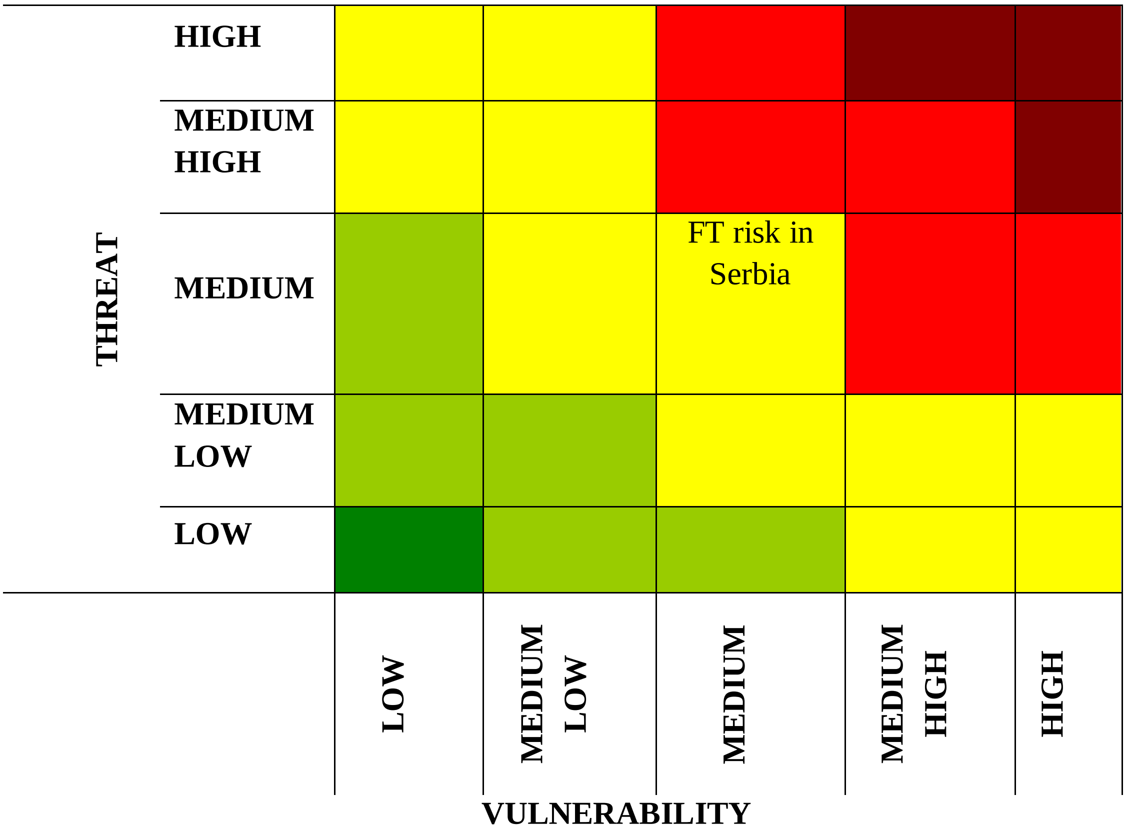


Figure 1. Terrorist Financing Risk in the Republic of Serbia

Based on the analysis of quantitative data, which is mainly related to the recent case, and of qualitative data, the Working Group has made an assessment that the factor ‘Terrorism Threat’ is ‘medium/high’, while the factor ‘Impact on the Terrorist Financing Threat’ in the Republic of Serbia is assessed as ‘low’.
Also, by analyzing the mentioned quantitative and qualitative data, the level of the ‘Terrorist Financing Threat’ has been rated as ‘medium’ with a ‘no change’ tendency.

Bearing in mind the analyzed factors, the ‘Terrorist Financing Vulnerability’ has been assessed as ‘medium’.

Consequences for the system

The assessment of the risk of money laundering and terrorist financing, in addition to the threat and vulnerability assessments, includes the assessment of consequences for the system. They should be understood as the harm that money laundering could cause and include the impact of criminal activity on a reporting entity, the financial system, society and the economy as a whole.
Bearing in mind that threats and vulnerability are assessed as medium, the consequences for the system should therefore be rated at the same level.

The largest and most serious negative effects of money laundering can be first seen in the economy, through a decline in public revenue, transparency and efficiency of the financial system, the expansion of the "gray economy". Its size in Serbia at this point is not at a satisfactorily low level, so any increase would give rise to negative effects across the entire economic and financial system. Money laundering, as a rule, leads to a decrease in budget revenues due to tax avoidance. It is one of the most common unlawful incomes that is the subject of money laundering.

The conclusion is that the problem of money laundering must be approached as a complex phenomenon in order to avoid its negative effects. The "route" of dirty money is not easy to spot or identify, which impedes the timely implementation of efficient measures for its detection, prevention and suppression. Money laundering is getting new forms every day, through the use of various methods and means.
Creating an efficient system for countering this problem requires improvement of the normative framework with solid mechanisms and clear roles of each of the institutions, both those that operate preventively, and those that act repressively.

In order to pre-empt the consequences of terrorist financing, it is necessary to maintain the efficient capacity of the system to prevent and combat terrorism and terrorist financing, make an analysis of the legislative framework regarding the efficiency of certain legal arrangements and their implementation, continuously promote and advance capacity of human resources, and renew technical capacities of the so-called repressive authorities (police, prosecution, security services) and the so-called administrative and preventive authorities (different organisational units of the Ministry of Finance – Administration for the Prevention of Money Laundering, Customs Administration, Tax Administration) to counter terrorist financing, and work to raise awareness about the threat of terrorism and all its manifestations, and exposure to the terrorism risk of the so-called vulnerable categories of persons and organizations.

The national risk assessment envisages that the next step after making the risk assessment is the adoption of an Action Plan defining all activities that constitute the state's adequate response to the identified threats and vulnerabilities of sectors and the national system.

Action plan

The NRA Action Plan notes that the legal provisions governing AML/CFT supervision of accountants is inadequate and that the relevant legislative framework should be analysed through a comparative analysis and overview of the relevant provisions in other countries (through good practice examples).

In addition, the NRA Action Plan notes that there is a lack of human resources in the APML to carry out supervision of accountants, auditors and factoring firms, and that these resources should be strengthened by recruiting additional staff and training so that they acquire competences to check compliance with the AML/CFT Law.

It also highlights high staff turnover as an issue.

Finally, the NRA Action Plan notes there is an insufficient number of onsite inspections of accountants and that a continuous offsite and onsite inspections of accountants should be carried out by intensifying the inspections (distributing questionnaires) and carrying out onsite inspection based on the risk matrix.

Guidelines do not set out a manner or methodology or the right sequence of steps for the obliged entity as to how to conduct the internal risk assessment. Research, both those at the national and international level, only help the obliged entity to better understand risks and give them an idea of specific actions to be carried out; yet there are no uniform instructions to be followed by the obliged entity.

Guidelines in no way explain how the authorities should assess the risk in the context of supervision or what in an obliged entity's risk assessment document can be considered accurate or inaccurate. It is recommended that the supervisor departs from the national risk assessment, and the obliged entities must understand and apply the risks found at national level.

It is key that the risk analysis and assessment process results in overall understanding of why ML or TF occur at all. A most general answer to this would that they should lead to 'legalisation' of crime and terrorism. Profit is essential for most criminal groups and criminals are investing serious efforts to move illicit proceeds or other assets and disguise the true nature and sources of funds they handle.

For terrorists to carry out their operations, organise attacks or maintain infrastructure of their units and chains of command, they need funds and these funds need to be moved to and from various areas.

Both for criminals and terrorists, the crucial thing is the possibility to use the assets.

On one hand, it is important to reveal sources of funds, assets they use, and then analyse the consequences of operations of crime groups and terrorists, assess certain risk situations so as to attempt in future to respond on time to these risks, to prevent them if possible, or at least mitigate them.

Money laundering and terrorism financing

Money laundering and terrorism financing are global issues that may have a negative impact on the economic, political, security and social structure of a country. ML and TF undermine stability, transparency and efficiency of the country's financially system, they cause economic disruptions and instability, damage the country's reputation and jeopardise national security. ML/TF risks occur also because of failure to comply with regulations, where the obliged entities can also be exposed to a significant extent to the reputational risk in case of supervisors' penalties.

In money laundering, the initial assets always derives from illicit activities, whereas in terrorist financing the sources can be both legitimate and illegitimate. Still, the main objective of terrorist financiers does not necessarily have to be concealing the sources of their assets but concealment of the nature of the financed activity. When individuals wish to invest funds generated in legitimate activities to financing of terrorist activities, the funds are more difficult to detect and trace, as the transactions are made in smaller amounts.

An efficient AML/CFT system must analyse both these risks.

Money laundering - definition and stages

There are numerous definitions of money laundering but regardless of how diverse they are, whether they are simple such as: legalisation of illegal proceeds, or complex, such as those defined in the Warsaw Convention as[2] and implemented in the Serbian Criminal Code[3], all professionals and practitioners agree about the following:

Money laundering is a process to conceal illegal origin of money or property acquired through crime.

Money laundering within the meaning of the AML/CFT Law means conversion or transfer of property acquired through the commission of a criminal offence; concealment or misrepresentation of the true nature, source, location, movement, disposition, ownership of or rights with respect to the property acquired through the commission of a criminal offence.

---

[2]the conversion or transfer of property, knowing that such property is proceeds, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his actions; the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is proceeds;

[3] The definition of money laundering contained in the provision of Article 245 of the Criminal Code is based on the approach that all criminal offenses can be predicate offenses and criminalizes both "self-laundering" and "laundering money for somebody else." The above amendments stipulate that the property that is the subject of the criminal offense of money laundering originates from "criminal activity ", instead of the earlier provision in force that such property originates from a "criminal offense", which is a more comprehensive description of the origin of such property, which does not require the provision of detailed information on a particular predicate offense in which the property was acquired, thus facilitating the prosecution and presentation of evidence.

Where property gain is acquired through commission of a crime, the perpetrator seeks ways to use the money so as not to attract attention of the competent authorities. Therefore they carry out a series of transactions serving to make the money appear as legitimate. Money laundering has three main stages:

1. **Stage I**: placement, means the disruption of the direct link between the funds and the illicit activity through which it was acquired. At this stage, the illegal proceeds are placed into the financial system. The money is placed into bank accounts, most frequently through a legal activity where payments are carried out in cash. One of the ways is to found a fictitious company that has no business activities but only serves to deposit the dirty money, or structuring (smurfing) large sums of money and then its depositing to bank accounts in amounts that are not suspicious and therefore not subject to the reporting requirement.
2. **Stage II**: layering or concealment. After the money was placed in the legitimate financial system, it is then moved from the account to other accounts, held by companies, with the aim to make it appear in some fictitious business activities or to carry out a legitimate business (trade or service) with companies operating in a legitimate way. The main objective of these transactions is to conceal the link between the money and the original criminal activity.
3. **Stage III**: integration. Dirty money appears as money originating from an allowed activity. A frequent method of integration fo dirty money into legal financial flows is through purchase of real estate or control packages of shares in joint-stock companies which is an example of concentration of dirty capital of large proportions, which is exactly the aim of money launderers. Integration focuses on market value, i.e. to what can be bought and traded. Renting real estate is legitimate, and the revenue from rent is not suspicious. Funds are frequently also invested in companies with difficulties in their business operations, and then they continue working successfully while the business outcomes constitute legitimate proceeds. When dirty money arrives at this stage it is very difficult to detect its illicit origin.

Illegal acquisition of property is the main, if not the only, driver for organise commission of offences. In order to enjoy the benefits acquired through crime, the proceeds must be disguised so that they look legitimate.

The 2018 NRA found that dirty money in Serbia is most often "laundered" by transferring money whose cover are fictitious legal transactions between legal entities that have been established for a specified purpose - to be used for performing such transactions, that is, money laundering through purchases of real properties and motor vehicles, investment in the purchase, construction and renovation of buildings – the construction industry, the purchase of legal entities, securities. What can be distinguished as characteristic of the Republic of Serbia compared to the countries of Western Europe is the investing of "dirty" money in the privatization of former socially-owned enterprises, which often represents a mere starting point of money laundering.

After the transfer of the ownership or control of such a company to the criminals, illicit funds are laundered through its activity, usually through loans of the new owners-founders or other forms of borrowing aimed at preserving the illusion of operation within the boundaries of the registered activity. At the end, money is usually "laundered" either by selling these legal entities, or by taking out a loan for which the assets of that legal entity are provided as collateral, or from the profit of that legal entity that is higher because of the costs that have been covered out of the dirty money.
Recently, a form of money laundering has been identified, which is performed through a large number of legal entities, most of which were opened specifically for this purpose. In these cases, without a real business relationship, business documents of untrue contents are created, which serve as a basis for monetary transactions. After money has been transferred based on false and fake documents, money is withdrawn in the country and abroad by various persons and returned to the payers in cash, reduced by the percentage charged for the service.

Terrorist financing

Definition and stages

For the purposes of the AML/CFT Law, terrorism financing is defined as providing or collecting of property, or an attempt to do so, with the intention of using it, or in the knowledge that it may be used, in full or in part:

1) in order to carry out a terrorist act;
2) by terrorists;
3) 3) by terrorist organizations.

Terrorism financing means aiding and abetting in the provision or collection of property, regardless of whether a terrorist act was committed or whether property was used for the commission of the terrorist act.

Terrorist financing constitutes a special form of financial crime. The main aim of individuals and organisations involved in terrorist financing does not necessarily have to be concealing the sources of funds but the main intention is actually to conceal the nature of the activity for which financing these funds are intended. Terrorists use a wide range of various methods to transfer funds so that they could cover the needs of their organisations and activities, which includes the financial sector services, cash transfer, trade, donations and charity, as well as formal and informal money laundering systems.

Funds intended for terrorist financing may originate from legitimate sources such as donations, funds acquired through legitimate operations, charity as well as illicit sources such as trafficking of drugs, arms, gold and diamonds, or embezzlement kidnapping, extortion, etc.

There are four stages in terrorist financing:

1. raising of funds from legitimate operations or from criminal activities;
2. keeping of funds raised;
3. transfer of funds to terrorists;
4. use of funds;

The first stage entails raising of funds from persons operating in a legitimate manner, but are linked to a terrorist organisation or terrorists, or from persons linked to criminal activities, e.g. drugs trafficking, extortion, embezzlement, etc. A major source of funds are also donations by individuals supporting the objectives of terrorist organisations or funds raising funds and directing them to terrorist organisations.

In the second stage, the funds are kept, i.e. held either directly in bank accounts of individuals or accounts of intermediaries - individuals also linked to terrorist organisations.

The third stage involves transfer of funds to a terrorist organisation's cells or individuals terrorist so as to use the funds for terrorist activities. The funds is most frequently transferred through the money service and banking systems, even though informal money remittance systems are also widely used.

The use of funds becomes obvious when it is used for terrorist activities, e.g. purchase of explosives, weapons, equipment, training camp financing, propaganda, political support, provision of shelter, etc.

The aim of these guidelines

The **aim** of these Guidelines is to provide a basis and/or preconditions based on which a general ML/TF risk assessment with respect to obliged entities' operations, and the way of carrying out an analysis/assessment in individual cases, i.e. at the level of the individual with whom the business cooperation is being established (client, associate, contracting party, etc.)
Each institution, regardless of its size or complexity, must develop an appropriate system to manage the risk of money laundering and terrorism financing.

The system must ensure that the risks are identified, assessed, monitored, mitigated and managed in a comprehensive manner.

FATF Recommendation concerning the requirement to assess risks at various levels - level of the sector (supervision) - level of the institution (obliged entity) - level of client

The main requirement of FATF recommendations is the risk based approach, especially under Recommendation 1, but this approach permeates many other recommendations and it is essential for the application of other recommendations (e.g. recommendations 10, 26, 28 etc. are indirectly related to this issue).

Countries should require the financial institutions and DNFBPs to establish, assess and undertake effective measures to mitigate their ML/TF risks.

The recommendations also require that financial institutions and DNFBPs must be able and willing to identify and assess ML/TF risks and to respond effectively to mitigate them.

Supervisory authorities and risk assessment

Recommendation 1 calls upon supervisors to review and assess the risks assessed by Fis and DNFBPs and to take into account the national risk assessment outcomes when conducting supervision.

Supervisory authorities should ensure that obliged entities effectively apply the risks - requirements - to analyse ML/TF risks at the national level and at the level of the specific sector and to act accordingly. In addition, supervision should establish whether obliged entities do profiling of some other risks at the level of the specific obliged entity itself, which is recognised by the institution itself, but which may have remained insufficiently researched in the course of the national risk assessment so that the system could respond on time and adequately to the new risks. When updating risk assessments, the supervisor should take into account the results of such analyses too.

The country should require the financial and non-financial segment of th system to take certain measures, i.e. to identify, assess and mitigate the risks.

Risk assessment is developed at all levels:

1. at the level of the country 2. supervision 3. sector 4. obliged entity 5. client

In order to apply the risk based approach supervisors and obliged entities should first of all understand the ML and TF risks that are characteristic of their business operations by identifying and assessing possible risks. Thus, a risk assessment is the first step that an obliged entity should take before establishing and developing measures for ML/TF control and prevention so as ensure that these measures are commensurate to the nature and volume of activities it engages in. Obliged entities should establish internal policy, system of control and procedures that will enable them to manage the risks identified and mitigate them. When assessing risk, the obliged entities should take into account all relevant risk factors before ultimately establishing the level of overall risk and identify on that ground the measures to be taken. Obliged entities can apply these measures to various extent, depending on the type and level of risk.

The risk analysis should contain a risk assessment for each group or type of customer, business relationship, service offered by the obliged entity within its business.

Risk at the level of obliged entity and at the level of client

Obliged entities and risk assessment

Obliged entities should be required to take appropriate steps to recognise and assess ML/TF risks that they face: towards clients, geographical areas, products services, channels or methods of establishment of business relationships, or service provision or sale of products, transactions, etc.

Obliged entities need to document their risk assessments and to make them available at the request of the relevant authority.

The nature and scope of any risk assessment should be commensurate with the assessed risk of the country, size of the sector, etc. This means that risk assessments will be different, in terms of volume and quantity of data, for a bank and for an accountant, for instance. A bank which may have thousands of clients will certainly have to take a more comprehensive and detailed risk assessment as the scope of products offered by a banking institution much wider than that of an accountant who may only do calculations of salaries for his/her clients who are no more than twenty.

It should be noted that risks researched must take into account sectoral differences and that every risk assessment should contain a proposal for measures and actions to mitigate the specific risks.

Risk assessment - definition

In order for the obliged entity to learn about risk assessments and about main factors of risk, they should learn about and understand the key terminology that is very often used in this area.

It is important first of all to define risk itself.

Three factors have an effect on risk assessment: threat from an event, vulnerability of the system and consequences of occurrence of an event.

Ideally, a risk assessment is a judgment of threats, vulnerabilities and consequences.

A threat can be one person or a group of persons, an object or activity which have the potential to cause damage, e.g. to cause damage to the obliged entity's institution, business operations, reputation. For instance, they could be clients recognised or suspected in some way to be linked to illegal activities, or suspected/identified fraud, forged documents and similar situations.

Threat serves as a point of departure for a risk analysis. That is why it is important also to asses the environment in which proceeds from crime are generated and where criminal offences are committed. An obliged entity must take into account the findings of the NRA and check how the environment and risk crimes impact their business, to which volume and extent was the obliged entity exposed to certain crimes. All other analyses of certain threats are useful, e.g. typologies and trends recognised in reports of the APML or supervisory authority, etc.

In the 2018 National Risk Assessment, threat is defined as a person or a group of persons, objects or activities that have the potential to cause harm, for example, to the country, society, the economy, etc. In the context of money laundering, this implies criminals, assets at their disposal, the environment in which predicate offenses are committed and in which criminal proceeds are generated, their size and amount.

Vulnerability, as used in risk assessment includes all those things that could be used in the event of threat or that could support or facilitate the effect of a threat. The aim is to focus on the factors that constitute weaknesses in the system for the prevention of money laundering and financing of terrorism, and the supervision system. If we talk about an obliged entity, vulnerability means all the things that makes an institution particularly exposed to money laundering or terrorist financing (lack of knowledge of legislation regulating this area, inadequate compliance with the legislation, inadequate training, complex or inadequate organisational structure of the obliged entity, unclear requirements in the process etc.).

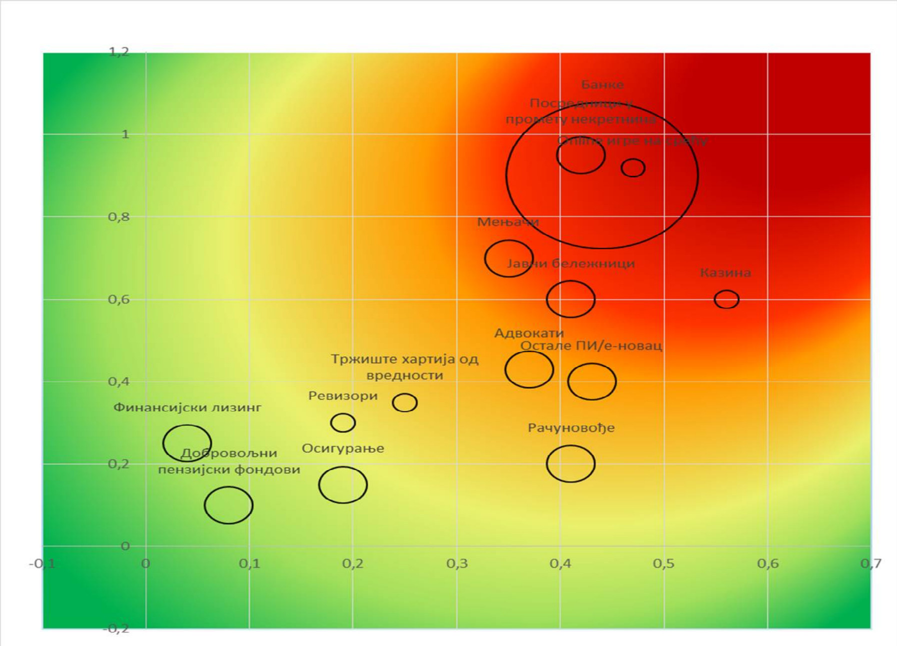
Consequence means the effect or damage that money laundering or terrorist financing may inflict or cause and includes the influence of a criminal or terrorist activity underlying such an activity on financial systems and institutions and more widely on the society and economy as a whole. Consequences can be short-term or long-term in nature. Consequences have an effect on reputation and attractiveness of the financial or non-financial sector of a country. A consequence could be measured by the amount of a sanction imposed against a certain financial or non-financial institution for failure to adequately confront the risks, or by the level of tarnished reputation of an obliged entity found to be supporting money laundering by inadequate analysis of risk and measures to mitigate it.

Relevant terms and key definitions for risk assessment

In a risk analysis, the key is to adopt an approach to make a difference between the levels of various risks so as to facilitate setting of priorities on which to focus attention and resources, at the national level and at the level of obliged entity and risk assessed at the level of the specific institution.

In order for the obliged entity to develop their own risk assessment, they need to be aware of the existence and take into account the National risk Assessment. In this context, the obliged entity should, when conducting a self-assessment, take into account the level of risk to which the obliged entity itself was classified in the National Risk Assessment.

A money laundering risk assessment map by sector



Assessment of the ML/TF risk in relation to the obliged entity's business operations

Risk identification

In order to establish the exposure of an obliged entity to the ML/TF risk, the obliged entity must know every segment of their operation where Ml/TF threat can emerge, i.e. they must assess the vulnerability with regard to the threat. Risks should be identified at all levels of management - starting from the operational level to the level of top management, and all organisational units, if more of them exist, should be involved in the process. The size and complexity of the obliged entity's operations plays an important role in establishing the obliged entity's vulnerability. For instance, in large systems, such as the banking system, employees may be less familiar with client behaviour than in the case of, for instance, accounting agencies providing services to a limited number of clients.

Exposure to risk

The obliged entity assesses the exposure to the ML/TF risk, i.e. the level of probability for a negative effect that stems from the risk, as well as the effect of the risk to the aims of business operation.

Risk identification and analysis

ML/TF risk assessment starts from the assumption that various products and services offered by obliged entities in their business or various transactions they conduct, are not all equally vulnerable to misuse by criminals. A risk assessment is made to ensure that control measures commensurate to the identified risk by applied. This allows to the obliged entities to focus on those clients, countries, products, services, transactions, way of doing business, that represent potentially highest risk.

Risk assessments stages are as follows:

1) identification of the areas of business that are exposed to money laundering and terrorist financing

This stage includes identification of clients, products, services, transactions and geographical areas that are specific for the obliged entity and client. The ML/TF risk and vulnerability to exposure will vary depending on the characteristics of clients, products, services, transactions and forms of business operations.

2) conducting an analysis with the aim of establishing the probability of ML/TF and impact

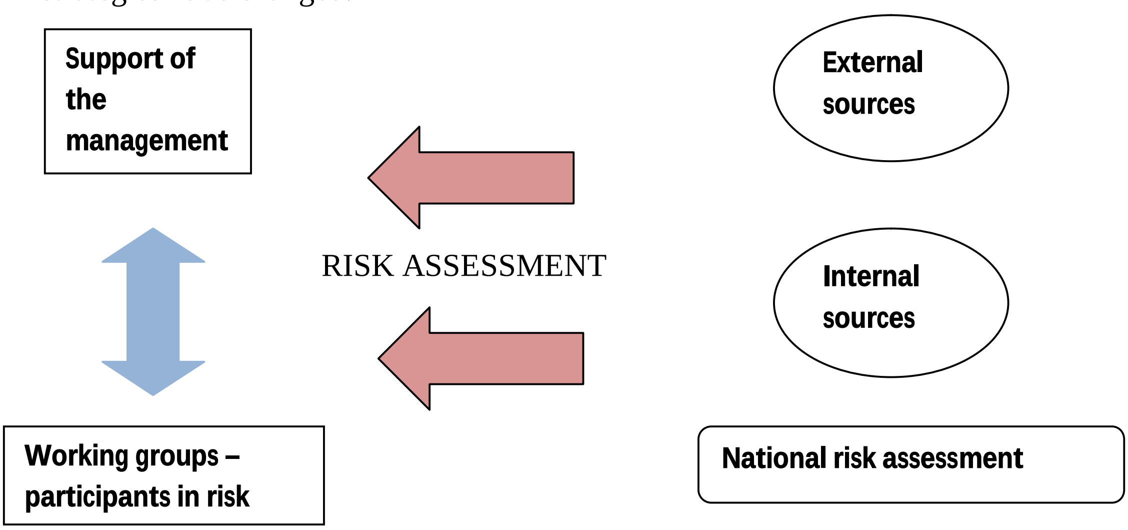
Risks faced by the obliged entity should be analysed, i.e. analysis of likelihood that a certain phenomenon will occur and assessment of negative effects of the occurrence. There should be an assessment of the reputational risk for the obliged entity or beyond - for the sector itself. The analysis of risk categories is specific for each individual obliged entity, so the conclusion concerning the overall level of risk must be based on relevant information.

3) risk management

Based on the risk analysis, a risk management strategy will be applied and an appropriate business policy established, i.e. an appropriate procedure will be apply. In order to mitigate or eliminate risk, adequate control mechanisms are also applied.

4) risk monitoring and update

The last stage entails review of risks. The obliged entity an do this through its internal supervision system. Risk assessment must be periodically updated in order to establish whether risks have changed and to what extent have the forms of obliged entity's business operations or strategies have changed.



RISK ASSESSMENT

Decision concerning the risk assessment

When making a decision concerning a risk assessment, the obliged entity should decide whether it will assess ML and TF risks together or separately, and depending on the decision taken it will adjust its work methodology and volume of data to be collected.

Factors taken into account in a ML risk assessment can be significantly different from the factors considered in the TF risk assessment. For instance, transactions linked to TF are much lower in amount and sporadic compared to ML transactions.

Ideally, the obliged entity's risk assessment picture should provide a comprehensive overview of potential threats and vulnerabilities and potential consequences and be sufficient in width and depth. The picture should provide an answer to the question how the national risks are reflected in the specific obliged entity as well as whether the obliged entity identified some new risks. In addition, the assessment can be followed by a plan of action to eliminate or mitigate the risks.

A risk assessment can consist of various types of assessment and various approaches can be combined, as well as methodologies, research of various sectors, in order to get a risk assessment picture at the level of obliged entity. Those assessing the obliged entity’s risk can also take into account in addition to the risks at national level research done by competent authorities, findings of previous inspections, analyses of regulators, results of supervision, analysis of performance of certain sectors, typologies, etc. By combining all available sources, the obliged entity assesses to which risks it is exposed the most and makes a conclusion as to the factors having an effect on the vulnerability of the institution conducting the assessment.

The important thing in this process is that top management is willing to complete this job and to support the process.

Organisation and information

Planning and organisation of the process is very important for the ultimate result of the risk assessment. At the outset of the process, certain issues should be addressed. The issues of whether for instance the document will be drafted only by persons involved in AML/CFT or staff in other organisational units linked to this process will also be part of the team, the team can be joined by persons establishing a business relationship with the obliged entity etc.

It may be a good idea to make a hierarchical concept in terms of what departments can most of all contribute reducing certain risks from placement of dirty money, and then list those segments of the institution that do not have an impact on the risks. In this way it will find the right concept for developing the document and designate the optimum number of persons.

It is not the same if the obliged entity has 1000 or 10 employees. It is natural that in situations where we have a diversified organisational structure a large number of branches or subsidiaries, a larger number of persons should be involved in the process than in a situation where that number of employees is fewer and there is no need to extend the working team.

The key question is who can contribute to the risk assessment. In large systems, it is not very likely that an organisational unit will have all the information required for an adequate risk assessment. That is why at the outset of the process, the segments of the obliged entity's system that may have essential information for the risk assessment should be indentified, i.e. the sectors that can recognise certain system vulnerabilities and help reduce threats.

In addition to the obliged entity's organisational units that may have relevant information for the risk assessment, one should also take into account so-called external information sources, such as for instance feedback information that the obliged entity receives concerning its suspicious transaction reports, information about typologies and trends, findings of both internal and external audits, research of international institutions such as the Council of Europe, OSCE, FATF, etc. A key document for the obliged entity, if not the most important one, is the national risk assessment.

For instance, to recognise certain organised crime group *modi operandi* and potential risk countries, or potentially risk countries, one can make use of SOCTA (Serious Organised Crime Threat Assessment) reports made by Europol, as well as EU member states and the countries in the EU accession process that are required to apply such reports, OCG-based ML typologies, research related to internet fraud4 etc. Obliged entities can also find useful information on:

http://www.eurasiangroup.org/MONEYVAL_typologies_eng.php ;
https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment;
https://rm.coe.int/typologies-report-on-laundering-the-proceeds-of-organised-crime/168071509d

Methodology

At the outset of the process it is important to decide about the methodology to be applied and describe it in short. This means that the obliged entity needs to determine what organisational units will be part of the process, how the data will be collected, who will coordinate the process (this will presumably be the compliance officer or its deputy), what data will be used, when the process will start etc. First of all, a risk assessment must be based on objective data and valid sources of information. It can be complemented with examples from the media, but the it should start from the findings of national risk assessment and it should be regularly consulted in the course of development of the document.

Methodology means that the obliged entity should at the beginning decide on the techniques to be used in the development of the document, the way they will be selected and processed, volume of information and the type of information to be used.

[4]A large number of reports an be found on the APML website, Typologies section

The one who reads the obliged entity's assessment document should have a clear picture as to how the obliged entity assessed certain risks at the institution level, how NRA risks were implemented in the process, and be given an overview of clear measures that the obliged entity intends to implement based on the findings.

It should be noted here that the volume of information to be used by obliged entities will vary, i.e. in some obliged entities for instance it will not be necessary to consider the influence of international settings and certain cross-border factors whereas for some obliged entities this may be more useful. For instance, in situations where obliged entities belong to a group and certain group-wide requirements dictate the way they will act, or where there are a large number of subsidiaries in a number of countries, or where certain negative circumstances or characteristics may be indirectly transferred to the domestic framework.

Risk assessment stages

As mentioned above, at the beginning it is useful to describe the methodology to be used and how the document will be produced. The risk assessment procedure can be dividided to a whole range of activities, but the main stages of the process are identification, analysis and evaluation - implementation of findings.

Risk identification

Identification starts when a risk is recognised. It would be useful to draw up a list of potential factors to be used to recognise ML/TF threats and vulnerabilities in the obliged entity. The list should include those factors that were recognised as risk factors at the national level if they are specific to the obliged entity. The idea is to draw up a comprehensive list of risk factors - risk-posing products, transactions, services, clients etc. For instance, if companies from a certain region were recognised as posing risk at the national level, including in particular transactions with such persons whether the obliged entity recognised such persons as posing risk, how the obliged entity assess such persons before, have there been any misuses by these clients which perhaps were not identified on time by the obliged entity and what are the reasons why transactions of these clients were not identified at the given moment as posing an ML risk.

In the early stages the list will be wide and cover all recognised factors. The list should also include ML/TF typologies, trends, etc. It would be also useful to include supervisor's remarks about some circumstances in the obliged entity that were identified as insufficiently addressed, etc.

After a comprehensive and wide list has been drawn up, it should be revised in terms of which of the specific items on the list is not relevant enough for the obliged entity's circumstances or perhaps the obliged entity does not offer a product identified as posing risk at the national level, or certain models of behaviour are not specific to the obliged entity, etc. Thus, the obliged entity may eliminate certain items from the list, but if it has identified in the past some models of behaviour or situations identified in the obliged entity as posing risk, they should by all means be included in the list and further developed.

In this initial stage, none of the factors can be said with certainty to pose more or less risk; rather, here we talk more about whether a certain factor is relevant enough for the ML/TF assessment.

It should be noted that there can be different approaches to this. One obliged entity may decide to start from certain models of behaviour, indicators, trends and to use certain scenarios identified at the national level, and than analyse to what extent such situations have been specific to the given obliged entity.

A different obliged entity may choose not to start from the scenario model, but from risk-posing products, services, transactions and than to further develop these initial assessment with certain typologies identified for specific products or executed transactions.

In any case, it is important that the persons drawing up this risk factor list, be open to changes and ideas. The list can be extended and shortened, depending on how the process develops. It will then become obvious to which factors should not be allocate resources, given that they are either not relevant for the obliged entity or their presence there is very limited, and which factors should be covered.

As has already been mentioned throughout this text, there is not one risk assessment model. There are certain guidelines, ideas, suggestions from domestic and international experience, but it is up to the obliged entity to decide what methodologies, records and what lists are the most useful for them and are the most relevant for their work methods.

When assessing risks, the following factors can be taken into account:

- a type of identified predicate crimes if such information is available to the obliged entity, i.e. tax evasion, crimes of corruption, document forgery, abuse of payment cards and other payment instruments,
- business relationships with high-risk countries,
- share of a certain group of clients in the total number of clients,
- available findings of the carried out supervision,
- number of suspicious transaction reports,
- share of a certain group of clients in the reported suspicious transactions over the last several years,
- whether a client who was subject to an investigation in the course of business cooperation had previously been assessed as a high-risk client.

In addition, the obliged entity when establishing a business relationship, will also assess the legal form - type of customer with which it enters into a business relationship, in terms of the type of company. Based on an analysis of previous suspicious activities, typologies and risks at national level, certain forms of companies will be identified as posing higher ML/TF risk. More specifically, an analysis of ML cases over the last several years shoed that ML cases feature limited liability companies as the most frequent legal form established by persons linked to criminal activities. When assessing the risk, the obliged entity must take such

circumstances into account. For instance, how many registered company forms are there and which form has most often been a subject to STRs, etc.
How the obliged entity carries out business with a client also has an effect on the assessment of client risk, at account should be taken of such circumstances with assessing risk - e.g. whether business is conducted through intermediaries or correspondent institutions, or business relationship established with non-face-to-face customers.

The obliged entity may asses the ML risk separately from the TF risk. Clients whose business operations are mainly done in cash must be carefully monitored by the obliged entity because of the TF risk. Here particular attention should be paid to the operation of non-profit organisations as the possibilities for their TF abuse are significant. Geographical risk in terms of TF is prominent in regions where terrorists are active based on information of relevant international organisations such as the United nations.

In order to assess risk, the obliged entity should describe all products, services, contractual relationships it makes, and to assess the likelihood of whether the clients will abuse this particular products for ML or TF and to assess the effect of this phenomenon in the same way as the client risk is assessed, as described above.

For instance, when it comes to client risk analysis, an accountant is not required to check every transaction registered in the book of clients, and certain accounting services are provided on a one-off basis, without establishing a lasting business cooperation with the client. However, a large number of services provided by accountants allow them relatively well, owing to the essential knowledge and access they have to business books and accounts of their clients and knowledge of control processes to recognize suspicious activities of their clients or their clients' business associates who would not be recognised by providers of other services. The assessment at the level of an accounting agency as an obliged entity will vary depending on the type of clients, contractual relationships etc.

While for instance the financing of construction of a building, (business) facility, international trade or other products and services offered, allowing for a wide range of actions and funds transfers, that entail a large number of transactions etc. pose higher risk due to the very complexity of the activity and because for instance some products are not transparent.

ASSESSMENT OF RISK AT THE LEVEL OF CLIENT, BUSINESS RELATIONSHIP AND TRANSACTION

Type of risk

Identifying the types of risk, i.e. client, transaction, service, form of business operations, geographical risk, is the first step in an obliged entity's and client risk analysis, whereby risk types can vary depending on the specific features of obliged entity's operation, and every obliged entity should take into account the risk types depending on their remit of operation.

I Types of risk in auditing companies, entrepreneurs and legal entities providing accounting services

Risk assessment for the purpose of these Guidelines should cover at least the following three types of risk: geographical risk, client risk and risk of the services offered by the obliged entity as part of their business. Where other types of risks are identified, and depending on the specific features of their operation, the obliged entity should cover in their assessment such types of risk too.

1.1. **Geographical risk** means risk predicated on the geographical area where the country of origin of the client, its owner of majority founder, beneficial owner or person otherwise controlling the client's operations is located or where the country of origin of the person carrying out a transaction with the client is located.

The factors based on which it is determined whether a geographic location or a particular country poses higher ML//TF risk are as follows:

1) countries against which the United Nations, Council of Europe or other international organisations have applied sanctions, embargo or similar measures;

2) countries designated by credible institutions (FATF, Council of Europe, etc.) as not applying adequate AML/CFT measures;

3) countries designated by credible institutions (FATF, Council of Europe, etc.) as supporting or financing terrorist activities or organisations;

4) countries designated by credible institutions (e.g. World Bank, IMF) as countries with a high level of corruption and crime.

The list of countries with strategic deficiencies in their AML/CFT systems is published on the APML website. The list of countries is based on the following:

1) FATF statements about countries with strategic deficiencies in their AML/CFT systems and that present a risk to the global financial system.

2) FATF statements about countries/jurisdictions with strategic deficiencies in their AML/CFT systems which expressed high-level political commitment to remedy the deficiencies, which developed an Action Plan together with FATF, and which are required to report on the progress to remedy the deficiencies identified,

3) reports on the assessment of national AML/CFT systems by international institutions (FATF and FSRB's such as the Council of Europe MoneyVal Committee).

Countries applying the AML/CFT standards at the EU level or higher are the following:

1) EU member states;

2) Third countries (other than EU member states) with effective AML/CFT systems as assessed in AML/CFT assessment reports by FATF or FSRBs (such as Moneyval);

3) Third countries (other than EU member states) identified by credible sources (e.g. Transparency International) as countries with a low level of corruption or of other criminal activity;

4) Third countries (other than EU member states) which based on credible sources, such as assessment of national AML/CFT systems by FATF and FSRBs (e.g. Moneyval) or published follow-up reports for the country, have legally binding obligations to fight ML and TF in line with FATF recommendations and effectively implement these obligations.

Clients who have a contractual relationship or have business with entities registered in offshore areas pose higher ML/TF risk. For instance, a client will be identified as posing high risk if it is involved in provision of services with a client with registered office in a country with a privileged taxation system.

A client with a contractual relationship with a client in the region may present a low ML risk. For instance, a client may present low risk if it is trading in goods with a client in a regional country as there is economic justifiability for such a relationship.

Or, it can be low risk if it is registered for trade in goods and if, judging by further business operations tracked, all transactions with suppliers and buyers were linked to the given business transaction and that they are not registered in areas indicating potentially higher risk.

1.2. The obliged entity will decide what approach to take to client risk, based on its own experience and knowledge of business rules. Nevertheless, it is required to apply the restrictions set out in the AML/CFT Law and other AML/CFT regulations.

1) An increased risk may be indicated by the following unusual activities:

- when establishing a business relationship with an obliged entity, the client avoids to come in person and insists on an indirect contact;
- the client demands without a particular reason that business or a transaction be conducted quickly, regardless of higher expenses that such an action entails;
- the client pays for goods or services that are inconsistent with the description of its line of business;
- the client offers money, gifts or other benefits in consideration of transactions suspected not to be entirely in line with regulations;
- a client wants to assure the accountant that there is no need to fill in or provide some of the documents required;
- the client avoids submitting the required documentation or the obliged entity has doubts as to whether the submitted documentation is accurate and complete;
- a client often changes its accountants/auditors;
- a client does not know where business documentation is kept;
- a client has no employees or business premises, which is inconsistent with the volume of its business operations;
- a client frequently changes its name, registered office, ownership structure, etc.

2) the customer where due to the organisational structure, the legal form or complex and unclear proprietary relationships, it is difficult to determine the identity of the beneficial owner of the customer or persons who control them, such as:
- foundations, trusts or similar legal arrangements,
- charity and non-profit non-governmental organisations,
- offshore legal entities with unclear ownership structure that are not founded by a company from a country applying AML/CFT standards at the level of the standards set out in the AML/CFT Law;

3) clients perform activities that are characterised by a large turnover or cash payments (such as restaurants, pumps, currency exchange offices, casinos, flower shops, dealers in precious metals, cars, works of art, operators transporting goods and passengers, sports societies, construction firms);

4) foreign and domestic officials, in accordance with the AML/CFT Law;

5) private investment funds;

6) clients whose offer for establishment of a business relationship was rejected by a different obliged entity, i.e. persons with bad reputation;

7) clients whose sources of funds are unclear or have not been identified, and/or clients who cannot prove the source of funds;

8) a client who has lived abroad for a long time, having no proof that it was employed there, organisation a large amount of cash to establish a company offering services (hospitality, consulting, marketing services, organisation services for celebrations etc.).

9) clients suspected not to be acting on their own behalf, or that they act based on instructions of a third party.

Clients subject to application of enhanced CDD are offshore legal entities in line with the AML/CFT Law or legal entities having an offshore legal entity in their ownership structure. An obliged entity shall set out a procedure for establishing whether a customer or a legal person which exists in the ownership structure of the customer is an off-shore legal person, according to the AML/CFT Law. In order to establish if a legal entity is an offshore company, the obliged entity can use the lists of IMF, World Bank or the list of countries which is an integral part of the Rulebook concerning the list of jurisdictions with a preferential tax system (Official Gazette of the Republic of Serbia, 122/12).

Additionally, if the obliged entity assesses that a client, which is an offshore legal entity or a legal entity whose ownership structure features an offshore legal entity, has a complex ownership structure (e.g. there is a large number of legal entities in the ownership structure and the legal entities having a significant share of the nominal capital are registered in offshore areas, and it cannot be easily established who is the beneficial owner of the companies), the obliged entity must obtain a written statement from the beneficial owner or representative of the company about the reasons for such a structure and to consider whether there are reasons to suspect ML or TF in the case, and to make an official note thereof which it must keep in accordance with the AML/CFT Law.

1.3. The **risk of service** means the following:

1) operations that are largely inconsistent from the usual business operations of a client engaged in a similar business line;

2) business operations that do not have economic justification (for example, frequent trading in securities when buying is done by placing cash on dedicated accounts, and soon afterwards they are sold below the price - the so-called trading in securities with a planned loss, unexpected loan repayment before the deadline or in a short time after the date of the loan approval, withdrawal of funds from the individual account of a voluntary pension fund member in the short time after their payment);

3) transactions carried out by a client in amounts that are slightly less than the amounts fixed as thresholds for reporting under the AML/CFT Law;

4) loans to legal entities, and in particular the loans provided by founders from abroad to a legal entity in the country without economic justification;

5) payment for consulting, management and marketing services, as well as other services for which there is no fixed value or price on the market;

6) payment for goods and services to partners of the client that originate from offshore areas, and it can be clearly seen from the documentation that the goods originate from the countries of the region;

7) purchase of goods from countries where such goods are not manufactured (e.g. import of coconut from Bosnia and Herzegovina);

8) frequency of transactions on the basis of advance payment of import of goods or performance of services in which it is not certain that the goods will actually be imported or services performed;

9) over-invoiced or under-invoiced goods or services; multiple invoicing;

10) multiple incoming and outgoing payments for the same goods or services (payment is made a number of times to the same or different supplier for the same products supplied or service rendered);

11) abuse of goods write-off (the client frequently writes off significant share of the sold goods due to various factors, for instance due to *force majeure,* perishability, losses in transportation inadequate storage, scrap, etc. - without such factors actually occurring).

12) the client pays for goods and services using electronic banking, and he/she has no documentation to be accounted;

13) client pays for life insurance in large one-off transactions fro all employees;

14) client deposits with a number of banks disproportionately high amounts of deposits (for example, 100%) as collateral for obtaining a credit or a loan.

II Type of risk in factoring companies

A risk assessment within the meaning of these Guidelines should cover at least the following four types of risk: geographical risk, client risk, transaction risk and service risk.

Where other types of risks are identified, given the specific nature of the purchase of claims business, the obliged entity should cover in their assessment those types of risk too.

The factors based on which it is determined whether a geographic location or a particular country poses higher ML//TF risk are as follows:

1) countries against which the United Nations, Council of Europe or other international organisations have applied sanctions, embargo or similar measures;

2) countries designated by credible institutions (FATF, Council of Europe, etc.) as not applying adequate AML/CFT measures;

3) countries designated by credible institutions (FATF, UN, etc.) as supporting or financing terrorist activities or organisations;

4) countries designated by credible institutions (e.g. World Bank, IMF) as countries with a high level of corruption and crime.

The list of countries with strategic deficiencies in their AML/CFT systems is published on the APML website. The list of countries is based on the following:

1) FATF statements about countries with strategic deficiencies in their AML/CFT systems and that present a risk to the global financial system.

2) FATF statements about countries/jurisdictions with strategic deficiencies in their AML/CFT systems which expressed high-level political commitment to remedy the deficiencies, which developed an Action Plan together with FATF, and which are required to report on the progress to remedy the deficiencies identified,

3) reports on the assessment of national AML/CFT systems by international institutions (FATF and FSRB's such as the Council of Europe MoneyVal Committee).

Countries applying the AML/CFT standards at the EU level or higher are the following:

1) EU member states;

2) Third countries (other than EU member states) with effective AML/CFT systems as assessed in AML/CFT assessment reports by FATF or FSRBs (such as Moneyval);

3) Third countries (other than EU member states) identified by credible sources (e.g. Transparency International) as countries with a low level of corruption or of other criminal activity;

4) Third countries (other than EU member states) which based on credible sources, such as assessment of national AML/CFT systems by FATF and FSRBs (e.g. Moneyval) or published follow-up reports for the country, have legally binding obligations to fight ML and TF in line with FATF recommendations and effectively implement these obligations.

Clients who have a contractual relationship or have business with entities registered in offshore areas pose higher ML/TF risk. For instance, a client will be identified as posing high risk if it is involved in provision of services with a client with registered office in a country with a privileged taxation system.

A client with a contractual relationship with a client in the region may present a low ML risk. For instance, a client may present low risk if it is trading in goods with a client in a regional country as there is economic justifiability for such a relationship.

Or, it can be low risk if it is registered for trade in goods and if, judging by further business operations tracked, all transactions with suppliers and buyers were linked to the given business transaction and that they are not registered in areas indicating potentially higher risk.

Client risk

The obliged entity will decide on their own what approach to take to a client, based on generally accepted principles and their own experience. A higher risk may also be indicated by activities performed by the following clients:

1) clients carrying out business activity or transaction under unusual circumstances, such as:
- client transfers claims for goods that are not typical of its business (e.g. goods are medicines, but registered to sell frozen fruit);
- client transfers claims from debtors which is not consistent with economic potential of the transferor or debtor, or with the business line;
- client offers guarantees of third parties without any business justification or of persons with bad reputation;
- economic dependence or relation between the client and factor management;
- knowledge of the way of factor’s operation;
- frequent and unexpected establishment of business relationships with several obliged entities having the same line of business, without economic justification;

2) clients the identity of whose beneficial owners or persons controlling them is difficult to establish due to the structure, legal form or complex or unclear relationships, such as in the case of offshore companies with unclear ownership structures that were not founded by

companies from countries applying AML/CFT standards at the level of standards set out in the law;

3) foreign arms dealers and manufacturers;

4) non-residents and foreigners;

5) clients represented by professionals (lawyers, accountants or other professional representatives) especially where the obliged entity is in contact with representatives only;

6) firms with disproportionally small number of staff compared to the volume of business they conduct, without their own infrastructure, business premises, unclear ownership structure, etc.;

7) persons with bad reputation, either bad public reputation or based on prior experience, in selling other products, etc.;

8) clients reporting claims that are not consistent with the economic potential and business line of the creditor;

9) client who is a foreign official, i.e. a natural person who holds or who has held in the last four years a high-level public office in a foreign country, such as:
- head of state and/or head of the government, member of the government and their deputies,
- elected representative of legislative bodies;
- judge of the supreme and the constitutional courts or of other high-level judicial bodies whose judgments are not subject, save in exceptional cases, to further regular or extraordinary legal remedies;
- member of courts of auditors, supreme audit institutions or managing boards of central banks;
- ambassador, chargés d'affaires and high-ranking officer in armed forces;
- member of the managing or supervisory bodies of legal entities whose majority owner is the state;
- member of the managing body of a political party.

10) client who is an official of an international organisation, i.e. a natural person who holds or who has held in the last four years a high-level public office in an international organisation, such as: director, deputy director, member of managing boards or other equivalent function in an international organisation;

11) client who is a domestic official, i.e. a natural person who holds or who has held in the last four years a high-level public office in the country, such as:

- president of the country, prime minister, minister, state secretary, special advisor to a minister, assistant minister, secretary of the ministry, director of a body within a ministry and their assistants and director of an independent organisation, as well as their deputy and assistants;
- member of parliament;

- judge of the Supreme Court of Cassation, Commercial Appellate Court and Constitutional Court;
- president, vice president and member of the council of the State Audit Institution;
- Governor, Vice-Governor, member of the executive board and member of the Council of the Governor of the National Bank of Serbia;
- person entrusted with a prominent position in diplomatic - consular offices (ambassador, consul general, chargé d'affaires);
- member of a managing board in a public enterprise or a state majority-owner company;
- member of the managing body of a political party.

close family members of an official meaning the spouse or extra-marital partner, parents, brothers and sisters, children and their spouses or extra-marital partners, and close associate of an official means any natural person who draws common benefit from property or from a business relationship or who has other sort of close business relationship with the official (e.g. natural person who is the formal owner of a legal person or a person under foreign law, whereas the actual benefit is drawn by the official).

12) client - foreign legal entity, which does not perform or which is prohibited from performing trading, manufacturing or other business in the country of its registration (legal entity with registered office in an offshore financial centre);

13) client who is a fiduciary or other similar legal arrangement with unknown or concealed owners or management (i.e. legal arrangement offering representation services for third parties, i.e. companies established in a contract between a settlor and administrator who manages the founder's assets for the benefit of certain users or beneficiaries, or for other specified purposes);

14) client with a complex status structure or complex ownership chain (complex ownership structure or complex ownership chain hampering or preventing identification of the client's beneficial owner or persons directly providing assets to the client, which gives them the possibility to perform supervision, which may be
have an effect on financial or business decision-making by the management of the client).

Transaction risk

Transaction risk exist where:
1) transactions that significantly differ from the standard behaviour of the customer;

2) transactions are not economically justifiable;

3) transactions conducted in such a way to avoid standard and usual methods of control;

4) transactions where the client refuses to deliver complete documentation;

5) transactions in which the documentation does not correspond to the way the transaction is carried out;

6) transactions involving frequent changes of credit notes, incongruence or contradiction between invoices and descriptions;

7) transactions intended for persons or entities against whom a measure of the United Nations or the Council of Europe is in force;

8) transactions that a client would conduct for and on behalf of a person or entity against whom a measure of the United Nations or the Council of Europe is in force.

Service risk

Service risk refers to the following risky services:

1) services that are new on the market, i.e., that have not been previously offered in the financial sector and must be monitored in particular to determine the actual degree of risk;

2) the types of services for which the obliged entity's employee assessed on the basis of their experience that they bear a high degree of risk;

3) services all bearer negotiable instruments and those issued to the bearer or for the benefit of a fictitious beneficiary, endorsed without restriction or in other forms allowing for title to be transferred on handover, and all other incomplete instruments that are signed without indicating the name of beneficiary.

The obliged entity should pay particular attention to every ML/TF risk that could be stem from the use of new technologies, and to take appropriate measures to prevent use of this technology for ML/TF.

The obliged entity in addition to the above criteria, should also cover other types of risk when identifying the level of risk of a client, business relationship, service or transaction, such as:

- obliged entity's size, structure and area of business, including the volume, structure and complexity of transactions performed by the obliged entity;
- client's status and ownership structure;
- intended purpose of the business relationship, service or transaction;
- obliged entity's knowledge of services and experience and knowledge of the specific area;
- other information showing that the customer, business relationship, service or transaction can present higher risk.

Risk analysis

Risk analysis contains:

-risk analysis in terms of overall business operations of the obliged entity;

- risk analysis in terms of each group or type of client and/or business relationship, that is, the service provided by the obliged entity and transaction;

Following the initial list and determination of risk category is the analysis stage. This stage is crucial to risk assessment. Description stage proceeds into stage of risk understanding - therefore the analysis is the very core of risk assessment. At this stage external (environmental) factors should be considered in addition to internal factors. For example, what political or economic circumstances affect the obliged entity's business. Proper consideration should be given to legislation - are there any discrepancies, are certain legal provisions seen as non-applicable, is the obliged entity's business hindered by discrepancies in legislation, etc.

Transparency of certain information should be considered as well. To what extent is certain information available to the obliged entity; is the informaton published on the websites of state authorities; is the information on ownership of companies obtained and how; how valid and up-to-date is public information?

Apart from taking previous experience into consideration, typical situations recognized at the level of sector should be considered as well. At this stage of risk analysis having as many meetings among obliged entities is highly beneficial, to discuss the list of factors affecting the individual obliged entity. All the persons directly or indirectly involved in detection money laundering or terrorism financing should exchange their views at this stage, they should satisfy themselves that there is proper understanding of risks, that the relevant persons are trained enough, that they know the system, etc. The meetings might indicate that certain risks have not been recognized or that some factors have been left out - therefore this is the moment for the list to be supplemented.

Following consideration of all internal and external factors and risk categories, following discussions of factors, there comes weighting of factors or money laundering and terrorism financing risk assessment for each factor. Each risk factor is assessed individually in comparison to other risk factors, thus its effect on risks in obliged entities are determined.

Effects of illegal activities by criminals and terrorists on obliged entities should be analysed. Have certain risk factors been recognized by the obliged entity and to what extent; have there been any preventive actions; have suspicious activities been identified or not and why; have there been any seizure of assets belonging to the obliged entity's client; is the client a damaged party and to what extent; what is the attitude of senior management - all these questions deserve to be answered at this stage.

Have the perpetrators of criminal offences been recognized by the obliged entity, and what offences; was it possible to recognize them and to what extent; what behaviour patterns have been recognized -perhaps typologies indirectly indicating a criminal offence - tax evasion; perhaps situations and clients that can be related to drug trafficking, etc.

It would be useful to include the list of criminal offences in risk assessment and label what and how many have been identified; how many clients from previous period are known to have been perpetrators of a criminal offence; what are the sources of information - the media or the feedback on a STR. Particular attention should be paid to high risk criminal offences from the national risk assessment.

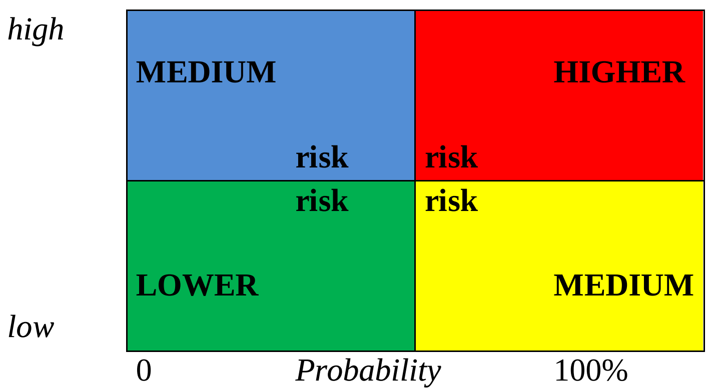
In no way does the above mean that the obliged entity has to recognize a particular criminal offence exactly, which is almost impossible in reality, but rather to try and assess if certain behaviour patterns could be related to a criminal offence and to what extent. This is only an example.

The analysis should be supplemented by certain examples. These can include submitted STRs, feedback given by the APML, indictments, cases referred to a state authority based on STRs, etc.

Then the obliged entity draws a conclusion on the levels of risk. This can be done numerically, but there has to be an exact description of how a certain risk was expressed through a numerical indicator. Conversely, it can be done descriptively - higher, lower, medium risk, or small, medium, high, very high probability that a factor carries a certain risk. Effects can be described as significant, small, insignificant, of outstanding significance.

It is up to the obliged entity to decide on how to express an assessed risk, whether descriptively or numerically, and what risk matrix is to be used for that purpose.

An example of risk analysis:



When assessing risk, the obliged entity should establish if all recognized categories of risk belong to low, medium, high or unacceptable risk for doing business. The obliged entity has to consider different ways of cooperating with its client, whether in direct contact or without physical presence. Risk assessment for money laundering and terrorism financing depends on combination of all risks and their various combinations. The assessment will be different among institutions and clients themselves.

For example, a client can be assessed as low risk for a bank, and high risk for an accountant, due to different impact of type of risk and business relationship.

Obliged entities can use different ways and matrices for risk assessment to establish what clients are in what risk categories. Risk matrix is not constant, it changes along with change in circumstances surrounding the obliged entity itself.

For example, a low risk product combined with a high risk country results in a higher risk and can be assessed ad medium risk. If subsequently the client establishes a new business relationship and/or uses a high risk product, the risk of the client will change into high risk, etc.

When classifying risks, the obliged entity can define additional levels of risk, taking its own specificities into consideration. Development of the risk matrix can include consideration of the whole range of risk categories, such as products and services offered by the obliged entity, clients to which the products and services are offered to, size of the institution, its organizational structure, types of companies with which the obliged entity cooperates, etc.

Risk assessment helps the obliged entity understand how money laundering and terrorist financing risks can differ from one client to another, as well as along products and geographic areas, so it helps the obliged entity focus attention on high risk areas for the relevant business.

Risks must be explained and documented to be used both for developing and defining policies and procedures in terms of AML/CFT and for submitting this type of information at a supervisor's request.

In risk analysis attention has to be paid on combination and influence of all factors.

For example - based on the regulations in force, a client can be low risk, that is, simplified CDD is applied, as is the case of legal persons the stocks of which are listed on an organized securities market. When establishing a beneficial owner, suppose that a foreign PEP appears on the function. According to the Law, a foreign PEP is a high risk client. Thus, no simplified CDD is possible for this legal person, but rather, enhanced CDD, because of the risk of the client and the Law itself.

According to Article 6 of the AML/CFT Law, the obliged entity can classify a client as low risk if it assesses that, due the nature of business relationship, form and type of transaction, business profile of the client and other circumstances surrounding the client, there is an insignificant or low risk for money laundering or terrorism financing.

Evaluation and risk management

The third stage includes compilation of results obtained, based on which priority actions are set. What risks are seen as very significant and what risk-mitigation actions are to be undertaken without delay, which are of less significance, how common are the risks, which have been identified in the national risk assessment, in the obliged entity itself, etc.

It is on the obliged entity to decide what methods for risk mitigation will be used. For example, will a service be prohibited, will more attention be given to certain indicators, does the level of training need to be stepped up in the obligor, etc.

Risk assessment should contain action plan for mitigating risks, as well as the order and priority of undertaking necessary activities, in case its final results show that risk management system is inefficient or that significant deficiencies have been identified. It has been observed that most employees who should possess certain knowledge of money laundering and terrorism financing do not properly understand nor do they have adequate level of knowledge, so it is recommended that trainings be developed in advance.

This stage includes active **risk management**, from defining priorities to the activities provided for each measure to mitigate risks.

Money laundering and terrorism financing risk is specific for every obliged entity and it requires a risk management approach, proportionate to the level and structure of risk, as well as to the size of its business organizations. Aims and principles of risk management should enable obliged entities to establish adequate business policy and procedures, which includes CDD rules, promotion of ethical and professional standards, that is, prevention of intentional and unintentional abuse of entities for criminal activities.

All organizational units with different terms of reference should engage in money laundering and terrorism financing risk management. It is important for each unit to know its role, level of powers and responsibility towards the organization as a whole, as well as depending on the level of exposure to and the effect on risks.

The role of management

Management directs a business policy by formulating goals and makes decisions on strategic choices. When finalizing plans and a business policy, management must take into consideration money laundering and terrorism financing risks. The ways risks are documented and presented are very important for the decision making and planning process. This is exactly the reason why management should be included from the very beginning in the preparations of and money laundering and terrorism financing risk assessment and to make certain steps to establish adequate system of supervision. It includes that an AML officer and a deputy AML officer undergo training, that solutions be implemented for the system of supervision, etc. Management must ensure that the employees abide by internal procedures, established policy, etc.

Risk assessment findings

Once all three stages are completed and risks of an obliged entity are established, the findings should be documented. As already said, in the very beginning of the process a decision should be made as to who would take part in the risk assessment, in what way data would be compiled, what data would be used, which would all be reflected in a written report, which will, in addition to the definition of basic concepts and the description of methodology, have its greatest relevance due to the findings and detected risks. It is on the obliged entity to decide to what extent the report will be detailed and what data it will contain. It is relevant to show the findings and how the findings were obtained, as well as how perceived risks are reflected on the obliged entity itself.

Senior management should be familiar with all the findings and should supervise the entire process. At the very end of the process a decision will be made as to who within the obliged entity will be provided with the findings. For example, an obliged entity may decide to provide data to all the organizational units - all employees, or an obliged entity may decide to provide data only to the organizational units relevant for the prevention if money laundering and terrorism financing. An obliged entity may decide to provide the complete text of the assessment to all the employees, but that certain parts of the text should not be transparent. It is all on the obliged entity to decide.

Internal procedure

Once the risks are established and analysed, AML/CFT risk management strategy is applied to enable the obliged entity to pursue adequate internal policy and risk mitigating procedures, or risk eliminating procedures, the purpose of which is to eliminate reputational and business risk, risk that irregularities would be found by supervisory authority and other forms of risk.

By risk assessment and by developing adequate policies and procedures the obliged entity ensures continuity of money laundering and terrorism financing risk management despite all changes that may occur in management or among employees, and/or in the structure of the employees.

Established business policies and procedures should enable the obliged entity to manage perceived risks effectively and to mitigate them, as well as to focus its efforts on those areas of business which are most subject to different types of abuse with the aim to prevent money laundering and terrorism financing. The greater the risk, the more control measures must be applied.

An obliged entity may, for example, establish certain restrictive mechanisms for high risk products, that is, introduce requirement that for the use of a certain type of service, permission of senior management is necessary, etc.

Special policies and procedures must be introduced at the level of the organization, in terms of customer due diligence, supervision of the activities, records that should be kept and in terms of all reports filed to the Administration for the Prevention of Money Laundering.

Customer due diligence

AML/CFT Law authorizes the obliged entity to classify clients and business relations into three levels of risk, depending on the level of money laundering and terrorism financing risk. On the basis of the level of assessed risk, the obliged entity implements adequate customer due diligence measures. Risk assessment of a client is done throughout the entire duration of a business relationship and the level of risk can change. For example, a business relationship with a client can at first be assessed as low risk and then circumstances may occur which will increase the risk, or vice versa. This does not refer to the cases classified according to the AML/CFT Law into high risk, on which increased CDD measures are to be applied (correspondent relationship, foreign PEP, domestic PEP, offshore company, state-of-the-art technology and emerging services, a client from the country with strategic deficiencies and establishing business relationship with non-face-to-face customers).

Customer due diligence actions and measures can be general, simplified and increased.

General customer due diligence includes: establishing and verifying the client's identity, establishing and verifying the beneficial owner's identity, obtaining information of the intended purpose of the client's business relationship.

Simplified due diligence is implemented on the clients classified into low risk. To classify a client in low risk, the obliged entity must comply with requirements from the AML/CFT Law and Rulebook on Methodology for Implementing the AML/CFT Law. Examples of low risk include establishing business relationship with a state authority, with a joint stock company quoted on a securities market in Serbia, etc.

Enhanced customer due diligence includes additional actions and measures that an obliged entity undertakes in the cases prescribed by the Law and in other cases when it assesses that there is a high risk of money laundering and terrorism financing due to the nature of business relationship, ownership structure of the client and/or other circumstances in relation to a client or business relationship. High level of money laundering or terrorism financing risk requires gathering of additional information on the nature of business relationship, as well as more frequent monitoring of the customer's business operations.

The obliged entity is required to provide in an internal act how often clients classified in low, medium and high level of risk respectively are to be monitored.
For example, an obliged entity may monitor clients classified in low level of risk in line with Article 6 of the Law at least once in 2 years; clients classified in medium level of risk at least once in one yea and clients of high risk at least once in 6 months.

For the purpose of undertaking actions and measures, an obliged entity is required to:

1) establish and verify a client's identity when:

- establishing a business relationship,

- when there are reasons to suspect money laundering and terrorism financing with respect to a client or service,
- when there is suspicion with respect to veracity or authenticity of data on the client:

2) monitor business operations and check compliance of the client's activities with the nature of business relationship;

3) submit reports on transactions or persons for which there are grounds to suspect money laundering or terrorism financing to the APML.

The obliged entity is required to develop a list of indicators for recognizing suspicious transactions or clients, which will include the indicators published on the website of the APML. When establishing elements of suspicion with respect to a transaction or client, if a transaction meets one of the indicators, it does not necessarily mean that the transaction is suspicious and that it should be reported to the APML immediately.
Conversely, a transaction can be suspicious without meeting any of the indicators.
One should consider a broader picture, in line with the principle that nobody knows a client better than an obliged entity, and assess whether a transactions goes beyond usual framework, that is, beyond the client's expected business operations.
Officials5

Clients on which enhanced due diligence is applied are foreign and domestic officials in line with the Law.

---

[5] Official means an official of a foreign country, of an international organisation and of the Republic of Serbia.

Foreign official means a natural person who holds or who has held in the last four years a high-level public office in a foreign country, such as:
-head of state and/or government, member of the government and his/her deputy,
-an elected representative of a legislative body,
- justice of supreme and constitutional court or of other high-level judicial bodies whose judgments are not subject, save in exceptional cases, to regular or extraordinary legal remedy;
- member of a courts of auditor, supreme audit institution and member of managing boards of central banks;
- ambassador, chargés d'affaires and high-ranking officer in armed forces;
-member of the managing and supervisory body of a legal person whose majority owner is the state;
- member of the managing body of a political party.
Official of an international organization is a natural person who holds or has held in the last four years a prominent public function in an international organization, such as: director, deputy director, member of a managing board or other equivalent function in an international organization;
Republic of Serbia official means a natural person who holds or who has held in the last four years a high-level public office in the country, such as:
- president of the country, prime minister, minister, state secretary, special advisor to a minister, assistant minister, secretary of the ministry, director of a body within a ministry and his/her assistants and director of an independent organisation, as well as his/her deputy and assistants;
- member of Parliament;
-justices of the Supreme Court of Cassation, Commercial Appellate Court and Constitutional Court;
-president, vice president and member of the council of the State Audit Institution;
Governor, Vice-Governor, member of the executive board and member of the Council of the Governor of the National Bank of Serbia;
person holding a prominent function in diplomatic - consular offices (ambassador, consul general, chargé d'affaires);
member of a managing board in a public enterprise or a state majority-owned company;
- member of the managing body of a political party.
Close family member is a spouse or extramarital partner, parents, brothers and sisters, children, adopted children and stepchildren and their spouses or extramarital partrners;
A close associate is a natural person benefiting from common property or from established business relationship or a person who has any other close business relationship with an official (for example, a natural person who is a formal owner of a legal person or person under a foreign law, whereas an official actually benefits from it); senior management is a person or a group of persons who, in line with the law, run(s) and organize(s) business activities of an obliged entity and is responsible for compliance of business activities with law;

The obliged entity is required to prescribe in an internal act a procedure for establishing if a client with whom it wishes to establish business relationship or the client's beneficial owner is a domestic or foreign official.

In line with the Law, an official, being a politically exposed person, is a high risk client, therefore the obliged entity has to conduct an analysis in all the cases when such a person appears as a client, before entering a business relationship or conducting a transaction in the amount of EUR 15.000,00, if business relationship has not been established.

Enhanced analysis of the client includes undertaking additional measures, such as:

1. gathering data on the source of funds and property that is subject or will be subject of a business relationship/transaction, from official documents and other documentation submitted by a client. If the data cannot be obtained in a manner described, the obliged entity will take the statement from a client on the source of funds/property;

2. gathering data on the source of entire wealth owned by an official,

3. necessity to obtain written approval of the senior responsible person before entering business relationship with such a client . It should be defined in internal acts who is responsible to grant written approval. It could be a member of senior management referred to in Article 52, para.3 of the Law or another member.

4. monitoring transactions and other business activities undertaken by a politically exposed person with special attention after the business relationship has been established.

Information as to whether a specific person is an official or not can be obtained by an obliged entity from a special written statement signed manu propria, given by the client before business relationship is established or before a transaction is conducted.

The written statement should include the following information:

1) name and surname, permanent residence, date and place of birth of the client entering business relationship or requesting a transaction, as well as number, type and issuer of the valid personal ID document;
2) statement as to whether the client is an official - politically exposed person, according to the criteria from the Law;
3) information as to the type of a politically exposed person (a person who holds or has held in the last four years a prominent public function, a close family member or a close associate),
4) period of holding a prominent public function, if the person holds or has held it in the last four years,
5) type of public function that the person holds,
6) information on a family relationship, if the client is a family member of a politically exposed person,

7) form and type of business cooperation, if the client is a close associate.

The obliged entity can obtain data on an official by inspecting public data and other available data (it is on the obliged entity to judge to what extent publicly available information will be considered credible and relevant for the client analysis) and the data can be verified by checking the website of the Anti-Corruption Agency, of state authorities competent for keeping the register of foreign officials , foreign consulates or embassies in Serbia, and/or the Ministry of Foreign Affairs and other publicly available databases.

In case a business relationship is established with a public enterprise or a company which is majority-owned by the state, given the fact that members of the managing authority can be regarded as officials pursuant to the Law, the obliged entity can consider different approaches, including one that the specific business relationship should not be classified as high risk solely because of this criterion. This is mostly because such natural persons act in their professional capacity before legal persons. In case there are additional indicators, such as negative reputation of an official, the legal person can indirectly be classified in high risk. Additionally, if the natural persons establish business relationship in their name or on their behalf, or in the name of and on behalf of a company of which they are beneficial owners, enhanced due diligence should be applied, in line with the Law.

Non-face-to-face customers

Another situation in which the obliged entity is required to classify a client in high risk is when business relationship is established without physical presence of a client. This situation applies both on natural and legal persons. If business relationship is established by a proxy on behalf of a legal person, that legal person has to be classified as high risk.

In these situations, the obliged entity is required to apply enhanced due diligence, specifically: to gather additional information on the client's identity (for example, additional official documents, business documentation, authorizations signed by a responsible person, etc), to find reasons why the business relationship is established without physical presence of the client, to make an additional contact with the client by phone, e-mail, skype, viber, etc, to gather another identification document of the client, etc.

Supervision and updating of risk

The obliged entity must constantly update money laundering and terrorism financing risks by establishing and describing periodical reviews of the assessment. The obliged entity must be abreast of latest money laundering and terrorism financing methods and trends, international developments in this area and amendments to legislation. These reviews can include the assessment of resources for risk management, such as allocated funds and staff, but also future needs relevant for the nature, size and complexity of the client's business activities. Risk updating should be conducted when a business policy and strategy is about to be changed, when deficiencies are observed in the effectiveness of measures undertaken, etc.

The obliged entity must be able to establish if the measures undertaken are adequate vis-a-vis perceived money laundering and terrorism financing risks, as well as to establish if the risk of the client was properly assessed when establishing business cooperation or some changes occurred during cooperation.

There is no such thing as a constant risk assessment. The obliged entity must prescribe in internal acts when and how risk reviews are conducted, both at the level of the obliged entity and at the level of client.

It is necessary to establish a system which constantly monitors and reviews money laundering and terrorist financing risks. Risk updating should be conducted in the framework of tasks undertaken by the obliged entity to ensure that internal policies and procedures are in place, that there is compliance with regulations.

Reports submitted to the management should contain information on monitoring activities, risk mitigation activities, internal audit reports, monitoring suspicious transactions and reports, number of high risk clients, as well as findings of supervisory authorities presented in on-site supervision reports. Management should be provided with all relevant information which will enable checking the level of control of money laundering and terrorism financing prevention, as well as possible consequences on the obliged entity’s business activities if control and prevention mechanisms do not function properly.

The risk report should indicate whether appropriate control measures are in place, whether they are adequate and fully implemented so that the obliged entity could protect itself from possible money laundering and terrorism financing abuse.

Supervision process should include and check exposure to money laundering and terrorism financing risk for all clients, products, services, transactions, locations, destinations, forms of business, as well as to ensure the review of thee risks in a certain period of time.

Supervision process should draw the attention of the obliged entity to all possible failures (for example, lack of compliance with regulations), inadequate customer due diligence, new risky circumstances arising for some clients, etc, and to indicate that the awareness of the obliged entity is not commensurate to the potential rikl exposure.

Sectoral risks with examples

What follows are some examples of risk assessment by sectors, but it is on the obliged entity to develop and apply matrices and procedures for developing risk analysis and to document them.

Accounting agency - an example of high risk

An accounting agency was established as a limited liability company and according to the criteria from the Law on Accounting, was classified as a medium size company. There are 10 employees in total. Since the day the agency was founded, it has established business relationship with 56 clients. They provide following services within their line of business: accounting services, payroll, financial reporting, registration of legal and natural persons with the Business Registers Agency and tax advisory services. In terms of the structure of clients, 80% of them are limited liability companies and 20% are entrepreneurs. The clients are mostly registered for wholesale and retail trade in country and abroad, production, consulting, and construction of residential and non-residential buildings, whereas the entrepreneurs are mostly registered for crafts (hair salons, beauty parlours, etc). Of the total number of clients, 5 clients were not physically present when establishing and verifying the identity of a client, whereas one client is a domestic official.

A client is a medium-size company, registered with the Business Registers Agency, with the code of business 4120 (construction of residential and non-residential buildings). The client is registered to do business with foreign companies, as well as for designing and consulting in its line of business. The client engages in payment operations in country and abroad and its transactions involve payments to suppliers and collections from purchasers from country and abroad. Transactions are mostly related to the client's line of business and are substantial in value. The client does not provide documentation on time, with the excuse that they are waiting for the signature of supervisory authorities. The identity of the client was not established when establishing business relationship, as the owner is a foreign legal person and the legal representative authorized an administrative assistant to establish business relationship with the agency.

Risk assessment at the level of the obliged entity: Clients are limited liability companies and entrepreneurs, which indicates that they are at risk of abuse of money laundering and terrorism financing. The clients also pursue their line of business in country and abroad. In addition, the obliged entity has established a relationship with a client which is classified as high risk in the national risk assessment. Furthermore, five clients were not physically present when their identities were established and verified, and one client is a domestic official, which also indicates a high risk of money laundering and terrorism financing. The client did not identify the beneficial owner, there are several indicators that the client poses high risk. Risk assessment at the level of the obliged entity - high risk.

Risk assessment at the level of the client: Geographic risk is low, as the client is registered and operates in the territory of Serbia. The client poses a high risk as it did not appear on the occasion of establishing cooperation, does not submit complete and accurate documentation and the beneficial owner of the client was not identified. The service also poses high risk, as the client engages in construction of residential and business premises, both in country and abroad, and provides designing and consulting services in construction business. Risk assessment at the level of client - high risk.

Accounting agency - an example of medium risk

An accounting agency is registered with Business Registers Agency as a limited liability company. According to the criteria from the Law on Accounting, the company is classified as a small enterprise, with 5 employees in total. In addition to comprehensive accounting services, the agency provides services of drafting reports on transfer prices. The agency has a business relationship with 100 clients, 50 of which are limited liability companies, 40 are entrepreneurs, whereas 10 are representative offices of a foreign legal person. The clients' line of business is related to the manufacturing, trade, consulting services, legal services, as well as services. All clients were physically present when business relationship was established, and so each client was identified. It should also be mentioned that out of total number of representative offices of foreign legal persons, one representative office was registered for consulting services in Serbia and 100% owner was a legal person registered in the British Virgin Islands.

A client is a medium-size company, registered in the Business Registers Agency for import and export of commercial goods. It is mainly involved in the import of components for toys, which are manufactured in Serbia. The client conducts payment operation in Serbia and is connected with 3 legal persons from abroad, as follows: one legal person from Switzerland, one from Cyprus and from the Czech Republic. The transactions are mostly about settling accounts in favour of suppliers in the country and abroad, as well as about collections from buyers in the country and abroad. There is also a record of incoming payments related to the increase of capital, as well as loans of associated companies for liquidity. It has been observed that the client often writes off a part of goods due to loss in transport and damage.

R A bank should regulate through an internal document on internal organization and job classification that the organizational unit in charge of implementing AML/CFT requirements be outside other organizational units, such as compliance unit, or that it be located within another organizational unit in the way that ensures that the AML/CFT compliance officer/deputy and other staff working on AML/CFT matters be independent in decision-making, as well as be directly accountable to the bank's executive board. Banks should also be recommended to provide for a sufficient number of staff in the organizational unit so that it is proportionate to the workload, having in mind the number and the type of clients, products offered and transactions conducted. In addition, banks should be advised to ensure that a job description for AML/CFT compliance officers, deputy AML/CFT officer and other staff in the organizational unit includes AML/CFT operations only. In a bank with a complex organizational structure due to its size and workload, it is also necessary to initiate the establishment of a robust system for the implementation of the Law, where obligations and responsibilities of all the relevant stakeholders will be clearly defined and transparent;

Risk assessment at the level of client - its founders are associated persons, one of which is from an off-shore destination, so one can conclude that geographic risk is high. The risk of the client is low, as the obligor has identified the client and transactions are conducted in line with the client's line of business. Risk of service is medium, as the client receives loans from associated companies, incoming payments based on the increase in capital, and it writes - off goods. Comprehensive risk of the client would be medium, as the obliged entity is satisfied that all transactions related to the increase in capital and loans are justified and write-off occurs truly because of damage and loss in transport. Risk assessment at the level of the obliged entity - medium risk.

Accounting agency - an example of low risk

An accounting agency is registered in the Business Registers Agency as a limited liability company. According to the criteria from the Law on Accounting, the company is classified as a small enterprise, with 3 employees in total. It has established business relationship with 42 clients, 90% of which are entrepreneurs and 10% are limited liability company. The clients mainly engage in service industry, trade in mobile phones and computers. In addition, a client provides services to real estate agencies. All the clients are domestic legal and natural persons, with known ownership structure.

A client is a small-size legal person, registered at the Business Registers Agency for repair and sale in mobile phones. It mainly engages in the import of mobile phones and its components from China. The client mostly refer to payments in favour of suppliers in country and abroad and daily takings.

Risk assessment at the level of the obliged entity - clients are mostly entrepreneurs, whose line of business poses no ML/TF risk. The clients engage in their business activities in the country. The services they provide are specified in their line of business, the obliged entity has established and verified the identity of the client. The above said, this is a low-risk client as all its clients are known, they are from Serbia, their turnover is insignificant, transactions are about collections and payments to suppliers. No large cash deposits have been perceived and there have been no withdrawals without justification. Risk assessment at the level of obliged entity - low risk.

Risk assessment at the level of client - geographic risk is low, as the client is registered in Serbia. The client's beneficial owner is 100% a natural person - Serbian national. The transactions are related to payments in favour of foreign and domestic suppliers, as well as payments of daily takings, so the risk of the client is low. The risk of the client's line of business is low, as the client engages in repair and sale of mobile phones and there are no unusual transactions, beyond the line of business. Risk assessment at the level of client - low risk.

An auditing company - an example of high risk

An auditing company is registered with Business Registers Agency and is licensed to engage in auditing by the Ministry of Finance. According to the criteria from the Law on accounting, this auditing company is classified as a medium-size company. In addition to auditing, this company provides tax advisory services, accounting services and capital valuation services. This company has established business relationship with 340 clients, 90% of which are limited liability companies, 5% are joint stock companies and 5% are local self-government. Out of total number of clients 10 clients were founded by foreign legal persons, therefore the beneficial owners are not known. The clients with established relationship with the company are registered for manufacturing, import and export of commercial goods, construction of residential buildings, transportation services. In addition, the company conducts audit in commercial banks and municipalities of Serbia. The auditing company issued 42% of unqualified opinions, 10% of disclaimers, 10% of adverse opinions and 38% of qualified opinions.

A client is a micro-size legal person, registered at the Business Registers Agency for engaging in other financial services. The company was founded by two Serbian nationals and a legal person from Serbia, founded by a legal person from the British Virgin Islands, with 80% share in capital assets. The company's beneficial owner could not be established on the basis of information kept by the Business Registers Agency. When establishing business relationship, the client requested to keep in indirect contact and avoided coming in person, therefore the identity of the client was not properly established and verified. According to the information of the Business Registers Agency, the company has a registered seat in the premises owned by an accounting agency. During auditing process, auditors discovered that one of the founders of the company was under investigation and that the person had participated in a number of suspicious valuations of socially-owned and state-owned companies preparing for privatization. The other owner took part in the purchase of a disputed land in Serbia, together with the first one. It was also discovered during the auditing process that the company took part in the purchase of land owned by an individual with criminal background, who is now being contested in court. Having inspected incoming and outgoing payments through the current account as well as a loan account, the team of auditors established that, according to a Loan Contract, the company loaned more than 10 million EUR from a Liechtenstein-based company. The collateral was supposed to be the stock of subsidiary companies, but the creditor neither realized it nor registered the collateral in the register of mortgage. Then the claim was purchased by a company from Panama, which decreased the company's debt. Then the client loaned 300.000 EUR to its subsidiary. The company is also a guarantor for the amount of 950.000 EUR, based on a long-term credit between a commercial bank and a legal person, which often changes its name, according to the Business Register Agency. In addition to these transactions, the company has several incoming and outgoing payments, unsupported by authentic documentation, which are related to its line of business.

Risk assessment of the obliged entity - based on its line of business and services it provides, the company is classified in low, even insignificant ML/TF risk. The company has established a business relationship with more than 300 clients which are limited liability companies and other clients are joint stock companies and local self-government, which do not pose ML/TF risk. Furthermore, for some clients ownership structure has not been established and certain irregularities have been found during the auditing process in several clients. This can be inferred from adverse opinions and disclaimers of opinion. Risk assessment of the obliged entity - medium risk.

Risk assessment of a client - Based on the above it can be inferred that the client has a complex ownership structure vis-a-vis its line of business; there is also suspicion that the client is involved in fictitious transactions, and it receives significant transfers from off-shore companies, whose ownership structure is difficult to identify . In addition, the client concludes contracts with different auditing companies each year. When establishing business relationship, the client avoided to be present in person and insisted to be in contact indirectly. The client does not have its own business premises, its business operations have no economic justification. Based on the above, it can be inferred that geographic risk, risk of service and risk of client is high.
Risk assessment of the client - high risk.

An auditing company - an example of medium risk

An auditing company is registered at the Business Registers Agency and is licensed by the Ministry of Finance. According to the criteria from the Law on Accounting, it is classified as a small-size company. Its sole business activity is provision of auditing services and it employs two certified auditors, according to the Chamber of Certified Auditors. It has established business relationship with 30 clients, which are limited liability companies. An auditing company is registered at the Business Registers Agency and is licensed by the Ministry of Finance. According to the criteria from the Law on Accounting, it is classified as a small-size company. Its sole business activity is provision of auditing services. The company's clients are registered to engage in manufacturing, import and export of commercial goods, forwarding services and software development. The auditing company has issued 85% of unqualified opinions and 15% of qualified opinions.

A client is a company registered at the Business Registers Agency as a company engaging in final construction works. The company was founded by a Serbian national. During the auditing process, the team of auditors discovered that in the year of audit the company received significant payments, based on the founder's loans, which were recorded by the National Bank of Serbia. It was also detected that the company changed its auditor every year. Outgoing payments from the company's accounts are related to its line of business, and include payments for office material, salaries to the employees and other operating costs. As for the incoming payments, these are accounts receivable from its buyers and founder's loans, which were documented in the auditing process.

Risk assessment of the obliged entity - based on its line of business and services it provides, the company is classified in low, even insignificant ML/TF risk. It has established business relationship with more than 30 clients, which are limited liability companies. Based on the issued opinions, it can be inferred that the company established cooperation with clients which represented their financial statements and business results in an accurate and honest manner and in line with regulations on financial reporting. Risk assessment of the obliged entity - low risk.

Risk assessment of the client - low geographic risk as the company was registered in Serbia and its owner is a Serbian national. Risk of service can be classified as medium as the company's line of business is classified in high risk in national risk assessment process and the company received several loans in a business year, but the loans are justified. This is a medium risk of service as the company often changes its auditing companies, which could result in hiding its illegal business activities. Risk assessment of the client - medium risk.

An auditing company - an example of low risk

An auditing company is registered at the Business Registers Agency and is licensed by the Ministry of Finance. According to the criteria from the Law on Accounting, it is classified as a small-size company. Its sole business activity is provision of auditing services and it employs one certified auditor, according to the Chamber of Certified Auditors. The auditing company has established business relationship with 10 clients, which are limited liability companies. These clients are registered to engage in the import and export of commercial goods, computer equipment, production of and trade in seed materials. The auditing company has issued 100% of unqualified opinions.

A client is a company registered at the Business Registers Agency for production and trade in seed materials and plant protection substances. The company was founded by a British national, who is a 100% shareholder. The legal representative is a Serbian national. When establishing business relationship, the legal representative was present and so the certified auditor was able to establish and verify the identity of the client. During the auditing process it was discovered that in a year the company received loans from its founder (foreign national), the purpose of which was the purchase of goods and maintaining the company's liquidity. It was also established that there were significant outgoing transfers from the company's account based on the procurement of goods and payments in favour of subcontractors who did production work for the company, as well as repayment of a credit in the amount of 800.000 EUR to a commercial bank that granted it in the previous year. Furthermore, it was established that the company had concluded an agreement with a leasing company, from which the main vehicle for the transport of goods was purchase, which was documented with contracts and repayment plans.

Risk assessment of the obliged entity - based on its line of business and services it provides, this company is classified in low, even insignificant ML and TF risk. The company has established business relationship with 10 clients which are limited liability companies. Based on the issued opinions, it can be inferred that the company established cooperation with clients which represented their financial statements and business results in an accurate and honest manner and in line with regulations on financial reporting.
Risk assessment of the obliged entity - low risk.

Risk assessment of the client - geographic risk is low, as the company is registered in Serbia and the owner is from Great Britain, country which applies AML/CFT standards. Risk of service is medium, as the company's line of business is conducive to manipulation in production process, and to the write-off of goods due to treacherous weather conditions, which is not the case with this particular company. Risk of product is low, as the company produces goods in Serbia, goods are related to the company's line of business, founder's loans are documented and justified, the auditor did not find the abuse of write-off of goods. In addition, the company obtained an unqualified opinion of an independent auditor, which implies that it represented its financial statements and business results in an accurate and honest manner and in line with regulations on financial reporting. Risk assessment of the client - low risk.

A factoring company - an example of high risk

A factoring company has been licensed by the Ministry of Finance, it has 4 employees and has established business relationship with 20 assignors of claims, which are mostly limited liability companies. Of the total number of clients, 15 engage in the trade in commercial goods and 5 of them engage in provision of services. Two clients were not physically present to have their identity established and verified when establishing business cooperation, whereas other two clients have owners which are known as perpetrators of criminal offences.

The assignor of claims (client) is a limited liability company engaging in the import, export, production and trade in seed materials in Serbia. The client operates within a group with three more companies engaging in the same line of business. The owner of the group where the client is a member is a natural person with a reputation for assigned claims which were investigated by the police. The client changed its ownership structure during the process of establishing business relationship with the factoring company, which was notified to the factoring company in an e-mail by the director, informing the factoring company that he had been removed from his position before business relationship was established and that his signature had been forged. The assignor assigns claims for the goods unrelated to its line of business, nor to the debtor's line of business. In addition, the client is not able to settle debts within deadline, but it uses factoring or credits to finance its business activities, thus managing to handle its liabilities. The inspection of financial reports of the debtor has showed that its account payables to suppliers are significantly less than assigned claims.

Risk assessment at the level of the obliged entity: Clients are limited liability companies and entrepreneurs, which indicates they are at risk of ML/TF abuse. The clients pursue their activities in the country and abroad. Out of the total number of clients, 5 engage in the business that per se poses risk and it relates to the provision of services. Furthermore, 2 clients were not physically present when their identity was established and verified, and 2 are known to have criminal background. Judged by this example, the client did not establish the beneficial owner and there are several indicators the client would be classified as high risk.

Risk assessment at the level of the client - geogarpahic risk is low, as the client is registered and engages in the activity in Serbia and its owner is a Serbian national. Risk of a client is high as its owner is already known to the factoring company based on the claims already assigned by another member of the group, which was investigated by the Ministry of Interior, and the signature was forged. Risk of service and of transaction is high as well, as the client has some claims related to goods which are unrelated to the company's line of business, it is not solvent enough to settle its debts in time and it insists on the services provided by the factoring company. Risk assessment for specific clients - high risk.

A factoring company - an example of medium risk

A factoring company has been licensed by the Ministry of Finance, it has 6 employees and has established business relationship with 20 assignors of claims, which are mostly limited liability companies. Ten of these companies engage in buy-out, sale and export of fruit, five of them engage in trade in commercial goods and five of them engage in service industry. Three clients were founded by a legal person from Panama. One client was not physically present for establishing and verifying its identity, but beneficial owners were established for all the clients, as they were registered in Serbia factoring company has been licensed by the Ministry of Finance, it has 6 employees and has established business relationship with 20 assignors of claims, which are mostly limited liability companies and are 100% owned by natural persons.

An assignor of claims (client) is a limited liability company engaging in buy-out, sale and export of fruit, mostly raspberries. The owner of the client is a legal person from Austria, whose beneficial owner has a Serbian origin. All the transactions are related to the buy-out of fruit, sale of related products and payments for services and other costs related to everyday business activities. The client assigned the claims related to the export of raspberries to the factoring company. The debtor is a company with a chain of retail stores in Austria, the owner of which used to be the same natural person that owns the client with which the factoring company established business relationship. The deadline for settling the debt is 90 days. When establishing business relationship, the client notified the factoring company of a change in the debtor's ownership structure and that it was not sure any more as to the collection of the assigned claim.

Risk assessment at the level of the obliged entity: The clients are limited liability companies, usually related to manufacturing business. The clients undertake their activities in country and abroad. One client was not physically present for establishing and verifying the identity, three clients were founded in an off-shore territory, but the beneficial owner was established for all the clients that have business relationship with the obliged entity. In this specific case, geographic risk and risk of transaction would be medium. Risk of clients would be medium, because of the legal type of the companies and because of the clients that provide services. Risk assessment for the client would be medium.

Risk assessment at the level of client - low geographic risk - the client was registered in Serbia, its owner is from Austria, where the ownership structure is known. The risk of client is low as it was physically present when establishing business relationship with the factoring company; its beneficial owner was established; the client warned of possible difficulties with regard to the collection of the assigned claims. Risk of service and transaction is high, as this is the collection of claims for the goods that were sold to a company and the deadline for collection is close to expiry; the debtor changed its ownership structure. Risk assessment of the specific clients - medium risk.

A factoring company - an example of low risk

A factoring company has been licensed by the Ministry of Finance, it has 2 employees and has established business relationship with 30 assignors of claims, which are mostly limited liability companies. 25 of these companies engage in trade in commercial goods and 5 companies engage in production and trade in agricultural produce. All the clients were physically present for establishing and verifying their identities when establishing the business relationship and the beneficial owner was established for all the clients, as they were all registered in Serbia and are 100% owned by natural persons.

An assignor of claims (client) is a limited liability company trading in construction materials in Serbia. The company's owner is a natural person, residing in Serbia. All transactions are related to the trade in construction materials and payments for services and other regular operational costs. The client assigned its claims, which relate to the sales of large amounts of cement to the factoring company, because of many outstanding claims and problems with liquidity. The debtor is a construction company, founded in 1991, which engages in construction of residential and non-residential buildings. The client was physically present when the business relationship was established, when all the terms of cooperation were agreed.

Risk assessment at the level of the obliged entity: clients are limited liability companies and entrepreneurs, which indicate that they are at risk of abuse for ML/TF purposes. The clients run their business in country and abroad. All the clients were physically present for establishing and verifying their identities and the beneficial owners were established for all the clients. Risk assessment of the client - low risk.

Risk assessment at the level of the client: Geographical risk is low, the client is registered in Serbia, its owner is a Serbian national. The risk of the client is low as the client was physically present when cooperation was established with the factoring company, its beneficial owner was established. Risk of service and transaction is low as well, as the claims that are to be collected are related to the goods that were sold to a company and the deadline for payment still did not expire; the claims are assigned for the purpose of liquidity. Risk assessment of the specific client - low risk.