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

No: ON-000261-0001/2022
Belgrade, 22 March 2022

On the basis of Article 6 para 1 of the Law on the Prevention of Money Laundering and Terrorism Financing (Official Gazette of the Republic of Serbia No 113/17, 91/19, 91/10 and 153/20 hereinafter referred to as: the AML/CFT Law), Article 38, para. 1 of the AML/CFT Law and Article 114 of the AML/CFT Law in relation to Article 105, para.1 of the AML/CFT Law), the Acting Director of the Administration for the Prevention of Money Laundering issues

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

These Guidelines shall regulate the manner in which the obliged entity supervised by the Administration for the Prevention of Money Laundering carries out a ML/TF risk analysis; the procedure by which the obliged entity determines whether the customer or the beneficial owner of the customer is an official (a PEP), a procedure by which the obliged entity determines whether the customer or an entity within the ownership structure of the customer is an offshore legal person, as well as s well as the manner of applying other provisions of AML/CFT legislation.

The obliged entity supervised by the Administration for the Prevention of Money Laundering (hereianfter refered to as: the obliged entity) shall be understood to mean a legal person and an entrepreneur providing accounting services and a factoring company.

The aim of these Guidelines is to define bases and/or presumptions based on which an obliged entity should conduct ML/TF risk asssessment with relation to its own business operations, as well as the manner of conducting risk assessment/analysis on a single case, that is, at the level of a person buisness cooperation is established with (a client, an associate, a contracting party, etc.), for the purpose of uniform implementation of the provisions of the AML/CFT Law and establishing an effective AML/CFT system within the obliged entity.

The Guidelines are aimed at raising awareness of the obliged entities of their role and position within AML/CFT system, as well as at stressing the importance of the implementation of all laws and bylaws in this area, because that is the only way to comba ML/TF efficiently.

General Part of these Guidelines is applied by entreperenurs and legal persons providing acounting services and factoring companies, whereas the Specific Part of these Gudelines is applied by the obliged entity the Sepeciifc Part refers to, given the circumstances referring to the obliged entity presented herein.

GENERAL PART

The concept of 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 financialy system, they cause economic disruptions and instability, damage cthe country's reputation and jeopardise national security. ML/TF risks occur also as a result of the failure to comply with regulations, where the obliged entity can also be exposed to the reputational risk to a significant extent in case of being penalised by the supervisor.

When it comes to money laundering, the initial assests always derive from illicit acitivites, 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 soruces of their assets but concealemnt of the nature of the financed activity. When individuals wish to invest money generated through legitimate activities into the 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 includes the analysis of both ML risk and TF risk.

Money laundering - definition and stages

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

Money laundering for the purpose of 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. For the purposes of this Law, money laundering shall include the activites above when committed abroad as well.

When proceeds originate from a criminal offence, the perpetrator seeks ways to use the money so as not to attract attention of the competent authorities. Therefore, the perpetrator carries out a series of transactions serving to make the money appear to be legitimate. There are three main stages in money laundering:

1. **Stage I:** placement, means the disruption of the direct link between the money and the iliict activity through which it was acquired. At this stage, the illicit money is placed into

the financial system. The money is placed into bank accounts, most frequently through a legal activity where payments are made in cash. One of the ways is to establish a fictitious company that has no business activities but only serves to deposit dirty money, or to structure large sums of money and then to deposit it into 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 is placed in the legitimate financial system, it is then moved from the account to other accounts, held by companies, with the aim to simulate a business activity 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 criminal activity it derives from.
3. **Stage III**: integration. Dirty money appears to be the money originating from a legal activity. A frequent method of integration of dirty money into legal financial flows is through the purchase of real estate or control packages of shares in joint-stock companies, which is an example of concentration of a large scale dirty capital, exactly the aim of money launderers. Integration focuses on market value, i.e. to what can be bought and sold. Leasing a piece of real estate is legitimate, and the revenue from the lease is not suspicious. Money is often invested in companies facing difficulties in their business operations, after which they continue operating successfully and the revenues constitute legitimate proceeds. When dirty money comes to this stage, t is very difficult to detect its illicit origin.

Illegal acquisition of assets is the main, if not the only, motive for concerting the commission of criminal offences. In order to enjoy the proceeds from crime, the assets must be disguised to look legitimate.

Terrorist Financing - definition and stages

For the purposes of the AML/CFT Law, terrorism financing is understood to mean the provision or collection of assets, or an attempt to provide or collect assets, with the intention of using them or in the knowledge that the they may be used, in full or in part:

1) for the execution of a terrorist act;
2) by terrorists;
3) by terrorist organizations.

Terrorism financing is also understood to mean aiding and abetting in the provision or collection of assets, regardless of whether a terrorist act was committed or whether assets were used for the commission of the terrorist act, whereby the main goal need not necessarily be the concealment of the source of funds but the concealment of the nature of activities for whose financing such assets were intended.

There are four stages in terrorist financing:

1. collection of funds from legitimate business or from criminal activities (for example, donations, drug traficking, extortions, embezzlements, etc);

2. holding and/or keeping of the funds collected (in accounts directly or in accounts held by intermediaries). [1]

3. transfer of the collected funds to terrorists so that they could be used for terrorist actions (through money transfer system or through informal transfers);

4. the use of funds to purchase explosives, weapons, equipment, to finance training camps, propaganda, political support, provision of shelter, etc.

Risk assessment

Risk assessment is conducted as follows:

- at the state level (national risk assessment);
- at the level of an obliged entity;
- at the level of a business relationship (a client).

Pursuant to Article 6 of the AML/CFT Law, obliged entities are required to take into account the national risk assesment when conducting risk analysis at the level of an obliged entity and/or risk analysis with regard to all their business operations (so called self-risk assessment), as well as when conducting risk assessment at the level of a business relationship (a client).

When conducting risk analysis at the level of the obliged entity and/or with regard to all its business operations, the obliged entity is required to take into account the level of threat and sectoral vulnerability of the sector it belongs to according to the findings of national risk assessment; if the client is also an obliged entity from AML/CFT Law , when conducting risk analysis at the level of a business relationship (of a client), the obliged entity is required to take into account the level of threat and sectoral vulnerability of th sector the clientt belongs to. In particular, when conducting risk analysis at the level of the obliged entity, the obliged entity is required to take into account the risk of the form of a legal person, the former being assessed within NRA, to which the obliged entity belongs; when conducting risk analysis at the level of a business relationship (a client), the obliged entiy is required to take into account the level of risk of the type of the legal person, regardless of whether the client is an obliged entity according to AML/CFT Law.

In addition, in line with Article 6 of the AML/CFT Law, the risk analysis must be done in accordance with the guidelines issued by the relevant supervisory authority.

if the client is high-risk according to the Law itself (e.g. if the client or the beneficial owner of the client is an official or is a legal person that is or in whose ownership structure there is an offshore legal person or the client was not physically present when establishing a business relationship), the obliged entity is obliged to classify such a client as high risk for money

[1] This phase can also occur after the third phase, i.e. after the phase of transferring the collected funds.

laundering and terrorist financing and to apply enhanced CDD. Therefore, when conducting a risk analysis, such a client must, according to the Law itself, be classified as high risk.

The obliged entity is required to conduct the risk analysis in accordance with the guidelines of the supervisory authority, that is, when conducting a self-assessment, the obliged entity is required to take into account the criteria for risk analysis at the level of an obliged entity, as defined by these Guidelines, and when analyzing the risk at the level of busines operations (of a client) the obliged entity is required to take into account criteria for risk analysis at the level of business operations (a client), that is, to assess geographical risk, a client risk, a service risk; factoring companies are required to assess a transaction risk in additon to the previously stated, the criteria of which are defined in a separate part of these Guidelines

ML/TF risk assessment at the country level (national risk assessment)

The country must conduct a national ML/TF risk assessment (NRA) and define measures and activities that need to be implemented in order to mitigate the risks identified. The findings of the NRA provide the necessary information to the obliged entities and serve as the starting and mandatory point in risk assessments that the obliged entity will conducat itslef at the level of an institution.

ML/TF NRA indicates what sectors and practices in a country pose a potentially higher and lower risk respectively, of money laundering and terrorist financing so that the country could adequately respond to the identified risks, by applying a range of measures and activities, and 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.

NRA in the Republic of Serbia was adopted in September 2021. [2]

For the purpose of the national risk assessment conducted in 2021, data were collected for the period from January 1, 2018 to December 31, 2020, and the assessment was conducted through thematic units as follows:

1) National money laundering risk assessment (performed according to the methodology of the World Bank)
2) Terrorism financing risk assessment and NPO sector risk assessment (performed according to the methodology of the World Bank);
3) money laundering and terrorist financing risk assessment in the digital assets sector (performed according to the methodology of the Council of Europe);
4) Risk assessment of the financing of the proliferation of weapons of mass destruction (performed according to the methodology of the RUSI Institute for Defense and Security Studies that is, the Guide for the implementation of the national risk assessment of the financing of proliferation was used with the participation and consultation of experts from the USA and the EU).

[2] http://www.apml.gov.rs/uploads/useruploads/Documents/NRA2021.pdf

The novelty in this cycle of national risk assessment is that the Republic of Serbia has for the first time conducted both an assessment of the risk of money laundering and the financing of terrorism in the sector of digital assets and an assessment of the risk of financing the proliferation of weapons of mass destruction.

A concnept of risk, risk assessment, threat, vulnerability and consequences

- ***Risk*** is a function of three factors: threat, vulnerability, and consequence.
- - Risk assessment is a product or process that is arrived at, that is, that is carried out on the basis of a methodology that seeks to determine, analyze and understand the risks of money laundering and terrorist financing, and is the first step towards their mitigation. Ideally, a risk assessment includes assessments of threats, vulnerabilities (weaknesses), and consequences.
- - A threat is a person or a group of persons, an object or an activity that has the potential to cause harm, for example, to the state, society, economy, etc. In the context of money laundering and terrorist financing, this means persons engaged in criminal activity, terrorist groups and their supporters, funds and assets in the broadest form at their disposal, as well as past, current and future money laundering and terrorist financing activities.
- - The concept of vulnerability or weakness used in risk assessment refers to parts of the system through which a threat can be realized or which can contribute to or enable the performance of activities that a threat implies, that is, a series of mechanisms that can be a deterrent to the realization of a threat.
- - Consequence refers to the impact or damage that money laundering or terrorist financing can cause and includes the effect that the preceding crime and terrorist activity can have on financial systems and institutions, as well as on the economy and society in general. - The consequences of money laundering or terrorist financing can be short-term or long-term and reflect on the population, specific communities, business environment, national or international interests, as well as on the reputation and appeal of the financial sector in the country.

When we talk about risk assessment, it is necessary to keep in mind that the assessment includes inherent risk and residual risk. Inherent risk means the result of threats and vulnerabilities that are specific for a sector. This level of risk is influenced by various factors, and above all, the quality and effectiveness of measures for prevention and repression applied by competent authorities. These factors can reduce the level of risk, if there is consistent and effective law enforcement, developed supervision, adequate capacity, etc., ultimately resulting in a lower residual risk. A number of control mechanisms that contribute to reducing the risk of a particular product, service, business practice or way of providing a particular product or service can lead to a lower residual risk.

Results of the 2021 national risk assessment

1) National ML risk asssessment - assessment of threats from money laundering, vulnerability from money laundering at the national level and a part related to sectoral vulnerability;

This assessment is a result of the assessment of money laundering threats and national vulnerability to money laundering.

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 ML vulnerability 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".

ASSESSMENT OF MONEY LAUNDERING THREATS

The data collected, processed and analyzed with the aim of determining the frequency of predicate crimes indicate that, excluding property crimes, the most common crimes are still the unauthorized production and distribution of narcotic drugs from Article 246 of the CC[3] , tax crimes, abuse of the position of a responsible person from Article 227 of the CC and the criminal offense of abuse of office from Article 359 of the CC and criminal offenses against legal relations, namely forgery of a document from Article 355 of the CC and forgery of an official document from Article 357 of the CC.

During the national risk assessment in 2021, a list was compiled of 115 criminal offences that can be identified as predicate crimes, that is, criminal offences that precede money laundering, the commission of which generates, directly or indirectly, illicit gain - illegal assets that can subsequently be the subject of money laundering, regardless of whether proceedings for money laundering have also been initiated as part of proceedings for those crimes.

[3] Criminal Code ("Official Gazette of RS" no. 85/05, 88/05 - corrected, 107/05 - corrected, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 and 35/19)

Predicate offenses classified as high-level threats for money laundering include: abuse of the position of the responsible person, tax offences, unauthorized production and distribution of narcotic drugs, abuse of office, illegal crossing of the state border and human smuggling and criminal offences committed by organized crime groups.

Predicate crimes with a medium level of threat for money laundering are fraud, crimes of forgery (of documents and official documents), human trafficking, procuring, illegal trade and illegal storage of goods.

Other offenses can be classified as **criminal offenses with a low level of ML threat**. All other crimes are marked as crimes of a low level of threat for money laundering because the perpetrators of such crimes do not try to "launder" the illegally acquired assets, by concealing its illegal origin, but, as a rule, spend it for ordinary daily needs.

A growing threat in terms of money laundering is posed by environmental crimes, smuggling of protected plants and animals, and the use of agricultural holdings.

The analysis of cases in which persons were prosecuted for money laundering has showed that persons who own registered agricultural holdings and who hold special accounts in banks are often the perpetrators of this criminal offense.

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

The national ML/TF risk assessment of 2021 also included the assessment of cross-border threats from money laundering; In assessing cross-border money laundering threats, 164 countries were analyzed. On the basis of the performed analyses, a list was formed of 29 countries that are relevant from the aspect of cross-borderML threats (11 countries were assessed as a high level of threat; 15 countries were assessed as a medium level of threat, and 3 countries were assessed as a low level of threat).

The sectors exposed to a high level of ML threat are the real estate, organizers of online games of chance and banking sectors. They are followed by the accounting sector as a medium-high exposed sector threat level with a tendency towards high exposure. Sectors that are exposed to a medium-high level of ML threats are money changers and casinos. Sectors that are exposed to a medium degree of ML are real estate agents, attorneys, virtual assets service providers (VASPs), car dealerships, postal operators and factoring companies. In medium threat level with a tendency towards medium low exposures are life insurance companies, and in a medium-low degree threats are the capital market sector, payment institutions and electronic money institutions, auditors and notaries, while financial leasing providers and voluntary pension funds have a low degree of exposure to money laundering threats.

Although investors in construction of residential and non-residential buildings[4] and car dealerships are not obliged entities in terms of AML/CFT Law, they were the subject of ML risk

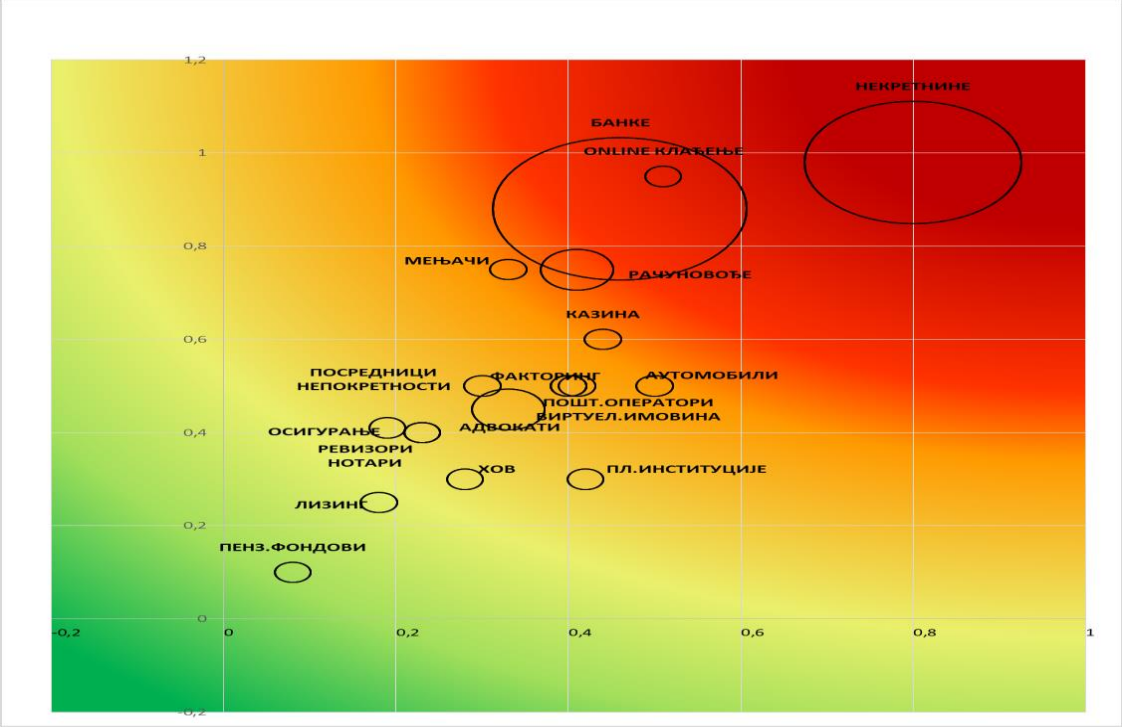
[4] According to the national risk assessment from 2018, real estate agents were separated from investors in real estate, because it was estimated that these are two completely different lines of work, although they are included in the same sector of real estate business. Mediation in the sale and lease of real estate refers to the service, while real estate investors deal with the construction and sale of real estate in all stages of construction.

assessment. According to the results of the national risk assessment of 2021, the real estate sector is the most exposed to the threat of money laundering, while the trade in cars sector is moderately exposed to the threat of money laundering

It is also important to note that the biggest factor in the financial part of the system of the Republic of Serbia is made up of banks, whose balance sheet total amounts to about 90% of the balance sheet total of the entire financial sector, while about 9% refers to the insurance sector, the sector of financial leasing providers and the sector of voluntary pension funds Of all DNFBPs by far the largest market share is accounted for by real estate sector, followed by the games of chance sector, lawyers, accountants, postal operators, notaries public, auditors .

Table of the level of money laundering threats by sector

High	Real Estate
	Organizers of online games of chance
	Banks
Medium high/High	Accountants
Medium high	Currency exchange offices
	Casinos
Medium	Real estate agents
	Attorneys
	VASPs
	Trade in cars
	Postal operators
	Factoring companies
Medium/Medium low	Insurance companies
Medium low	Capital market
	Payment institutions, public postal operator and e-money institutions
	Auditors
	Notaries public
Low	Financial leasing providers;
	Voluntary pension funds



Money laundering risk assessment map

ML vulnerability at the national level

This capability 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 stakeholders in the system for the prevention and repression, the effectiveness of national 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 the 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.

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

Sectoral vulnerability

As national vulnerability is affected by the vulnerability of specific sectors that can be abused for money laundering, in addition to the country’s capacity to defend itself against ML threats, financial and non-financial segments of the AML/CFT system have been analysed.

The sectoral risk analysis was undoubtedly important for the risk assessment.

The financial sector of the Republic of Serbia consists of banking sector, insurance sector[5], providers of financial leasing sector, voluntary pension funds, other providers of payment services and issuers of electronic money, - payment and electronic money institutions, capital markets (broker - dealer companies, banks authorised to deal with securities, investment fund management companies and custody banks), authorized exchange offices and factoring.

In the financial part of the system, the most vulnerable institutions are banks, payment institutions public postal operators and electronic money institutions, followed by exchange offices, factoring companies and the capital market sector, and then life insurance companies, financial leasing providers and voluntary pension funds.

Vulnerability assessment table - financial sector

Financial sector	Vulnerability
Banks	medium
Payment institutions, public postal operator and e-money issuers	medium
Currency exchange offices	medium-low
Factoring companies	medium-low
Capital market	medium-low
Life insurance sector	low
Financial leasing providers;	low
Voluntary pension funds	low

DNFBP sector consists of obliged entities by the AML/CFT Law: real estate agents, organizers of online games of chance, casinos and postal operators, so-called "gatekeepers" which include auditors, accountants, lawyers and notaries.

Also, the DNFBPs include investors in the construction of residential and non-residential buildings and car dealerships, which are not obliged entities by the AML/CFT Law.

Real estate sector, games of chance, accounting agencies and postal operators were identified as the most vulnerable among DNFBPs, followed by awyers, notaries public and auditing companies.

[5] Obliged entities of the Law are insurance companies that have a license to carry out life insurance and insurance mediation companies when they perform life insurance mediation activities; insurance representation companies and insurance agents, who have a license to perform life insurance business, except for insurance representation companies and insurance agents whose work the insurance company is responsible for in accordance with the law.

Vulnerability assessment table - DNFBPs

DNFBPs	Vulnerability
Real estate agents	medium
Organisers of special games of chance in casinos;	medium
Organizers of special online games of chance	medium
Accountants	medium
Postal operators	medium
Attorneys	medium-low
Notaries public	medium-low
Auditing companies;	medium-low

Findings of the 2021 NRA which refer to the entities supervised by the APML

Accountants - According to the assessment, the sector of accountants has medium vulnerability exposure to ML threat with a tendency towards high exposure.

In the reference period, there was a significant improvement of the normative framework, firstly with the amendments to the Law on Accounting in 2018[6], and then with the adoption of the new sectoral law[7] in 2019, primarily by implementing Recommendation 28 of the FATF. Amendments to the Law on Accounting from 2018 introduced a ban on criminally convicted legal entities and natural persons to be founders, owners or members of the management bodies of legal entities engaged in the provision of accounting services, as well as natural persons to engage in this activity as entrepreneurs if they have been convicted for pre-determined criminal offenses, including the criminal offense of money laundering and the criminal offense of terrorist financing. With the adoption of a new sectoral law, the said prohibition was tightened and expanded, so the persons with prior convictions for criminal acts committed in the country and abroad are banned from holding the above said positions. The ban applies both to the accounting firm and to the founders, owners and management structure. The new sectoral law also introduced the obligation for providers of accounting services to be registered in the Register of Accounting Service Providers, which is kept by Serbian Business Registers Agency, based on a previously issued permit by the Chamber of Licensed Auditors (hereinafter: the Chamber), which, in accordance with Moneyval's requirements, introduced the licensing requirement, non-conviction requirement for the founder, beneficial owner, or member of the governing body, and

[6] Official Gazette of RS no. 30/18
[7] Official Gazette of RS", no. 73/19 and 44/21 – other law

a requirement to employ a person with a professional title in the field of accounting or auditing obtained from a member of the International Federation of Accountants An additional mechanism of system protection is reflected in the fact that natural persons are prohibited from being founders, beneficial owners or members of the governing authority in case of serious or repeated AML/CFT violations for as long as the prohibition to provide professional accounting services is in force as an imposed security measure. By adopting this norm, the international standard is fully met and vulnerability is reduced. One of the reasons for revocation of an accountant's license is acting contrary to the AML/CFT regulations, which is when the Chamber revokes the license based on a well-explained proposal of the relevant AML/CFT supervisory authority.

Although a total of 28 trainings were held for accountants in the period from 2018 to 2020, it was noticed that, despite this, there is insufficient understanding and a low level of awareness of the importance of taking actions and measures related to ML/TF by this group of obliged entities, so it is necessary to intensify training for this group of obliged entities.

In addition to the trainings, APML created a new website, the goal of which is to provide a better forum for informing the obliged entities and a manual for accountants with models of internal acts[8] was created, which should contribute to and facilitate the implementation of CDD measures.

Although progress was noted compared to the reference period covered by the previous national risk assessment from 2018 , since the number of submitted reports increased by 217% and data from 26% of submitted reports were forwarded for further processing, bearing in mind the number of registered taxpayers in this sector (over 8,000), it can be stated that the number of submitted reports on suspicious activities is small and that therefore the intention of APML is to intensify training, with a special emphasis on case studies, money laundering typologies, as well as on raising awareness that accountants can be abused by organized criminal groups as well as individuals .

Factoring sector - Factoring companies have been assessed as a sector with medium-low vulnerability and has a medium exposure to ML threat.

This sector is defined by the Law on Factoring[9], which was amended in 2018 in order to prevent persons with prior convictions from being founders and owners of factoring companies. natural and legal persons, who are founders and owners of factoring companies, submit proof, in accordance with the law, that they do not have prior convictions. This obligation also applies to previously established factoring companies.

---

[8] The manual for the application of the Law for accountants is published on the website of APML (http://www.apml.gov.rs/) in the section Library - Professional texts and brochures : http://www.apml.gov.rs/uploads/useruploads/Documents/Preparation-for-the-implementation-of-the-law-on-prevention-of-money-laundering-and-financing-of-terrorism-for-ra%C4%8Dunovo%C4%91e- cir.pdf ,
as in the section What we do - Supervision of accountants and factoring companies - Documents : http://www.apml.gov.rs/dokumenti

[9] Official Gazette of RS, nos. 62/13 and 30/18

In the reference period, covered by the 2021 national risk assessment APML provided education and held 9 trainings for factoring companies. APML made sure the trainings would include new bylaws, such as the Guidelines issued by APML or some new initiatives with regard to AML/CFT. Factoring companies have always responded and actively attended such trainings. These obliged entities demonstrate a high level of compliance. In the period from 2018 to 2020, factoring companies submitted one STR, based on suspicion with regard to the identity of the beneficial owner of the legal representative. This STR supports the claim that factoring companies monitor the risks associated with the client, that is, with the possibility that someone else operates the client's capital.

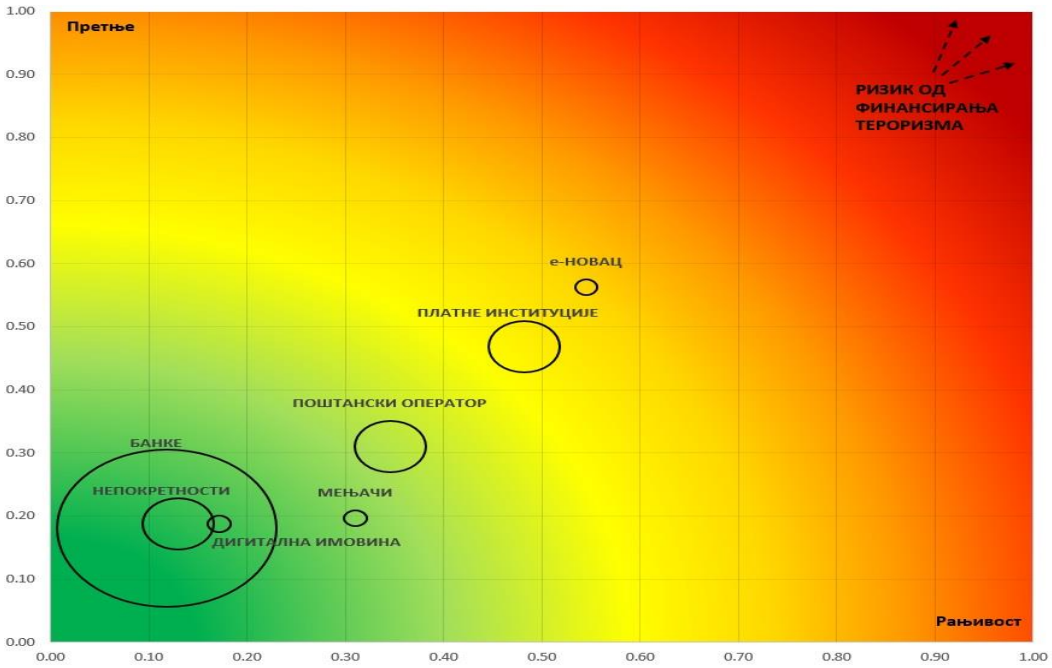
2**) TF and NPO Risk assessment**

National TF risk assessment for the period 2018-2020 was based on the assessment of terrorism threat, national TF threat, TF sectoral risk and the country's vulnerability to TF.

Overall assessment of the TF in the Republic of Serbia is **medium low**, taking into account that the TF threat posed by terrorists and terrorist organizations is assessed as **low.** The TF threat at the national level is assessed as **medium to low.** The sectoral risk of terrorist financing was assessed as **medium.** The country's vulnerability to TF was assessed as **low.**

From the perspective of abuse for TF purposes, the sectoral risk assessment showed that the financial sector is more susceptible to abuse than than DNFBPs. The sector analysis indicates that not all the sectors are of the same level of risk; the products of the following sectors are the most susceptible to the abuse for TF purposes:

- Electronic money issuers;
- Payment institutions;
- The Public postal operator;
- Licensed exchange offices;
- VASPs;
- Real estate agents;
- Banks.



An illustration of sectoral risks

In cooperation with Mihajlo Pupin Computer Systems Institute, the APML developed a search engine for the lists of designated persons sanctioned by the UN, i.e. a tool for searching the database of designated persons. http://www.unsearch.apml.gov.rs The search engine allows all natural and legal persons to check quickly and easily whether they have contacts or any business with designated persons, ensuring a timely implementation of the Law on the Freezing of Assets with the Aim of Preventing Terrorism and Proliferation of WMD[10].

b) NPO Risk assessment

The exposure of non-profit organizations to the abuse for TF purposes in the Republic of Serbia, in the period 2018-2020, is **low to medium** that is, lower than the period covered by the previous national risk assessment, conducted in 2018 .

In the reporting period, associations were not reported in SARs related to TF.

3) ML/TF Risk assessment in VASPs

There is a **medium ML/TF risk** with regard to transactions with virtual currencies and a **low risk** when it comes to investment and user tokens. When it comes to VASPs, there is a **medium** risk.

4) PF risk assessment

PF Risk assessment is **low to medium.**

The use of covert persons and companies that provide support for the proliferation of WMD and " front entities " operating on behalf of persons under the sanctions regimes of the

[10] Official Gazette of RS, nos. 29/15, 113/17 and 41/18

United Nations and international organizations of which the Republic of Serbia is a member can be considered a high degree of threat for the financing of WMD proliferation.

In addition to using front persons, there is also a risk of the abuse of offshore entities and complex ownership structures, politically exposed persons of foreign countries, re-export transactions, forged documents and documentation, etc.

From the aspect of exposure to the risks of financing the proliferation of WMD, the financial system (especially the banking sector and the sector of payment institutions), taking into account the market share of the financial sector, its products and services, as well as the number of clients is more exposed to the possibility of abuse.

In addition to the above, when preparing the national risk assessment from 2021, the risk of a complex ownership structure was also taken into account. Despite the regulations in place and the Centralized Records of Beneficial Ownership, there is a threat to some extent and the use of front persons is one of ever present risks. There is an increased risk when establishing the benficial owner of non-resident legal persons and when trusts and legal arrangements (persons under foreign law) appear in the ownerhip structure.

The analysis of ML cases did not show business entities with a trust in their ownership structure. However, due to the potential ML risk that may arise from a business entity's legal form, clients with trusts in the ownership structure are at a higher risk and are the subject of increased monitoring by the obliged entities.The obliged entity is required to identify the beneficial owner of a customer that is a legal person or person under foreign law, including trust, by obtaining the following data: name and surname, date and place of birth and permanent or temporary residence of the beneficial owner of a customer[11]. The obliged entity is required to enter the aforementioned data in the records of clients, business relations and transactions.

Effects on the system

ML/TF risk has taken into account the assessment of effects for the system in addition to the assessment of threats and vulnerabilities. The effects should be understood as the damage that money laundering could cause and include the impact of a criminal activity on the obliged entity, financial system, society and the economy as a whole. Bearing in mind that threats and vulnerability are assessed as **medium,** the effects on the system should therefore be rated at the same level.

The "path" of dirty money is not easy to spot and identify, which impedes the timely implementation of effective measures for its detection, prevention and suppression. Money laundering is getting new forms every day, through the use of various methods and means. The major negative effects of money laundering can be first seen in the economy, through a decline in

[11] In accordance with the Law, the beneficial owner of the trust is the founder, trustee, protector, beneficiary if designated, as well as the person who has a dominant position in the management of the trust. This provision applies mutatis mutandis to the beneficial owner and other persons under foreign law

public revenues, transparency and efficiency of the financial system and the expansion of the "shadow economy". Currently any increase in the latter would casue negative effects on the entire economic and financial system. Money laundering, as a rule, leads to a decrease in budget revenues due to tax evasion. It is one of the most common unlawful proceeds that are the subject of money laundering. Such situations often further undermine the tax system as they cause an increase in tax rates and liabilities of entities that meet their obligations. All this puts them into an unequal market position and makes it difficult for them to do business.

Risk-based approach:

The risk of money laundering and terrorism financing is the risk of adverse effects on the financial performance, capital or reputation of the obliged entity, due to the use of the obliged entity (direct or indirect use of a business relationship, transaction, service) for the purpose of money laundering and/or terrorism financing.

The work of accountants is one of the key levers of criminal structures in the process of money laundering, for the reason that after a criminal act has been committed, it is necessary to create a semblance of legality for certain transactions through bookkeeping. Involving the accounting sector is very appealing to potential "money launderers" because every accounting document submitted for making an entry, if it is correct in form, will be entered regardless of whether there have been sopme changes in business or not. Accountants can be misused in order to launder illegally obtained money through the entering of fictitious revenues, i.e. revenues arising from non-existent business activities, through inflated invoices; through the entering of inflated invoices, when products and services are invoiced at unrealistically high prices, thereby showing increased income and profit, and creating a false image of making profit; through the false reporting of earnings; through providing advice on tax evasion; through the establishment and management of companies and charities, helping to create complex ownership structures to conceal a complex money laundering scheme; through rigging data in financial statements, etc. In addition to the above, accountants can also provide tax consulting services, which "money launderers", also find appealing, because accountants can provide them with professional advice regarding tax regulations.

The accounting services that "money launderers" are most interested in are as follows:

a) Financial and tax advice - criminals can introduce themselves as individuals seeking financial or tax advice on how to put assets out of the reach of others in order to avoid future obligations;

b) Establishment of business companies - criminals can try to create confusion or conceal the link between illegal assets and the perpetrator by forming corporate mechanisms or other complex legal arrangements;

c) Buying or selling property - criminals can use property transfers as either a cover for transfers of illegal funds (layering stage) or as a final investment of those funds after they have gone through the laundering process (integration phase);

d) Performing financial transactions - criminals can use accountants to perform or facilitate various financial operations on their behalf;

e) Introduction to financial institutions - criminals can use accountants as someone who introduce them to the institution or who act as an intermediary. This can also happen in the opposite direction, ie criminals can use financial institutions to meet accountants.

In addition to the above services, keeping the records incomplete by clients, which is detected by the accountant while providing accounting services to the client, is also a high risk conduct. Also, the preparation, review and audit of financial statements may be exposed to abuse by criminals if there is a lack of oversight by a professional body or the mandatory use of accounting and auditing standards.

Services considered to be an area of particular vulnerability are:

- Establishment of companies

Accountants participate in the formation of companies or sometimes provide advice on initial corporate, tax and administrative matters.

Criminals may look for an opportunity to maintain control over illicit assets while making it more difficult for authorities to discover the origin and ownership of assets. Companies are seen by criminals as potentially useful means of achieving this result. Although fictitious companies, which have no business activities or assets, can be used for legitimate purposes, such as being a vehicle for the transaction of funds, they can also be used to conceal beneficial ownership or enhance the perception of legitimacy. Criminals can also try to abuse "dormant companies", which can be set up by accountants, by seeking access to companies that have been in financial predicament for a long time. This is an attempt to create the impression that the company is reputable and works in regular circumstances because it has been in existence for many years. Inactive companies can also further complicate the corporate structure and further obscure basic and beneficial ownership information.

- Management of business companies

In some cases, criminals will look for accountants who are involved in the management of companies in order to provide more reputation and legitimacy to the company and the given activities. The above ensures that any funds related to the company’s business activities can go thrrough the relevant accountant’s bank account.

- Nominee directors/shareholders

Individuals may sometimes hire accountants or other persons to be nominee shareholders if there are legitimate questions as to the privacy, security or business interests. However,

criminals may also use fictitious shareholders to conceal their ownership of assets. Accountants should identify beneficial owners when establishing business relationships in these situations. This is important in order to prevent illegal use of legal persons and arrangements, by gaining sufficient knowledge about the client to conduct a proper assessment and mitigation of potential ML/TF risks in business relationships. If accountants are required to be nominee shareholders, they should understand the reason for such a request and be sure they can verify the identity of the beneficial owner of the shares and the legitimacy of the purpose.

- - Accounting services for fraudulent accounts and tax evasion, misuse of the client's accounts and services related to insolvency

Criminals can abuse the services provided by accountants to create a sense of legitimacy with fraudulent accounts to disguise the source of funds. For example, accountants can review and sign such accounts for companies that commit criminal acts, thereby aiding in money laundering. Accountants can also handle high value financial transactions allowing criminals to misuse the client's accounts. Insolvency-related services, which may be performed by certain accounting professionals, may also be subject to the risk of abuse by criminals who will cover up the audit trail of money laundered through the company and the proceeds of crime transferred. Accounting services can also be used to assist with tax evasion and VAT evasion.

The risk of money laundering and terrorism financing arises in particular as a result of the failure to harmonise the obligors' business with the law, regulations and internal acts regulating the prevention of money laundering and terrorism financing, or as a result of the mutual incompatibility of internal acts regulating the behaviour of the obligor and its employees in connection with the prevention of money laundering and terrorism financing.

Money laundering and the financing of terrorism is a real and serious problem that obliged entities must face in order not to inadvertently or otherwise encourage it.

ML problem must be approached as a complex phenomenon so as to avoide its negtive effects. The "path" of dirty money is not easy to spot and identify, which impedes the timely implementation of effective measures for its detection, prevention and suppression. Money laundering is getting new forms every day, through the use of various methods and means.

It is necessary for obliged entities to adopt a risk-based approach to detect, assess and understand the risks of money laundering and terrorist financing, in order to focus their resources where the risks are teh greatest and thus implement appropriate risk mitigation measures.

Key elements of a risk-based approach are as follows:

Identification and assessment of risks	Detection of ML/TF risks faced by the obliged entity with regard to clients, services, countries of operation, also taking into account publicly available information on the risks and typologies of money laundering and terrorist financing
Risk management and mitigation	Identification and implementation of measures for efficient and effective ML/TF risk management and mitigation
Continuous monitoring	Defining policies and procedures for monitoring changes in ML/TF risks
Documentation	Documenting risk assessments, policies and procedures for monitoring, managing and mitigating ML/TF risks

Risk analysis (assessment) at the level of the obliged entity (self-assessment)

In the process of development of the risk analysis, the obligor assesses the probability that its business be used for the purpose of money laundering or terrorism financing. The risk analysis in relation to the overall operations of the obliged entity is aimed at identifying the exposure of the obliged entity to ML/TF risk assessment and segments of business operations that should be given priority in undertaking activities for effective management of this type of risk.

The obliged entity is required to undertake self-assessment once a year, by 31 March of the current year at the latest for the previous year, on the basis of the analysis of the self-assessment criteria listed below.

A prerequisite for conducting a risk analysis at the level of the obliged entity is a risk analysis of all clients with whom the obliged entity has an established business relationship, which, in addition to taking into account of the findings of the national risk assessment and mandatory legal provisions, includes geographic risk, risk of a client and risk of a service; factoring companies should include a risk of transaction as well. The criteria for self-assessment are given in the text below.

When assessing the risk at the level of the obliged entity, the obliged entity is required to take into account as a minimum the following:

NRA findings, that is, threats and sectoral vulnerability. According to the results of the national risk assessment from 2021, the accounting sector is assessed as having medium vulnerability with a medium-high exposure to money laundering threats with a tendency towards high exposure, whereas the factoring sector is assessed to have medium-low vulnerability and has medium exposure to money laundering threats Also, during the self-assessment of risk, the obliged entity must take into account the level of risk of its legal form, which is defined in NRA findings, presented below.

if there are any products or services offered by the obliged entity that can be abused for ML purposes;

the size of the obliged entity, whether the obliged entity has a complex ownership structure, the number of employees directly responsible for performing tasks related to the prevention of money laundering and terrorist financing in relation to the total number of employees, the number of employees who are in direct contact with the clients, the way duties and responsiiblities are shared, the frequency of employing new staff, the quality of training, etc.

total number of clients;

number of clients with complex ownership structure;

number of clients by its legal form - according to the results of the national risk assessment from 2021, limited liability companies and entrepreneurs are forms of business entities with a high level of ML threat, joint stock companies and cooperatives with a medium level of threat , other legal forms (limited partnerships and partnerships) with a low level of threat , while the legal form of registered agricultural holdings represents a growing threat, because the control of money flows in these entities is small or almost non-existent, and it has been observed that they are used for money laundering by organized criminal groups. In addition to the above, according to the results of the national risk assessment from 2021, the exposure of non-profit organizations to abuses for the purpose of financing terrorism is rated as low to medium;

assessment of the obliged entity's exposure to cross-border threats (the number of clients who are residents and the number of clients who are non-residents, the number of clients whose beneficial owners are domestic nationals and the number of clients whose beneficial owners are foreign nationals, and if there are beneficial owners who are foreign nationals, from what countries);

- the level of risk of its clients (the number of clients with a low, medium and high level of risk, especially taking into account the number of offshore legal persons, officials (PEPs) and persons who were not physically present during the establishment of the business relationship)

• Number of clients with suspicious actiivities/transactions;

number of suspicious activities/transactions noted in internal reports and the number of STRs submitted to the APML.

Based on the criteria listed above, as well as the measures it takes to mitigate the ML/TF risk the obliged entity assesses its own overall exposure to ML/TF risk as low, medium or high.

The obliged entity is not expected to establish whether the crime of money laundering or terrorist financing has occurred. The main task of the obliged entity is to ensure the availability

of all the necessary CDD information on their clients to assess whether certain patterns of behaviour can be linked to a crime and to what extent and to take all necessary measures according to the AML/CFT Law to submit SARs, while the APML and investigative authorities take the case further to establish whether there is a criminal offense or not.

Risk analysis (assessment) at the level of a business relationship (a client).

As stated above, when conducting risk assessment at the level of a business relationship (a client), an obliged entity shall take the following into account:

- - The findings of the NRA (if the client is an obliged entity by AML/CFT Law, the obliged entity is required to take into account the degree of threat and vulnerability of the sector to which the client belongs, as well as the level of risk of the client's legal form, regardless of whether the client is an obliged entity);
- - imperative provisions of the Law (the Law prescribes cases when the obliged entity is required to classify the client as high risk and to apply enhanced CDD);
- Guidelines of the Administration for the Prevention of Money Laundering (geographical risk, client risk, service risk, and factoring companies must take into account a transaction riks, whose criteria are given in a separate part of these Guidelines).

The assessment of the client risk is conducted not only when establishing a business relationship with the client, but throughout the business relationship, and the level of risk may change. For example, a certain business relationship with a client may initially be assessed as low-risk, and then circumstances may arise that will increase that risk and vice versa. This does not apply to cases that are classified as high-risk based on the Law and to which enhanced CDD must be applied (e.g. when the client is an official (a PEP), when the clent is not physically present during the identification and verification of identity, when the client or the legal person that appears in the client's ownership structure is an offshore legal person, when establishing a business relationship or conducting a transaction with a client from a country that has strategic deficiencies in AML/CFT system).

The degreel of risk at the level of the business relationship (a client) and the types of CDD measures

Based on the performed risk analysis for each group or type of a client or business relationship; the services provided by the obliged entity within the scope of its professional activity or transaction, the obliged entity in accordance with the Law classifies the customer into one of the following risk categories:

- **low ML/TF risk** - at least simplified CDD measures are applied;
- **medium ML/TF risk** - at least general CDD measures are applied;
- **high ML/TF risk** - enhanced CDD measures are applied.

The obliged entity may also envisage additional risk categories with its internal acts.

International standards and AML/CFT Law allow the obliged entity depending on the degree of ML/TF risk to apply three types of CDD measures from simplified to enhanced.

General CDD measures include identification and verification of the identity of a client and of the beneficial owner; obtaining and assessing the information about the intended purpose of the business relationship or transaction as well as ongoing monitoring of the client's business operations and ensuring that they are in line with the nature and business profile of the client.

Enhanced CDD measures include, in addition to general CDD measures include obtaining and assessing the reliability of information about the source of wealth that is or will be the subject of a business relationship and additional actions and measures that the obliged entity undertakes in cases prescribed by the Law, as well as in other cases when it assesses that there is or could be a high degree of ML/TF risk. The obliged entityor defines with its internal act which enhanced CDD measures, and to what extent it will undertake in each specific case.

What additional measures the obliged entity will take when classifying a client in a high-risk category based on its own risk assessment depends on the specific situation (e.g. if the client is classified in a certain category due to the ownership structure, the obliged entity can provide for the obligation to obtain additional data and the obligation to check the submitted documentation through its procedures).

The obligation to undertake enhanced CDD measures exists in the following cases prescribed by the AML/CFT Law:

a) new technologies and services

The obliged entity is required to identify and understand the risks associated with a new or innovative product or service, especially when it involves the use of new technologies or payment methods. New products and new business practices, including new ways of product delivery and the use of new developing technologies (both for new and existing products), especially if there is no clear understanding of them, can contribute to an increased ML/TF risk.

In applying new technologies and new products or services, in accordance with the Law, the obliged entity is required, in addition to general CDD measures, to apply additional measures that reduce the risks and manage the risk of money laundering and terrorism financing (for example, more frequent monitoring of the client for the purpose of determining whether its business is expected, given the knowledge the obliged entity has of the customer, the customer turnover, etc.).

b) an official (a PEP)

The obliged entity shall determine the procedure for establishing whether the customer or the beneficial owner of the customer is an official (a PEP), a member of the close family of an official (a PEP) or a close associate of an official (a PEP).

Customer due diligence measures should be a key source of information about whether the customer is an official (a PEP) (for example, information on the basic occupation or employment of the client). The obliged entities also use other sources of information that may be useful to identify an official (a PEP).

To obtain relevant information for identification of an official (a PEP), the obliged entity shall undertake the following activities:

- -obtain a written statement of the client on whether he/she is an official (a PEP), a member of the close family of an official (a PEP) or a close associate of an official (a PEP);
- -use electronic commercial databases containing lists of officials (PEPs) (for example, World-Check, Factiva, LexisNexis);
- – search for publicly available data and information (for example, the register of officials in the Anti-Corruption Agency);
- –create and use internal database of officials (for example, larger banking groups have their own lists of officials - PEPs).

The number, that is, the sequence of the activities above) undertaken by the obliged entity should enable a reliable determination of whether the client or the beneficial owner of the client is an official (a PEP), a member of the official's close family, or a close associate of an official (a PEP).

The written statement contains the following information:

- name and surname, date and place of birth, permanent or temporary residence and personal ID number of the official who establishes a business relationship or performs a transaction, i.e. for whom a business relationship is established or a transaction is performed, as well as the type and number of the personal document, name of the issuer, date and place of issue;
- the statement on whether the client is an official (a PEP) according to the criteria set out in the AML/CFT Law (in the statement, it is necessary to specify all cases stipulated by the Law);
- information on whether the official is a natural person performing or has performed over the past four years a high-ranking public office in the state or other state or international organisation, whether he/she is a member of the family of the official or his/her close associate;
- data on the period of performing this function;
- information on the type of public office that the official performs or has performed in the last four years;
- data on family relations, if the client is a member of the close family of the official;

- information on the type of business cooperation, if the client is a close associate of the official.

When establishing a business relationship with a client that is an official, a member of the close family of an official, or a close associate of an official, that is, whose beneficial owner is one of those persons, the obliged entity applies enhanced CDD measures. These measures are also applied by the obliged entity when a natural person ceases to perform a public function (a former official), and for as long as it takes to conclude that that person did not abuse the position he held and at least four years from the day he/she ceased to perform that function.

The data and documentation obtained under the procedure shall be kept in the client's file, ten years following the termination of a business relationship.

c) Establishing and verifying identity without the physical presence of the client.

If, during the identification and verification of identity, the client or the legal representative, i.e. the person authorized to represent a legal entity or a person under foreign law, is not physically present in the obliged entity - in accordance with the Law, the obliged entity is required, in addition to general CDD measures to apply additional measures prescribed by Article 39 of the Law which refer to obtaining additional documents, data or information, on the basis of which it checks the identity of the client; additional verification of submitted documents or additional confirmation of information about the client; obtaining information about the reasons for the client's absence (it is necessary to try to establish additional contact with the client by phone, email, Skype, Viber or in another way and to collect another identification document of the client).

d) off-shore legal person

In line with the law, 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. In order to establish if a legal person is an offshore legal person, 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, nos. 122/12, 104/18 and 161/20). If, on the basis of the conducted procedure, it has been established that the client or the legal person that appears in the client's ownership structure is an offshore legal person, the obliged entity is required to take additional (enhanced) CDD measures.

e) countries which do not implement international standards in the area of the prevention of money laundering and terrorism financing

In accordance with the Law, strategic deficiencies in the system for combating money laundering and the financing of terrorism of the state relate in particular to 1) the legal and institutional framework of the state, and in particular to the incrimination of criminal offenses of

money laundering and financing of terrorism, CDD measures, provisions with regard to the storage of data, provisions regarding the reporting of suspicious transactions, the availability of accurate and reliable information about the beneficial owners of legal persons and persons under foreign law 2) authorizations and procedures of competent authorities of those countries in relation to money laundering and financing of terrorism; 3) effectiveness of the system for combating money laundering and terrorist financing in eliminating the risk of money laundering and terrorist financing.

When establishing a business relationship or carrying out a transaction when the business relationship has not been established with a client from a country that has strategic deficiencies in the system for combating money laundering and terrorist financing - the obliged entity is required to apply enhanced CDD.

- **Simplified CDD measures** undertaken in the cases and in the manner prescribed by the Law and the Rulebook on the Methodology for Performing Work in accordance with the Law on Prevention of Money Laundering and Financing of Terrorism ("Official Gazette of RS", No. 80/20 and 18/22, hereinafter: the Rulebook[12])and apply to clients with a low risk of money laundering and terrorist financing. Clients can be classified in this risk category based on the risk analysis conducted. The CDD measures that the obliged entity is required to undertake are the same as the general CDD, except in the case when the client is a state authority, authority of an autonomous province, authority of a local self-government unit, public enterprise, public agency, public service, public fund, public institute or chamber, i.e. a company whose issued securities are included in the organized securities market located in the Republic of Serbia or in a country where international standards are applied at the level of the European Union standards or higher, and which refer to the submission of reports and provision of data to the competent regulatory body, when the obliged entities are not required to determine the beneficial owner of the client. The obligor shall implement an adequate level of monitoring of business operations of the customer so as to be able to detect unusual and suspicious transactions. When there is a suspicion of money laundering or financing of terrorism in connection with the client or transaction to which these CDD measures were applied, the obliged entity is required to perform an additional assessment and possibly apply enhanced CDD.

Continuous monitoring

Frequency of customer monitoring by risk category

[12] http://www.apml.gov.rs/podzakonska-akta

After the obliged entity has classified the clients into categories according to the degree of risk, as follows:

- − low risk of money laundering and terrorist financing;
- − medium risk of money laundering and terrorist financing;
- − high risk of money laundering and terrorist financing;

the obliged entity applies CDD measures during the duration of the business relationship, in frequency and intensity which corresponds to the assessed risk and changed circumstances regarding the client, so that:

- clients classified as low risk are monitored at least once every two years;
- parties classified as medium risk are monitored at least once a year;
- parties classified as high risk are monitored at least once in six months;

Documentation

An approach based on risk assessment also requires documenting the risk assessment, as well as the existence of appropriate internal acts in order to determine the starting points and the application of adequate measures and procedures.

Internal acts

In accordance with the provisions of the Law, the obliged entity is obliged to adopt and apply appropriate internal acts that will, in order to effectively manage the risk of money laundering and terrorism financing, include all actions and measures for prevention and detection of money laundering and financing of terrorism defined by the Law, by-laws on the basis of the Law and these Guidelines. , The obliged entity is required to take into account the established risks of money laundering and terrorist financing in internal acts, whereby those acts must be proportionate to the nature and scope of business, as well as the size of the obliged entity, and must have the approval of a member of the senior management. The obliged entity is required to ensure the implementation of these internal acts by determining the appropriate procedures and internal control mechanisms.

The obliged entity must in particular regulate in its internal acts the following:

- - the development of ML&TF risk analysis;
- procedures and mechanisms for detecting suspicious transactions and/or customers, as well as the manner in which employees will behave after identifying such transactions and the procedures for providing information, data and documentation at the level of the obliged entity;

- -appointing the persons responsible for the implementation of this Law (hereinafter referred to as: AML compliance officer) and their deputies, as well as creating conditions for their work[13];
- measures and actions for monitoring the operations of the customer that it will, in accordance with the risk category of the customer, take or perform in the course of the duration of the business relationship, as well as the conditions for changing its status according to the degree of exposure to the risk of money laundering and terrorism financing.
- examining whether a client is acceptable given the ML/TF risk when establishing business cooperation and during the period the cooperation lasts;
- establishing the risk category of the customer, services, transactions according to risk factors related to ML/TF risk;
- the procedure for conducting CDD measures on the client and the client's business operations in accordance with the established risk category, including the verification of compliance of the activities with the nature of the business relationship usual scope and type of its business, as well as any possible change in its risk category;
- - the procedure for implementing enhanced CDD measures when the client is high-risk according to the Law itself or based on the performed risk analysis, and especially the procedure for determining whether the client or its beneficial owner is an official (a PEP), as well as the procedure for determining whether the client or the legal person that appears in the ownership structure is an offshore legal person;
- - the procedure for regular internal control of the compliance with the Law, in accordance with the Law and the preparation of an annual report on the internal control and the measures taken after that control no later than March 15 of the current year for the previous year with the content prescribed by the Rulebook;
- - the procedure for conducting regular professional education, training and development of employees that perform the tasks of preventing and detecting money laundering and terrorist financing, in accordance with the program of annual professional education, training and development, which is drafted by the end of March for the current year with the content prescribed by the Rulebook[14].
- record keeping, protection and storing of data from such records;

An integral part of the internal acts is also a list of indicators for identifying persons and transactions for which there are grounds to suspect money laundering or financing of terrorism, as well as the list of indicators for identifying suspicious activities related to TF, which contain all the indicators developed by APML and posted on APML website.

[13] Data on the personal name and job title of the authorized person, his deputy and the member of the highest management responsible for the implementation of the Law (notification or decision on appointment with the specified data), as well as any change in that data, the obligee is obliged to submit to the Directorate for the Prevention of Money Laundering at the latest within 15 days from the date of appointment.

[14] In addition to the above, the obliged entity is required to make an official note (a memo) on the conducted training, the content of which is also prescribed by the Rulebook.

http://www.apml.gov.rs/srp49/dir/Indikatori.html In addition, obliged entities can supplement the list of indicators with the trends and typologies of money laundering known to them, as well as according to the circumstances arising from the obliged entites' business activities.

The list of indicators for identifying suspicious transactions is the starting point for the obliged entity when identifying suspicious activities of a client. In the process of determining the elements for classifying a transaction as suspicious, the indicators developed by the APML as a supervisory authority should be taken into account. However, a transaction can be suspicious without any links to any indicator. In that case, the obliged entity should look at the broader framework, because the obliged entity knows its party best, and in this sense, it can assess that the transaction is suspicious, even though it cannot be classified under any of the indicators posted by the APML. On the other hand, in the event that a transaction can be characterized as suspicious based on an indicator of APML, this does not mean that the obliged entity must immediately submit a STR to APML but that the client should be closely monitored; depending on emerging circumstances, the obliged entity will assess whether a STR should be made to the APML. A SAR is made on the form that is an integral part of the Rulebook.

If an employee in an obliged entity who is in direct contact with a customer suspects that there is a risk of money laundering and terrorism financing in relation to that customer or their transaction, they are obliged to make an internal written report thereon and, within the deadline and in the manner determined by the internal act of that obliged entity, to send it to a person in charge exclusively of the implementation of the Law and other regulations governing AML/CFT (hereinafter referred to as: AML compliance officer). This report should include such information on the customer and transactions that enable a AML compliance officer to assess whether the customer or the transaction are suspicious.

If on the basis of this report or other information on ML/TF risks directly known to the AML compliance officer they assess a transaction as suspicious – the AML compliance officer further acts in accordance with the Law, and if it does not assess so – the officer is obliged to make a note (a memo) on that assessment.

In addition to drafting internal documents, the obliged entity is required to document all actions and measures it undertakes with respect to the client in accordance with the Law.

Identification of the client, its representative, attorney, beneficial owner, risk analysis of the client, entering data into the records (all actions and measures) are carried out when establishing a business relationship with the client, and all data and documentation are regularly updated and stored in the business documentation. Identification of the client is carried out by inspecting the documentation from the official public register of the country where the client has its registered seat or by directly inspecting the documentation, i.e. by inspecting the personal document, on whose paper copies or printed excerpt there is the date, time and the name of the person who has inspected the document, that is, the copy of the document in electronic form contains a qualified electronic stamp, and/or a qualified electronic signature with an related time stamp. In addition, a digitalized document and the copy of documentation is understood to be

the copy of documentation and/or the printed excerpt of a personal document and it can be stored in paper or electronic form.

Also, the obliged entity is required to keep data and related documentation on the implementation of the Law for ten[15] and/or five[16] years, respectively.

SPECIAL SECTION

The Special Section of these Guidelines is applied by the obliged entity to which the section applies, given the specific circumstances related to risks.

1. Types of risks in entrepreneurs and legal persons 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 line of business. Where other types of risks are identified, and depending on the specific features of business activities, the obliged entity should cover in their assessment such types of risk too.

I Geographical risk means a risk determined by the geographical area of the country of origin of the client, its owner or majority founder, the beneficial owner or person otherwise controlling the client's operations or of the country of origin of the person conducting a transaction with the client.

The factors based on which it is determined whether a particular country or geographic location carries a 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 those not applying adequate AML/CFT measures;

3) countries designated by credible institutions (FATF, UN, etc.) as those 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.

5) countries that have been named by credible sources for not providing beneficial ownership information to the competent authorities, which can be determined from FATF mutual assessment reports or reports from organizations that also take into account different levels of

[15] For data and documentation related to the party, established business relationship with the party, performed risk analysis and executed transaction, from the day of termination of the business relationship.

[16] For data and documentation about the authorized person, deputy authorized person, professional training of employees, performed internal controls since the day of termination of duties of the authorized person, performed professional training or performed internal control.

cooperation, such as reports from the OECD Global Forum on compliance with international standards of tax transparency. The list of countries with strategic deficiencies in their AML/CFT systems is published on the APML website[17]. 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/juridictions 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 the evidence from credible sources, such as assessment of national AML/CFT systems by FATF and FSRBs (e.g. Moneyval) or the published follow-up reports for the country, have obligations stemming from the law to fight ML and TF in line with FATF recommendations and effectively implement these obligations.

Clients who have a contractual relationship or do business with entities registered in offshore areas carry a higher ML/TF risk. For instance, a client will be identified as carrying a high risk if it trades in services with a client whose registered office is in a country with a preferrential tax system. This was reflected in the NRA, having examined case studies, ML convictions and criminal groups' behaviour typologies, especially in terms of organized criminal groups; an obliged entity must be aware of the assessed cross-border threats and carefully analyse relationships where offshore zones and countries of the region appear.

Even though certain countries apply the AML/CFT standards, this does not mean that they will immediately be placed in the group of low-risk countries; the obliged entity must carefully approach relvant typoogies and ML cases, which indicate a higher risk in certain countries.

[17] http://www.apml.gov.rs/vesti/clanak/jurisdikcije-u-visokom-riziku-i-pod-pojacanim-pracenjem-fatf-februar-2021

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 trades in goods with a client from a country in the region as such a relationship is economically justified.

Or for example, a client may be low-risk if it is registered for trade in goods and if, judging by subsequent business operations all transactions with suppliers and buyers are linked to the line of business and the registered seat is not in a country/jurisdiction that may indicate a potentially higher risk.

II The client risk - an obliged entity asesses the 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 providing the required documentation or the obliged entity suspects that the documentation is false or incomplete; the client does not know where business documentation is stored;

- a client often changes its accountants;

- a client has no employees or business premises, which is inconsistent with the volume of its business operations; the client often changes the name, registered seat, ownership structure, etc.

2) the client where due to the organisational structure, legal form or complex and unclear relationships, it is difficult to determine the identity of the beneficial owners or persons who control them, such as:

- foundations, trusts or similar legal arrangements,

- charity and non-profit non-governmental organisations,

- offshore legal persons 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) agricultural holdings;

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

5) officials (PEPs), in accordance with the AML/CFT Law;

6) private investment funds;

7) clients whose offer to establish a business relationship was rejected by another obliged entity, tha is, persons with bad reputation;

8) clients whose source of funds is unknown or unclear and/or cannot be proved by the client.

9) a client who has lived abroad for a long time, having no proof of employment, and yet deposits a large sum of money to open a legal person which will be engaged in the provision of services (hospitality services, consulting services, marketing services, event management services, etc);

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

Additionally, if the obliged entity assesses that a client, which is an offshore legal person or a legal person whose ownership structure features an offshore legal person, has a complex ownership structure (such as a large number of legal persons 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 legal persons), the obliged entity must obtain a written statement from the beneficial owner or the proxy of the company and consider whether there are reasons to suspect ML or TF in the case, and to make an official note (a memo) about it, which wil be kept in accordance with the Law.

An obliged entity must pay increased attention if it enters into a business relationship with a client which deals with: trade in real estate, investments, construction activities, property development, trade in goods and services, if it handles large amount of money frequently without supporting documentation, persons that invest in securities.

The situations described in the national risk assessment indicate a higher risk involving the above-mentioned activities. All the activities listed, which are recognized by the client, deserve more significant attention and risk assessment, and should be monitored and assessed more often.

III Service risk includes the following:

1) operations that differ significantly from the usual operations of a client engaged in similar line of business, as well as operations that do not have economic justification (e.g. frequent trading in securities by depositing cash into special - purpose accounts, promptly followed by selling below the price - the so-called trading in securities with a planned loss;unexpected loan repayment before the due date or within a short period from the date of loan approval; withdrawal of funds

from the individual account of a member of a voluntary pension fund within a short period after their payment) ;

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

3) loans to legal persons, and in particular the loans provided by founders from abroad to a legal person in the country without economic justification;

4) payment for consulting, management and marketing services, as well as other services for which there is no determinable value or price in the market;

5) payments for goods and services to partners from offshore destinations, while it is clear from the documentation that the goods originate from the countries of the region;

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

7) frequency of transactions on the basis of advance payment for the import of goods or provision of services where it is not certain that the goods will be actually imported or services provided;

8) over - or under-invoicing for goods or services; multiple invoicing; multiple payments/withdrawals for goods and services or payments to multiple suppliers for the same goods; misuse of write-off of goods (the client frequently writes off significant portions of the sold goods due to various factors, for instance due to force majeure, perishability, losses due to transportation, inadequate storage, breakage, etc, without such situations actually occurring).

9) a client pays for goods and services using electronic banking, and has no relevant documentation to present to the accountant;

10) a client pays for life insurance in large one-off transactions for all employees;

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

2. T**ype 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 factoring business, the obliged entity should cover in their assessment those types of risk too.

I Geographic Risk The factors based on which it is determined whether a particular country or geographic location carries a 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 those not applying adequate AML/CFT measures;

3) countries designated by credible institutions (FATF, UN, etc.) as those 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.

5) countries that have been named by credible sources for not providing beneficial ownership information to the competent authorities, which can be determined from FATF mutual assessment reports or reports from organizations that also take into account different levels of cooperation, such as reports from the OECD Global Forum on compliance with international standards of tax transparency. The list of countries with strategic deficiencies in their AML/CFT systems is published on the APML website[18]. 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/juridictions 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 the evidence from credible sources, such as assessment of national AML/CFT systems by FATF and FSRBs (e.g. Moneyval) or the published follow-up reports for the country, have obligations stemming from the law to fight ML and TF in line with FATF recommendations and effectively implement these obligations.

Clients who have a contractual relationship or do business with entities registered in offshore areas carry a higher ML/TF risk. For instance, a client will be identified as carrying a high risk if it trades in services with a client whose registered office is in a country with a preferrential tax system.

[18] http://www.apml.gov.rs/vesti/clanak/jurisdikcije-u-visokom-riziku-i-pod-pojacanim-pracenjem-fatf-februar-2021

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 trades in goods with a client from a country in the region as such a relationship is economically justified.

Or for example, a client may be low-risk if it is registered for trade in goods and if, judging by subsequent business operations, all transactions with suppliers and buyers are linked to the line of business and the registered seat is not in a country/jurisdiction that may indicate a potentially higher risk.

II Client risk

1) An obliged entity assesses on its own the risk of the client, based on generally accepted principles and its 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:

- a client transfers claims for goods that are not typical of its business (e.g. a medicine manufacturer handles frozen fruits);
- a client transfers claims from debtors, which are not consistent with economic potential of the transferor or debtor, or with the line of business;
- client offers guarantees of third parties without any business logic or of persons with bad reputation;
- economic dependence or relation between the client and factor company management;
- knowledge of the way the factoring company operates;
- frequent and unexpected establishment of business relationships with several obliged entities having the same line of business, without economic justification;

2) situations where

- - due to the structure, legal form or complex and unclear relationships, it is difficult to determine the identity of a client's beneficial l owner or persons who managethe client, such as e.g. offshore legal persons with an unclear ownership structure that were not established by companies from a country that applies AML/CFT standards at the level of the standards prescribed by the Law;
- There is a fiduciary or other similar legal arrangement with unknown or concealed owners or management (i.e. a person under foreign law 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);
- There is a complex status structure or complex ownership chain (complex ownership structure or complex ownership chain hindering or preventing identification of the client's beneficial owner or persons indirectly providing assets to the client, which gives them the insight into business operations, which may have a significant effect on decision-making on the finance and business by the senior management of the client).

3) foreign arms dealers and weapon 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 (proxies) only;

6) companies 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 publicly known for such a reputation or the client had a previous bad experience with them, etc

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

9) officials (PEPs), in accordance with the AML/CFT Law;

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

III Transaction risk

Transaction risk includes the following transactions:

1) 1) transactions that significantly differ from the standard behaviour of the customer;

2) 2) transactions that are not economically justifiable;

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

4) 4) transactions in which the client refuses to provide the entire documentation, as well as transactions in which the documentation does not correspond to the way of conducting the transaction itself;

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

6) 6) transactions that were intended for persons or entities against whom the measures of the United Nations or the Council of Europe have been imposed, as well as transactions that the client would perform in the name and on behalf of the person or entity against whom the measures of the United Nations or the Council of Europe have been imposed.

IV Service risk

Service risk refers to the following risk-carrying services:

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

2) the services assessed by the staff of an obliged entity as carrying high risk, based on the staff's experience;

3) services that carry a high ML/TF risk include all bearer negotiable instruments, negotiable instruments issued to a fictitious recipient, endorsed without restrictions or in other forms that allow the transfer of title upon delivery, and all other incomplete instruments that are signed without the recipient's name being specified.

In addition to the above criteria, the obliged entity should also cover other types of risk when identifying the level of the client risk, service risk or transaction risk, as follows:

-a client's size, structure and line of business, including the volume, structure and complexity of business activities the client undertakes;
- 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 client, business relationship, service or transaction can carry a higher risk.

Transitional and final provisions

The Guidelines for assessing ML/TF risk for entrepreneurs and legal entities engaged in the provision of accounting services and for factoring companies of 15 May 2020 shall be no longer valid as of the day these Guidelines start to apply.

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 30 days after they have been publishede on the APML website.

Done in Belgrade, on 22 March 2022

Acting Director

Željko Radovanović