

 Republic of Serbia

 **MINISTRY OF FINANCE**

 **TAX ADMINISTRATION**

 No. 000-424-00-94/2018/1

 Belgrade, 25.12.2018

Under Art. 4, para 1, item 8). 6, para 1, item 4), 104, para 1., 110, para 2 and 114, of the Law on prevention of money laundering and financing of terrorism („Official Gazette of RS“ no. 113/17-hereinafter the Law, Director of Tax Administration brings

**GUIDELINES FOR ASSESSMENT OF RISK FROM MONEY LAUNDERING AND FINANCINGHOF TERRORISM FOR OBLIGED ENTITIES THAT ORGANIZE SPECIAL GAMES OF CHANCE THROUGH THE MEANS OF ELECTRONIC COMMUNICATION**

Tax Administration, pursuant to Art. Article 104, paragraph 1, item 4) and Article 110, paragraph 2 of the Law, as a state body responsible for inspection in the field of games of chance, supervises the application of this law by the obliged entities referred to in Article 4, paragraph 1, item 8) i.e with organizers of special games of chance on-line, who perform their activities on the basis of a special law.

Guidelines for the prevention of money laundering and terrorist financing are adopted in order to reduce the risks to which the taxpayer is exposed in order to adequately assess the susceptibility to the risk of money laundering and terrorist financing, risk analysis and regular updating, developing risk identification and risk management procedures, in accordance with Article 6 of the Law in order to apply uniformly the provisions of the Law on Prevention of Money Laundering and Financing of Terrorism and on the basis of it adopted guidelines from the body competent to supervise the implementation of this Law.

The Tax Administration may, on the basis of Article 114 of the Law, make, independently or in cooperation with other bodies, recommendations or guidelines for the application of the provisions of this Law.

Pursuant to legal provisions, the risk of money laundering or terrorist financing is the risk that the party will abuse the organization of special games of chance on-line for money laundering or terrorist financing, that is, the party or transaction will be directly or indirectly used for money laundering or financing of terrorism.

The aim is for organizers of on-line games of chance to establish effective systems to prevent the receipt, giving, substituting, storing, disposing or otherwise handling of, or in relation to assets acquired through the commission of a criminal offense, to finance specific games of chance in casinos as free activities, not to be used in the money laundering or terrorist financing system.

In performing its registered activity, the taxpayer must comply with the legally prescribed obligations, which regulates the field of detecting and preventing money laundering and terrorist financing and to ensure compliance with the prescribed measures and activities at all levels, so that the entire business of the taxpayer is carried out in a legally prescribed manner.

Based on the updated National Risk Assessment of the Risk of Money Laundering and the Assessment of the Risk of Financing Terrorism, the organizers, through electronic communications, belong to the sector that is assessed as medium-vulnerable in relation to other non-financial sectors and have high exposure to money laundering threats.

**RISK-BASED APPROACH**

**The concept of risk**

The risk is a function of three factors:

1. **threats** that include all actions that the people involved in criminal behavor are undertaking to conceal and obscure the origin of the proceeds of crime and create the impression that the property is acquired legally and use the money so acquired without incurring any doubts;

2. **vulnerabilities** are all things that crime groups can use by threatening, to support or facilitate their activities to use illicitly acquired funds to factors that present weaknesses in the system of prevention of money laundering and financing of terrorism. This is all that the makes a taxpayer attractive for money laundering and financing of terrorism and the exposed to risk of money laundering or terrorist financing (eg. attractiveness or susceptibility to money laundering and terrorist financing, insufficient knowledge of regulations regulating this area, inadequate application of legal regulations, etc.). The aim is for the ogranizers of on-line games of chance to direct their capacities to those factors that are weak in the system for detecting and preventing money laundering and terrorist financing and control system in order to improve the effectiveness of the system of measures and actions to combat money laundering and terrorist financing and its capacities in this area;

3. **the consequences** represent everyting that relates to the impact or damage that money laundering or terrorist financing can cause, and includes the impact of criminal or terrorist activities that may negatively affect the economic, political, security and social structure of the state. Due to omissions in the prevention of money laundering and terrorist financing, the organizer of special games of chance on-line may be at risk of violating reputation and to be subjest to the prescribed penalty.

When assessing threats, organizers of special games of chance on-line should start from the results of the updated National Risk Assessment, in which it was estimated that the games of chance sector is exposed to a high level of money laundering threat, taking into account information on criminal proceedings initiated for the criminal offense of unauthorized organization of games of chance as a predicate with money laundering, or criminal proceedings involving employees in this sector, the fact that a large amount of money is being made within this sector, almost exclusively in cash.

Risk exposure is the weakness or vulnerability of obliged entities that can be used by a person or a group of persons through carrying out activities that represent a threat that money laundering and the financing of terrorism can occur.

The level of risk can be reduced by reducing threats and vulnerabilities, or their impact.

The consequences of money laundering and terrorist financing undermine the stability, transparency and efficiency of the financial system of the state, cause economic distortions and instability, jeopardize reform programs, reduce investment, damage the reputation of the country, and endanger national security.

The updated National Assessment of Money Laundering and Threat Assessment from Terrorism Financing, in addition to assessing threats and vulnerabilities, includes an assessment of the implications for the system. They should be understood as the harm that money laundering could cause and involves the impact of criminal activity on obliged entities, the financial system, society and the economy as a whole. The objective of the risk assessment is to draw conclusions which sectors and actions in a country's state system pose a potentially higher risk of money laundering and terrorist financing, which is lower, so that the state can adequately respond to identified risks through a range of measures and activities, and that in accordance with the assessed risks, it can make adequate decisions on the allocation of resources, with the intent to invest more effort and resources into high-risk areas.

**Assessment of risk exposure**

Identifying, assessing and understanding the risks of money laundering are an essential part of the application and development of anti-money laundering and terrorist financing systems in the country. This system includes laws, other regulations, enforcement measures and other measures taken to mitigate the risks of money laundering and terrorist financing. The assessment of the risks of financing terrorism has been made by looking at threats from terrorism, the impact on the threat of financing terrorism, terrorist financing threats and vulnerability to terrorist financing, within the updated National Risk Assessment.

Assessment of risk exposure implies that a taxpayer identifies risks, assesses his exposure from them to money laundering and terrorist financing, which will allow him to see the likelihood of a negative impact that might arise from that risk, as well as the potential effect of that risk on the realization of business objectives.

Risk assessment is carried out in order to allow for control measures that are proportionate to identified risk. This allows obliged entities to focus on those clients, services, transactions and channels of operations that represent the greatest potential risk.

The process of assessing the risk of money laundering and terrorist financing should run as follows:

а) recognizing the risks of operations that are susceptible to money laundering and terrorist financing: identify geographic locations that are specific to obliged entities, parties, services, transactions, etc..;

b) conducting an analysis to determine the likelihood of money laundering and terrorist financing being likely to occur, and what would be their impact in that case: analyze as a combination of the likelihood that this phenomenon might occur and the impact of the costs and damages that might arise in a given situation;

c) risk management: the taxpayer applies risk management strategies based on the analysis and implements the appropriate business policy, i.e appropriate procedures with adequate systems and control mechanisms;

d) supervision over risk and review: develop a supervisory regime through compliance and audit programs with periodic risk reviews.

**RECOGNIZING AND IDENTIFICATION OF RISK**

The first phase involves identifying different types of risks that are classified into four basic categories: geographical risk, client risk, service risk, and transaction risk.

Depending on the specific nature of the business of a particular taxpayer, other categories in which money laundering and terrorist financing can be taken into account, which may be subject to additional reinforced, general or simplified measures in the risk assessment process.

1. *Geographical risk*

Geographical risk involves an assessment of the exposure to the risk of money laundering and terrorist financing which depends on the country of origin of the party, that is, the person performing the transaction, areas or territories where the taxpayer is located, as well as the countries of origin of the ownership and management structure of the games of chance on-line organizer.

Namely, in order to recognize and minimize the geographical risk, it should be kept in mind whether the organization through electronic communications with a particular taxpayer is limited to organizing in one particular country or is licensed in several countries. It is necessary to bear in mind the fact that the Internet operator/provider server is in another country, and whether it is connected to servers from other parts of its business.

At the same time, the fact whether the operator/provider has other websites, through which it is possible to access the gaming account through electronic communications means.

When looking at geographical risks, the important variable is the level of general taxpayer arrangement, the way of organizing games of chance through means of electronic communications, or whether it is also subject to a comprehensive regulatory and supervisory regime that ensures the implementation of effective measures for the prevention of money laundering and financing of terrorism, which especially relates to:

* accessibility and seat of the internet operator/provider (in one or more countries?);
* type of internet hosting (e.g: dedicated server, virtual private server, specialized hosting, etc.);
* possession and management of other providers via electronic communications means in foreign countries by the operator/provider;
* the offer of various types of games via electronic communications from the operator / provider (e.g: "sports book", "premium players", etc.).;
* type and efficiency of existing control mechanisms e.g: electronic and/or physical loyalty clubs that monitor gaming;
* speed and scope of work;
* number of staff, turnover rate and level of experience with taxpayer and its operator/provider, etc..

There is a higher risk of money laundering and terrorist financing by parties originating from the countries:

* against which the United Nations, the Council of Europe, the OFAC, or other international organizations have applied sanctions, embargoes or similar measures;
* which by the credible institutions (FATF, Council of Europe, IMF, World Bank) are designated as countries that do not apply adequate measures to prevent money laundering and terrorist financing;
* which by the credible institutions (FATF, United Nations) were marked as countries that support or finance terrorist activities or organizations;
* which by the credible institutions (World Bank, IMF) are marked as countries with a high degree of corruption and crime.

The Minister of Finance, based on the powers from the Law, establishes a list of countres that apply international standards in the area of prevention of money laundering and terrorist financing at least at the level of European Union standards (the so-called white list), as well as the list of states that do not apply standards in this area at all (so-called black list).

Also, the risk of maintaining VPN (virtual private network - hereinafter: VPN) of the network is reflected in the fact whether the taxpayer has passed the process of determining the conditions for obtaining a license for organizing games of chance through means of electronic communication and whether he has a certificate of fulfillment of conditions informational characteristics of equipment for organizing games of chance through means of electronic communication, conditions of fulfilment and the manner of their examination, and hence whether these conditions are adapted to the country in which games are organized through means of electronic communication or additional adjustment is required.

1. *Client risk*

The taxpayer should describe all types or categories of parties with whom he operates and assess how likely these types or categories of parties will abuse that taxpayer for money laundering or financing of terrorism:

• client category:

- regular/frequentclient;

- irregular/occasional client;

- VIP client;

- random client etc..

• type of client:

- regular/frequent client, performing small to medium transactions;

- regular/frequent clilent, performing medium to large transactions;

- random client, who is a citizen of the Republic of Serbia;

- random client, who is not a citizen of the Republic of Serbia, etc.

The client risk involves assessing whether a party is associated with a higher risk of money laundering and terrorist financing and, on the basis of its own criteria, the taxpayer determines whether a client represents a higher risk on the basis of the performed categorization, with a previously performed assessment whether the organizational model of the organizer through the electronic communications means is based on any of the following options:

- attracts a large number of clients that play with relatively small amounts of money;

- attracts a small number of clients that play with relatively large sums of money.

 Higher risk represent:

1. regular clients whose usual behavior changes:

- a regular/frequent client that performs small to medium transactions, starts to spend larger sums of money;

- a regular/frequent party that performs a medium to large transaction, starts to spend significantly less money, but more often participates in games of chance, etc.;

1. clients representing politically exposed persons, or domestic and foreign officials;
2. clients from the SME sector;
3. clients from international corporations;
4. random clients, etc.

Obliged entities can easily identify customers with personal information, including name, home address, and date of birth. All this information must be verified. It is also useful to obtain information on "sources of funds" and the level of legitimate income (e.g occupation). This information can help obliged entities evaluate whether the level of gambling is within their approximate income or is suspicious. Evidence of identity can be verified by means of documents obtained from a client (e.g passport, driver's license, bank statement, utility bills, etc.), via electronic evidence.

Electronic evidence of identity: business without "face-to-face" may carry certain risks and requires an alternative or additional compliance method to compensate for the fact that obliged entities are not able to check the physical appearance of the client based on photographic identification documents. These methods rely on new technologies including the deposit and withdrawal methods provided on the website, when checking the customer's IP address, and if the taxpayer uses software systems to help control identity, the software should access a range of positive and negative checks.

Although not available in all countries, public data sources can be particularly valuable for the identification of politically exposed individuals and individuals who are subject to various sanctions as a result of organized crime and/or terrorist financing activities. When available, and where permitted by domestic law, the taxpayer can:

- subscribe to a national and/or international reporting agency that offers on-line or telephone search of parties, which can often provide historical data and information about the clients of other obliged entities (in connection with: individual application for a loan, that the client has outstanding debts with another taxpayer; etc.);

- use the public on-line search engine for a database that does not require subscription;

- subscribe to data research agencies documenting criminal records, employers, occupations, property locations, etc..;

- subscribe to organizations that allow search for different business activities, legal sources, and media, or documents in order to verify clients on questionnaires that provide personal information to clients (e.g name, date of birth, address, place of birth) from commercial databases.

The size of electronic "evidence" in relation to the obtained width and quality of data and the degree of data support provided by the client can provide a useful basis for evaluating the service offered by the taxpayer. Several commercial agencies that access many of the data sources available on the Internet browser can provide operators/providers with complex and comprehensive electronic verification via a single interface. As agencies use databases and derived negative information, they can therefore access high-risk warnings using specific data sources to identify high risk (for example: known identity frauds or inclusion on the list of sanctions). Positive information relating to the full name, current address, date of birth, can prove that an individual exists, and some may offer a higher degree of trust than others. Negative information includes reviewing lists of people known to be involved in fraud, including identity frauds and registered individuals. Verification against such information may be appropriate in the case of other factors that pose an increased risk of fraud for phishing. When electronic identification systems are used, the operator must be satisfied that the data provider is "broad, reliable and accurate". The operator must also ensure that the electronic check process satisfies the standard level, i.e the certificate prescribed by law and that the supervisory authority can rely on them (example of a check: one match to the full name and current address of the party, and another match to the full name of the client and to her current address and date of birth).

Determining whether individuals are politically exposed parties is not always easy and can pose difficulties. Where operators need to carry out certain checks, they may be able to rely on an internet browser, or consult relevant reports and databases on the risk of corruption published by specialized national, international, non-governmental and commercial organizations. Resources such as the Corruption Perceptions Index (CPI) of Transparency International, ranging in about 150 countries according to their perception of levels of corruption, can be helpful in terms of risk assessment. If there is a need to carry out a more thorough check, or if there is a high likelihood that an operator has politically exposed clients, the subscription to a specialized database for them may be the only adequate risk reduction tool. New and existing clients do not necessarily have to meet the criteria of politically exposed clients, but this position can be changed over time. Likewise, individuals who were initially identified as politically exposed clients may cease to be functionaries, for example, if they change their job or retire. In many cases, a longer period may be appropriate to ensure greater risk-related risk to the previous position of an individual as a politically exposed client and to see if it is reduced. Each policy and procedure of each operator should cover when and how they will check clients for the status of politically exposed persons.

The above risk analysis is a general analysis for different types or categories of clients and is the starting point for categorizing the risks of an individual client. Depending on the circumstances specific to individual clients, such as its origin and background, or what can be concluded on the basis of the information provided, it is also adapted to the categorization of the given client, to which the appropriate measures and acts of knowing and monitoring the client from the taxpayer are applied, in in accordance with Art. 7 and 8 of the Law.

The taxpayer is obliged to determine by internal act the procedure of checking whether the client or the actual owner of a client is a functionary, when establishing or during the established business relationship, in accordance with Article 38 of the Law.

*3) Risk of transaction, product and service*

In order to carry out a risk assessment, the taxpayer should describe all the transactions it carries out, the products and services it provides, and to assess the likelihood that a client will misuse them for money laundering or terrorist financing, as well as assess the impact, or the effect of such a phenomenon, through carrying out measures and actions of knowing and monitoring the client, such as:

- in the performance of a transaction of EUR 15,000 or more in dinar equivalent, regardless of whether it is one or more interconnected transactions;

- when withdrawing a win, investing a bet, or in both cases when transactions involving EUR 2,000 or more in dinar counter value are made, regardless of whether it is one or more interrelated transactions.

Transaction is the acceptance, giving, substitution, custody, disposal or other treatment of property at the taxpayer.

Assets are things, money, rights, securities, and other documents in any form that can determine ownership of property and other rights.

Money is cash (domestic and foreign), funds on accounts (dinar and foreign exchange) and electronic money.

Cash transaction is physical acceptance or giving of cash.

An alternative to the threshold approach (from 2,000 euros or 15,000 euros) is an "access approach" that is a requirement of a taxpayer to identify and verify the identity of a customer before enabling him to participate in games of chance through electronic communications. When a customer's identity is confirmed, it can start playing.

Generally, obliged entities should meet a range of regulatory requirements, commercial conditions and take security measures that can be supplemented with measures to prevent money laundering and terrorist financing, such as: client age verification, financial crime control, social responsibility provisions, security controls, game supervision (e.g that the taxpayer deals with the problem of gambling addiction, etc.).

The taxpayer must have follow-up procedures for monitoring and recording the total money paid or deposited on the account for playing through electronic communications means by each client.

The greater the risk of money laundering and terrorist financing are these transactions:

- enaled cash payment: most payments in the course of electronic communications are done directly from the accounts from financial institutions. However, the taxpayer can function as a part of a mixed organizing, which includes bookies, the so-called. ''Land Betting ''. Thus, it may be possible for the clients to cash invoice accounts at a payment site, and then use them for "on-line" games;

- transfers between parties: obliged entities may allow or be aware that customers transfer money between themselves without using their own account;

- misuse of third parties: criminals can use "third parties" or anonymous or identified gambling agents on their behalf to avoid client identity checks. "Third parties" can be used to gamble on behalf of others with a minimum amount;

- use of record accounts with obliged entities: without satisfactory internal controls, customers can use these deposit and withdrawal accounts without gambling and with minimum deposits;

- multi-user account - on-line wallet: operator/provider can own and control multiple websites. Individual websites also offer a variety of different types of gambling. Customers may separate different types of games of chance through electronic communications, carried out by the same operator/provider, or through the same website for legitimate reasons, for example, to monitor their performance in different areas. However, users may open multiple accounts or '' on-line wallets '' for unfair and inappropriate reasons, including an attempt to reduce consumption levels, or to avoid the check threshold level;

- changes in accounts of financial institutions: clients may have accounts in several financial institutions and may wish to change which of those accounts they use for online betting. This can be for legitimate reasons, or maybe the intent is to mislead the audit trail, or to introduce third-party transactions without drawing attention;

-Identity fraud: details about accounts of financial institutions can be stolen and used on websites. Stolen identities can also be successfully used to open accounts with financial institutions, and such accounts can be used on websites, through which multiple accounts can be opened for participation in games of chance through electronic communications, using stolen identities;

- prepaid cards: the use of cash to finance prepaid cards presents similar risks as with cash. Bonds can not make the same level of cross-reference checks on some types of prepaid cards, because they are able to execute transactions through the account of financial institutions;

- electronic wallet: a record account where only money is accepted through the account of financial institutions on behalf of the client usually does not present any greater or lesser risk of money laundering and terrorist financing than if the funds were received directly from a financial institution. However, when a customer makes a payment on a billing account, from the account of his financial institutions, and a statement issued by their financial institutions can only record payment from an electronic wallet, and not an online gambling transaction, that may indicate that the client wishes to conceal their payments in games of chance through means of electronic communication.

Also, games involving multiple operators/providers through electronic communications are often performed on platforms (i.e., a central computer system that connects electronic gaming devices to select games, function, supervision, security, and audit) shared by many different operators/providers through electronic communications, can be misused for the purpose of money laundering and terrorist financing. The platform is likely to play a key role in investing patterns and values of the game for potential money laundering activities (e.g chip, dumping, etc.), so without clear operator/provider policies in relation to the respective roles and actions of the client, this advantage can be lost.

The taxpayer should in particular monitor and identify suspicious transactions that are conducted in a way that avoids standard and common control methods involving multiple participants, more interconnected transactions that are performed in a shorter period or in more intervals in succession, in an amount that is just below the maximum prescribed by the law, in order to avoid filing and reporting.

The taxpayer is obliged to pay special attention to any risk of money laundering and terrorist financing that could result from the use of new technologies, the provision of new services not previously offered, as well as the provision of those services for which, on the basis of their experience, they estimate that they bear a high level of risk and take appropriate measures to prevent them from being used for the purpose of money laundering and terrorist financing.

The list of indicators for identifying suspicious transactions for organizers of specific games of chance is the starting point for employees/authorized persons in identifying suspicious circumstances related to a particular client and/or transaction performed by the client in order to use them in their work.

The taxpayer may, in addition also envisage additional risk categories and determine the appropriate actions and measures from the law for these risk categories.

**RISK ANALYSIS AND ASSESSMENT**

Risk assessment is an activity that shows the extent to which a particular risk can affect the achievement of the target.

Risk assessment is done based on probability and impact.

The probability represents the possibility that a particular event will arise, while the influence represents its effect.

In the next step, the measurement of impact and probability in the context of the question: "what is the consequence of the risk?''.

The impact and probability are measured by three categorizations: "high", "medium" and "low". Each categorization has a number, and the multiplication product with the categorization gives the degree of exposure to a particular risk.

The risk exposure is determined on the basis of a matrix that shows the relationship between the impact and probability in the 3x3 system, as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IMPACT** | high | **3** | 3 | 6 | 9 |
| medium | **2** | 2 | 4 | 6 |
| low | **1** | 1 | 2 | 3 |
|  |  |  | **1** | **2** | **3** |
|  | low | medium | high |
|  | **PROBABILITY** |

Exposure to risk is assessed as low (product is 1 or 2), medium (product is 3 or 4) and high (the product is 6 or 9).

 The taxpayer is exposed high to a certain risk, especially if it can lead to:

- interruption of all important programs, services and activities;
- loss of large financial assets;
- Serious breaches of the safety of employees and clients (endangered life);
- significant loss of public confidence, etc.,

and applies enhanced actions and measures.

 The taxpayer is subject to a medium risk exposure if it can lead to:

* interruption of some important programs, services and activities;
* loss of limited financial resources;
* breaches of the safety of employees and clients (serious injury);
* loss of public confidence to some extent, etc.,

and applies at least general actions and measures.

The taxpayer is low exposed to a certain risk if it can lead to:

- delays in small projects and provision of services;
- Loss of financial assets of low value;
- giving first aid to the injured;
- "step back" in building public confidence, etc.,

and applies at least simplified actions and measures.

 The taxpayer performs an analysis and assessment of risk exposure in relation to all recognized snd identified risk categories and places them in one of the categories listed above.

**RISK MANAGEMENT PROCESS**

**Internal policy and procedures**

The goals and principles of management of risk of money laundering and terrorist financing should enable obliged entities to determine appropriate policies and procedures, determine the role, level of authority and responsibility of the authorized persons with the taxpayer. The aim of accepting such a policy is primarily to determine at the level of the taxpayer those areas of business which, given the possibility of abuse of money laundering or financing of terrorism, are more or less critical, that is, for the taxpayer himself to establish and determine the main risks and measures for their resolving.

Management must ensure that employees respect internal procedures and established policies. It should stimulate the ethical business culture and ethical behavior of employees, to continuously strengthen the capacities, knowledge and awareness of employees about the importance of reviewing and updating risk assessment and the importance of effective risk management through the taking of adequate measures and actions for detecting and preventing money laundering and financing of terrorism.

Organizational unit managers who are responsible for risk management at the level of their unit, if the organizational structure is bigger, need to develop procedures for managing the risks of money laundering and terrorist financing, so that these procedures are tailored to the specific tasks in the organizational structure of the taxpayer and be harmonized with the procedures, objectives and principles of risk assessment of money laundering and terrorist financing at the level of obliged entities.

**Internal strategy**

 In order to carry out activities to establish the functioning and maintenance of the risk management process, the taxpayer adopts a strategy that represents a framework for identifying, assessing and controlling potential events and situations that may have a negative effect on the reputation of the taxpayer and his business. It should include the taxpayer's attitudes towards risks, set goals as well as the roles of authority and responsibility in the risk management process.

The goals of the strategy are to improve the efficiency of risk management, for the risk management to become:

- an integral part of planning documents;

- integral part of the process of planning and decision-making crucial for the realization of goals;

- to ensure that identification, assessment, treatment, monitoring and risk reporting are understandable to all employees;

- establishing coordination in risk management;
- that risk management includes all risk areas;
- ensuring that at the level of obliged entities the most significant risks are covered;
- ensuring that risk management complies with the regulations governing the prevention of money laundering and the financing of terrorism.

 The purpose of the strategy is to increase the capacity of the taxpayer to achieve the set goals at the strategic and operational level of the taxpayer using the risk management system as a tool, which also implies effective communication and learning that is implemented vertically and horizontally within the organizational structure of the taxpayer.

 Risk management with obliged entities strengthens confidence in the control system and leads to the development of a new positive management culture.

The strategy improves the efficiency of business processes, the quality of decision making and the provision of taxpayer services, improving the risk management system, which leads to an increase in the desired results, thus effectively minimizing the risk of money laundering and terrorist financing. It must contain performance indicators, as well as to be periodically updated, or revised and harmonized with standards.

**Competences, responsibilities and training**

The risk management process involves a number participants and structures and they have their roles, competencies and responsibilities. The taxpayer is obliged to appoint an authorized person and his deputy for performing certain actions and measures for prevention and detection of money laundering and financing of terrorism in accordance with Art. 49-52. of the law.

The senior management in the taxpayer determines the system for prevention and detection of money laundering and financing of terrorism, i.e internal policies and procedures, adopts internal strategy, establishes, maintains and provides conditions for carrying out activities in the risk management process and provides the highest level of support, dedication and commitment to the governance process risks.

Effective communication is carried out vertically and horizontally within the taxpayer. All employees receive from managers clear messages about the responsibility for risk management and how their individual activities are related to the work of other organizational units and employees.

Leaders of organizational units ensure that communication effectively transfers the goals, relevance and importance of effective risk management, inclination to risk and risk tolerance, as well as the roles and responsibilities of employees in the implementation of components in risk management.

The taxpayer is obliged to develop a program of regular vocational education, and training of employees for the prevention of money laundering and terrorist financing in accordance with Article 53 of the Law, as well as to provide the following:

* getting acquainted with the risk management strategy for all employees, with a constant obligation to introduce new employees;
* workshops on risk identification in the preparation of internal documents;
* workshops on risk assessment during the preparation of annual plans through the programs of work of organizational units;
* internal meetings and exchange of experiences of organizational units on risk management, etc.

**RISK SUPERVISION AND REVIEW**

**Internal control and internal audit**

The taxpayer is obliged to carry out regular internal control of the conduct of the prevention and detection of money laundering and terrorist financing. Internal control is carried out in accordance with the established risk of money laundering and terrorist financing.

The purpose of internal control is to detect and eliminate deficiencies in the implementation of the Law, as well as to improve internal systems for detecting persons and transactions suspected of money laundering or terrorist financing.

In performing the internal control, the obligor is obliged, by random sample method or in another appropriate manner, to carry out checks and tests the implementation of the system against the prevention of money laundering and financing of terrorism and the adopted procedures.

In the event of a change in the business process (e.g organizational changes, changes in business procedures), the taxpayer is obliged to check and harmonize its procedures in the internal control in order to be adequate for the fulfillment of obligations under the Law.

Checking of the harmonization of the system and procedures for the implementation of the Law and internal procedures, the taxpayer is obliged to carry out once a year, as well as every time there is a change, no later than the date of the introduction of these changes.

The taxpayer is obliged to draw up an annual report on the performed internal control and measures undertaken after that control, not later than March 15 of the current year for the previous year.

The taxpayer is obliged to organize an independent internal audit within the scope of which is a regular assessment of the adequacy, reliability and efficiency of the risk management system of money laundering and terrorist financing when the law regulating the activity of obliged entities prescribes the obligation of independent internal audit, or when the taxpayer estimates that, having in mind tha size and nature of the work, there needs to be an independent internal audit under the Law.

**Risk monitoring process and reporting**

Monitoring and reporting on the risks of money laundering and terrorist financing, as well as their management, is a continuous process. Leaders of all levels in the obliged entities, through risk analysis processes, monitor whether certain risks still exist, whether new ones have emerged, whether the impacts and probabilities of existing risks have changed, and whether the risk priority has changed.

The identifiable risks of the obliged entities are reviewed regularly, at the meetings of the high management twice a year and as necessary, after which the communication takes place with the lower managers in order to respond to the risks.

Risks at the level of organizational units are monitored permanently, and reviewed quarterly and,as necessary, by managers of organizational units.

Internal communication on risks ensures that managers and all employees with the taxpayer understand their place and responsibility in risk management.

The process of monitoring and reporting on the risks of money laundering and terrorist financing should be implemented as part of:

- business functions of the taxpayer for control of business, to ensure that all foreseen procedures are applied on a regular basis;

- regulatory compliance functions, which periodically monitors whether the internal policies identified are respected and whether all systems are in function;

- audit function, when determining whether business policies and processes are in accordance with the law and whether they are carried out in a legally prescribed manner;

- assessment of risk management resources, such as financial resources and staffing;

- determining future needs that are important for the nature, size and complexity of the taxpayer's complete business.

Regular reports to be submitted to managers should include data on the results of the risk monitoring process, internal control findings, organizational unit reports, internal audit reports, reports of persons authorized to detect, monitor and report suspicious transactions to the competent state authority, as well as the conclusions of the supervisory authorities set out in reports on the immediate inspection of obliged entities on money laundering and terrorist financing issues.

Heads of the obliged entities should also be provided with all other important information that will enable them to check the level of controls on the prevention of money laundering and terrorist financing, as well as possible consequences for the taxpayer's business if the mechanisms of control and prevention do not function adequately to the risks.

**PROTECTION AND CONSERVATION OF DATA AND KEEPING OF RECORDS**

The taxpayer is obliged to keep the data and documentation in relation to the client, the established business relationship with the client, monitoring the client and performed the risk analysis and the transaction performed, obtained in the prescribed manner, for at least ten years from the day of the termination of the business relationship, or the execution of the transaction.

The taxpayer is obliged to keep the data and documentation about the authorized person, the deputy of an authorized person, professional training of employees and performed internal controls at least five years from the day of termination of the duties of an authorized person, completed professional training or performed internal control.

The taxpayer is obliged to keep a record of the data referred to in Article 8 of the Law and submit it in accordance with Article 47 of the Law.

The taxpayer is obliged to keep a record of the data referred to in Article 98, paragraph 1 of the Law, the content of which is prescribed by the provisions of Article 99 of the Law.

The taxpayer or his employees, including members of the administrative, supervisory and other management bodies, as well as other persons to whom the data referred to in Article 99 of the Law are available, are obliged to protect them, in accordance with Art. 90 and 91 of the Law.

**MAKING A LIST OF INDICATORS**

The taxpayer is obliged to draw up a list of indicators for identifying persons and transactions for which there are grounds for suspicion that money laundering or terrorist financing is involved. During the development of the list of indicators, they are obliged to enter the indicators developed by the competent authority, which are published on the website of the Administration for the Prevention of Money Laundering.

The taxpayer is obliged to apply a list of indicators when determining the basis of suspicion of money laundering or terrorist financing, and to take into account other circumstances that indicate the existence of a suspicion of money laundering or terrorist financing. It is especially important that all employees be familiar with the indicators and trained to identify and solve the risk of money laundering of terrorism financing within the scope of their work.

**IMPLEMENTATION OF GUIDELINES**

The obliged entities are obliged to harmonize their operations with the content of the Guidelines and the drafting of an internal act, not later than April 1 2018, in accordance with the provisions of the Law on Prevention of Money Laundering and Financing of Terrorism.

DIRECTOR

Dragana Marković

 Предлог смерница израдила:

 Слађана Филиповић

Начелник Одељења за електронски надзор

 и канцеларијску контролу

 Сагласна:

 Зорица Ћетковић

 Координатор

 за област игара на срећу