THE NEED OF PUBLIC – PRIVATE PARTNERSHIP AND RISK ASSESSMENT

Associate Prof. Svetlana NIKOLOSKA PhD,
Faculty of Security, Skopje

Assistant Prof. Ivica Simonovski PhD,
Co-Founder of Cyber Security, Corporate Security and Crisis Management Initiative

доц. д-р Светлана НИКОЛСКА,
Факултет по Сигурност, Скопие

доц. д-р Ивица СИМОНОВСКИ
Съучредител на Инициатива за Кибернетична сигурност, Корпоративна сигурност и Управление на кризи

Summary: A long time, Europe is trying to find the strength to stay with the same values preserving individuals' rights and freedoms. Global concerns are put before the national. In such an environment there is no place for nationalist / populist ruling political structures.

But a wave of migrants caused by tectonic movements in the Middle East and north Africa, as well as terrorist attacks in Paris, Ankara, Istanbul and Brussels, has created Europe to live with a "new normality". That feeling of fear that terrorist attack will happen again, changed the face of Europe. In this context, the governing structures are aimed at defending national interests, disregarding the global. This situation does not correspond to policy led by the EU. In a situation where we need to be united, there is separation.

We can mention several reasons that led to it:

- The policy of integration of minorities in national societies. That policy has led these people to be excluded from the system or can not be integrated, and found solace in terrorism;
- Neglect of issues related to security challenges. Not investing in security structures.

Different perception of security challenges such as: brothers bombers from Brussels, for the US they are terrorists, for Belgium they are criminals.

The purpose of this paper will be based on analysis of the terrorist attacks in the last 15 years to determine the need to strengthen public - private partnerships, the timely exchange of information and identifying potential terrorists through profiling of high risk clients in the financial system, especially banking system.

Through this platform of cooperation we will not guarantee that every terrorist attack carried out by a wolf - a loner or a cell of a terrorist organization who decided to die blow up with home made explosives will be prevented, but it will help in early identification of suspicious activities which must not be neglected by the security services. We mention this because for the last terrorist attacks in Belgium and Paris, law enforcement agencies had information but they ignored them thinking they are frivolous.

Key words: migrants, terrorism, public-private partnership, cooperation, exchange the information.

Резюме: От дълго време Европа се опитва да намери сили да остане със същите ценности, запазвайки индивидуалните права и свободи. Общите проблеми са поставени пред националните. В подобна среда няма място за управление на националистически или популистки политически структури.

Но вълната от мигранти, предизвикана от сътресенията в Близкия Изток и Северна Африка, както и терористичните атаки в Париж, Анкара, Истанбул и Брюксел принудиха Европа да живее в "нова дествителност". Усещането на страх от нова терористична атака промени лицето на Европа. В този контекст управленските структури са призовани да защитават националните интереси, пренебрегвайки общите. Тази ситуация не отговаря на провежданата от Европейския съюз политика. Във време, когато трябва да сме обединени, има разделение.

Можем да изложим няколко причини, довели до това положение:

•Интеграционната политика за малцинствата в националните общности. Тази политика доведе до изключването на тези хора от системата и до състояние да не могат да бъдат интегрирани и да намерят утеха в тероризма;

•Пренебрегване на проблемите, свързани с предизвикателствата пред сигурността. Неинвестиране в структурите за сигурност.

Различно възприемане и окачествяване на предизвикателствата пред сигурността, като например: братята атентатори от Брюксел за САЩ са терористи, а за Белгия – криминални престъпници.

Целта на тази статия се основава на анализа на терористичните атаки през последните 15 години, за да обоснове необходимостта от засилване на публично-частното партньорство, навременния обмен на информация и идентифицирането на потенциалните терористи посредством профилиране на високорисковите клиенти на финансовата ситема, по-специално банковата система.

Ние не можем да гарантираме, че с помощта на такава платформа на сътрудничество ще се предотврати всяка терористична атака, проведена от вък-единак или клетка на терористична организация, решила да взриви домашно приготвени експлозиви, но това ще подпогне ранната идентификация на подозрителни дейности, които не трябва да се пренебрегват от службите за сигурност. Споменаваме това, защото правоприлагащите органи са имали информация за готвените терористични атаки в Белгия и Париж, но не са ѝ обърнали достатъчно внимание, смятайки я за несериозна.

Ключови думи: мигранти, тероризъм, публично-частно партньорство, сътрудничество, обмен на информация.

Introducing

In the "new normal" that Europe lives, citizens should always have been fortunate, but terrorists have need happiness once. As we said before, now is the time when we should be united and jointly fighting against the challenge called terrorism.

Terrorism and other challenges, depend on the funds. They are a key element for the maintenance and development of terrorism. Money is a prerequisite for all terrorist activity, and is often described as the "lifeblood" of the terrorist and terrorist organizations.[1] Without them, the body could not survive, and the terrorists will not be able to realize its goal.

For that reasons, disrupting the financial flows degrade the capability of terrorist groups over time, limited their ability to launch attacks, increasing their operational costs, injecting risk and uncertainty into their operations. [2]That is the key element in combating against terrorism.

Given the international nature of terrorist organizations, their network structuring and connectivity, establishment of a network of relevant institutions at national and international level which have a common interest, to speak a "common language", cooperate and exchange information in order to neutralize or minimize the risk of terrorism and its financing is crucial.

Hence, cooperation at the national level and creating a system to prevent the financing of terrorism is also crucial. Especially the building of public - private partnership where cooperation between the private sector (especially banks) and the investigating authorities should be high and always on time.

How terrorist cells in Europe financing their activities

We mentioned that the money is described as the "lifeblood" of terrorism. Without money, terrorism cannot flourish. In order to identifying the main sources of financing terrorism cells in Europe we surveyed the financing of terrorism cells that plotted the attacks in Europe last 20 years. For this purpose, we used data from court documents and media reports. This survey identifies how the terrorist cells in Europe generated income and transferred money in the periods they were planning the attacks, and the expenses that were directly attack – related.

Generally, terrorist organizations raise funds in many different ways. The most commonly income sources of funds are illegal activities, legal activities, state sponsorship and public support.[3]

[1] *Chadha Vivek, "Lifeblood of Terrorism: Countering Terrorism Finance", Bloomsbury Publishing India, 2015, p. 11-25;*

[2] *Financial Action Task Forces (FATF), "Financing of terrorism", February 2008, p. 20-30, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf ;*

[3] *Biersteker and Eckert, Countering the Financing of Terrorism, 8; Michael Freeman, "Sources of Terrorist Financing: Theory and Typologies" in Financing of Terrorism, p. 12-22.*

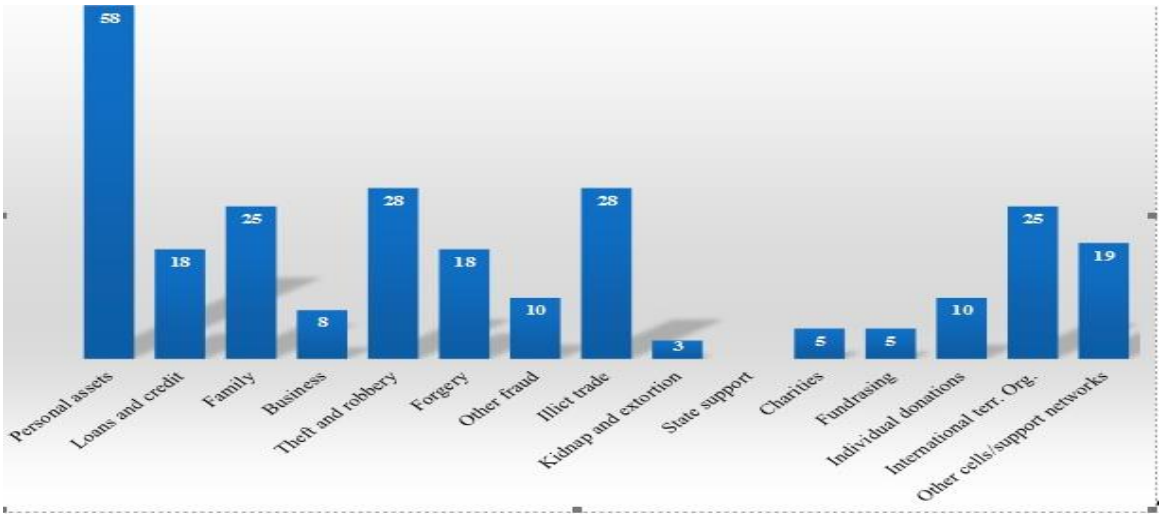

Figure 2.1. Proportion of the cells that have raised money

According to our data, approximately 57% of the cells raised money from legal activities such us: salaries, credits, loans, family support, personal assets and business. This fundraising is advantage for them because is more secure and because they do not want to attract attention. Negative side of the legal activities is that required various forms of documentation. With that, involved person reveal their identity.[4] Above proportion displays, that there is not cases in which the cells are financed by state support. This is so because the international community has mechanisms to take action against any country that sponsors terrorism. The second most used income source of funds is illegal sources such us: theft, robbery, and illicit trade. This financing type through illegal sources has several advantages. Money is collected very quickly. Crime always brings high profits. These activities allow terrorist to operate away from the eyes of law enforcement. But, on the other hand, these illegal activities entails risk especially of members who become more interested in making money than fighting for terrorism ideology.

For these reason, the focus should be on identifying the suspicious client and suspicious transactions in the financial sector (especially in the banks and fast money transfer agencies). Their task is to carry out a procedure for the identification and analysis of risk customers before they establish business relationship and during the business relationship. Based on the criteria for risk assessment, to design high-risk customers who would be subject to further analysis and monitoring.

Role of banks in system for prevention of money laundering and financing of terrorism

The main aim of money launderers is legalizing, dirty, criminal money. This most banks use the money where it entered the accounts of legal or physical persons, and then through the bank operation is transformed into other banks in the country or abroad. Usually this is done by entering the criminal money, through the transactions, it is a way of avoiding the legal obligation of reporting bank.[5]

[4] *Biersteker and Eckert, Countering the Financing of Terrorism. 9; Passas, "Terrorist Financing Mechanism and Policy Dilemmas", p. 25.*

[5] *Янев Р. ,,Противодействие на изпирането на пари, София, 2011, стр. 93.*

Banks are among the most distinguished financial institutions, entities in the system of money laundering and their role is quite important because they are part of the first pillar in a complex three-way system that already developed and provides the first results in Macedonia. The legal obligation of banks are to apply the provisions of the Law for Anti-money laundering and other proceeds from crime and financing of terrorism where the procedure provided for the detection of suspicious transactions made by banks and their obligation to inform the Financial Intelligence units.

The first pillar, or conditionally said first wall which is placed directly in front of money launderers is composed of entities - financial institutions have a legal obligation to take the following measures and actions to detect and prevent money laundering and terrorism financing:

- Client due diligence;
- Monitoring of certain transactions;
- Collecting, keeping and submitting data on transactions and clients performing them, and
- Introduction and application of programmes.

Depending on the type and activity, products offered and depending on the exposure risk for money laundering, the law imposes certain set of specific measures to be taken only certain entities including banks. The purpose of establishing an efficient system for the prevention of money laundering is conducting a proactive policy that includes measures and activities before any action happened. That means efforts to detect money laundering at an early stage, when establishing a business relationship with the client. From that point the banks have to perform simple and strengthened analysis of their clients when establishing a business relationship with its customers when carrying out one or several related transactions amounting to EUR 15,000 and when there is suspicion of money laundering, establishing and confirming the identity of customer, authorized persons and beneficial owner, as well as monitoring and analysis of transactions. If the banks for any reason are unable to take the measures listed above, are obliged to refuse the business relationship with the client which means that refusal, suspension of transactions.

Monitoring of transactions and activities is an obligation that requires special attention. This is especially true transactions realized without economic justification or purpose, unusual large transactions and for transactions where the ultimate owners are natural persons and legal persons coming from countries with inefficient legal system in which incomplete and insufficient measures and activities taken to prevent money laundering. The identification of suspicious transactions based on a list of indicators for identifying suspicious transactions that are prepared by the Office, separately for each subject, but often use their own clues and direct knowledge. These lists of indicators, the Office had submitted to each entity and is required to update annually.

If bank officials on the basis of indicators for identifying suspicious transactions or direct knowledge fix prepared and suspicious transaction reports submitted to a suspicious transaction to the Department of SPPFT and the same should be subject to further analysis. Also, banks are obliged to temporarily retain the transaction whenever you receive an order by the Office. This period lasts 72 hours, or until a decision by the competent court.

In terms of care and direction of strengthening the overall system to prevent money laundering, banks must not enter into business relationships with shell banks (Shell Bank). Also, based on international regulations and based on global experiences of detected cases of money laundering, banks are not allowed to open anonymous accounts are identified by number or no account information for the end user.

The need for risk assessment

"If you don't know where you are going any road will take you there." ***(****James Howcroft, George C. Marshall European Center for Security Studies, Director of Program on Terrorism and Security Studies****)***

The strategy is a plan that should answer the following questions:

- What do you do ... (Object);
- How to do ... (Methods);
- What.... (Resources)

The determination of threat is a driver in the creation of a specific strategy that will allow balancing the available tools and resources and allocating them in order to minimizing risk.

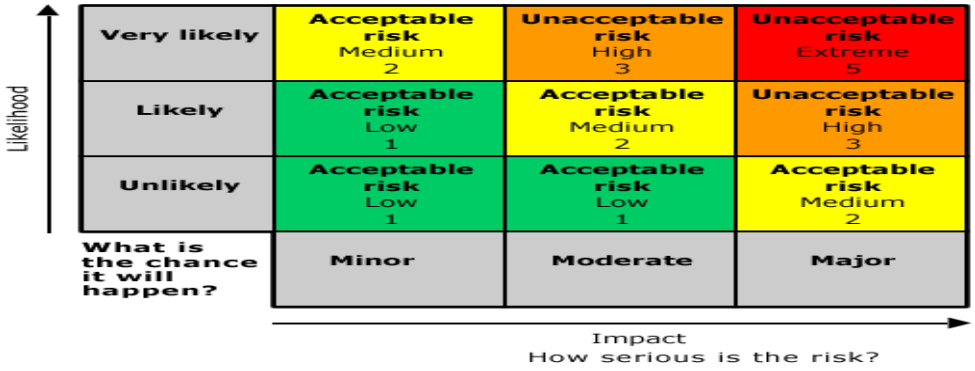

Figure 4: Security risk assessment

Profiling the high-risk customers is essential for the financial situation, in this case the bank in order to determine the potential risk of establishing a business relationship with them. In terms of competitive race in gaining customers, and more profits for the bank the question is whether the bank has an interest to establish business relationship with customers who are potentially risky customers? The answer depends on internal business policy of the bank. How the bank is ready to carry the burden called "risk client" on his shoulders, while consciously or unconsciously threatening reputational risk and security risk in the country. As an illustration, if the bank established business relationship with a customer who is on sanction list, the consequences will be borne by the bank and the state at international level because it has not taken appropriate measures to prevent it and to guarantee its own security. The main goal in this article is to perform profiling high risk profiles who wish to establish business relationship with the bank; or Profiling of high-risk profiles that have already established business relationship with the bank and in accordance with the objectives of the

strategy and aimed at minimizing risk, it is necessary to carry out their detection, determination of risk (rating), paying attention and monitoring.[6]

Know your customer procedure – KYC standards

As I mentioned before, the main objective of KYC Procedure is to prevent banks or other financial institutions from being used, intentionally or unintentionally, consciously or unconsciously for money laundering or financing of terrorism activities. This procedure will enable banks to know their customers, to know and better understanding their financial dealings. From other side, KYC procedure will help them to manage their risk prudently. An institution's AML program may have a very rigorous and robust KYC program, complete with stringent account opening procedures; however, if this data is not readily available, then banks can face the prospect of limited risk factors for consideration in their risk modeling.[7]

The KYC program should define the strict criteria, which will be implemented in the process during the establishment of the relationship between the client and the bank. The Customer Acceptance Policy indicated the criteria for acceptance of customers shall be followed by all banks, and the banks shall accept customer strictly in accordance with that policy. The banks *would not be allowed* to establish a business relationship in the following cases:

- In cases in which the entity wants to open an anonymous account or used fictitious name(s);
- In cases in which the entity is a famous perpetrator of crimes or having connections with the criminal organization (s), want to establish business relationship with the bank;
- In cases in which the entity is a terrorist or having connections with terrorist organizations;
- In cases where the entity coming from country where operating criminal or terrorist organizations;
- In cases where entity based in high risk countries/jurisdictions or locations;
- Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;
- In cases where entity is listed in sanctioned list issued by United Nation Sanction Committee, European Union, Interpol and other similar international organizations;
- In case of Non face-to-face customers;
- In all cases when the client due diligence measures cannot be implemented by the bank, the bank shall be obliged to reject to establish business relationship.[8]

In order to generate a risk, banks may include additional factors through which they would do an assessment. That factor included:

- The transparency of company structures and beneficial owners;
- Political connections of the customer or associated individuals;

---

[6] *Banks' management of high money – laundering risk situations How banks deal with high-risk customers (including politivally exposed persons), corespodent banking relationships and wire transfers, Financial Services Authority, June 2011;*

[7] *Customer due diligence for banks, Basel Committee on Banking Supervision, Oktober 2011.*

[8] *FATF (2008), "Financing of Terrorism" FATF+GAFI, Paris, www.fatf-gafi.org;*

- The customer's reputation and/or known adverse information about the customer;
- The source, structure and adequacy of information about the customer's wealth;
- The source of the customer's funds;
- Expected activity on the account (types of transaction, volumes, amounts, the use of cash);
- The customer's profession/industry sector; and
- Involvement of natural or legal entity in public contracts.

The branches shall make necessary checks before opening a new account so as to ensure that the identity of the entity (Potential client) does not match with any of abovementioned criteria. In cases when the entity is match with any of abovementioned strong criteria, the banks would not be allowed to establish a business relationship with the natural and legal person. Thus, the banks primarily protect its own reputation and are not included in any risk and protection form possible abuse for the purpose of money laundering and financing of terrorism.

Creating the high risk profile before the establishing business relationship

For the purpose of his research, we will present one different procedure for profiling the high-risk customers. There are two possible methods how the banks can create high-risk profile of his clients. The first method is creating the high-risk profile of person before the establishing the business relationship and included the following basic criteria:

- Gender;
- Age;
- Social status (data based from application);
- Economic status (data based form transaction analyses);
- Psychological profile (monitoring the activities of the client by the bank officer);
- Criminal past (based on online data and public information);
- Politically exposed persons (PEPs);
- Nature and intended purpose of the business relationship;
- Resident or nonresident;
- Environmental;
- High risk countries;
- Sanction lists or black list and
- Terrorist organizations.

Based on the above criteria, the bank officials should be observed and prepare an initial profile of their clients in order to identify whether it is a risky customer or not. Each of these criteria is linked to each other and each criterion answers the specific question that banking officer sets when profiling.

The determination of sex and age answers the question whether the client belongs to a certain vulnerable group which according to these two criteria are suspicions and that may be involved in suspicious activities related with money laundering and especially financing of terrorism.

Then, based on the information stated in the application for establishing a business relationship determines whether the status of the person, whether it is employee, whether he is

on welfare, pension, etc.. These data are compared with data obtained from the analysis of the economic power of the client, ie the dynamics and value of funds that have entered or are paid from the client's account.

Then compare the regions or branches in which the client performs banking services, ie entry and payment of funds.This information is important in order to determine whether the customer often changes various branches of the bank in order not to leave suspiciousness in some bank officer or a customer intends to perform banking services with just one bank officer then determines whether the bank branches where performed services are located in areas that are suspected to have the presence of supporters of terrorist organizations or radicalism and extremism. Using publicly available information through the media and Internet have to determine whether the client behind a criminal record and history in order to see what is his profile. Based on a psychological profile, banking officer should determine whether the client during his visit to the bank performs dubious activities, his physical appearance, nervous, scared, whether it comes in the presence of other people etc. And finally determines whether the customer is a politically exposed person (MP, Director, Minister, President etc..), whether a resident or coming from another country, which is high-risk country, i.e. a state that does not implement standards on the legal framework for prevention of money laundering and financing terrorism, or state in which there are terrorist organizations, terrorist organizations and sponsors etc.

In order to have a complete picture of your customer, the bank should provide information on the nature and intend purpose of the business relationship and means measures to establish the customer’s occupation and source of funds. This kind of information is crucial to provides banks with a solid basis for monitoring the business relationship and opportunity to assess whether the proposed business relationship is in line with the bank would expect.

Before, we mentioned that the banks *would not be allowed* to establish a business relationship in cases where entity is listed in sanctioned list issued by United Nation Sanction Committee, European Union, Interpol and other similar international organizations, or other internal “black” list issued by the bank or other institutions. In certain cases, may occur, the client who wants to establish a business relationship with the bank is not on a sanction list, but during the realization of business relationship to be put on a sanction list. In this case, the bank shall immediately freeze the accounts of the customer to terminate the business relationship or to set up monitoring, qualifying it as a high-risk client.

Above we mentioned that as a separate category for risk assessment is determined the geographical risk, i.e. risk from country of origin. This kind of information is important to provide banks with a solid basis with the residence country for natural person and the country in which is the legal entity’s seat. Also very important for the bank when analyzing the client to determine whether the customer realizes business activities with legal or natural persons from countries that are characterized as high-risk.

Each of these data are scoring (Scoring), and client rank and determine whether to proceed with further analysis.

If bank officials determine that it is a high-risk client access to further deeper analysis of its banking transactions, to determine whether there are suspicious transactions and to execute them scoring.

Figure 5.1. Example of scoring based on different criteria

No	Typology or criteria	Number of points (1-10)
1	Gender	5
2	Age	7
3	Social Status	6
4	Economic Profile	3
5	Psychological Profile	8
6	Criminal Evidence	8
7	PEP-Political Exposes Persons	1
8	Resident/Nonresident	6
9	Environment	8
10	Risk Country	5
11	Sanctions/Black Lists	5
12	Links with Terrorist organizations	5
	Total	67

Based on the scores and the degree of risk, the bank decides whether to establish a business relationship with a client or not.

Profiling of high risk profiles of clients in order to prevent money laundering and terrorism

The procedure of profiling high-risk profiles of clients is different from procedure of "The Customer Acceptance Policy". The reason is very simple. This procedure covers profiling of customers who have already established business relationship with the bank and who previously have passed through the filter of the strict criteria used in the process of establishing business relationship. This procedure will allow the bank to use the available tools and resources in order to determine the risk of risky customers, categorizing them into certain levels, such as low, medium and high, or they can be more elaborate, such as low, medium, medium - high, high and very high, with the ultimate aim to minimize and manage the risk. [9]

As I mentioned before, there is no business in the financial sector, which is immune from the activities with criminal elements. The level of Money Laundering and Financing of Terrorism Risk to the customer shall be assigned on the following basis: [10]

Low Risk Level:

Low-level risk, banks can determine in cases in which the identity and sources of wealth of the individuals and entities can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. Additional criteria for low risk customers could be employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover. Also customers who receive salary from Government Departments and Government owned companies, regulators and statutory bodies etc., can be designated as low

[9] *METAVANTE WHITE PAPER - Customer Risk Assessment, Metavante – Risk and compliance Solutions, 2008.*
[10] *THE BANKING SECTOR – Guidance for a risk – based approach, FINANCIAL ACTION TASK FORCE (FATF), Oktober 2014;*

risk. Depend case by case, only the basic requirements of verifying the identity and location of the customer shall be met. [11]

Medium Risk Level

Bank can categorize customers as medium or high risk according to their origin, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

- Customers in business or trading activity (including export/import, reexport) which live or place of business has a scope or history of unlawful trading and business activity;
- In cases in which the bank estimated that, the profile of the customer when opening the account is uncertain and doubtful.

High Risk Level

High-risk client's bank may categorize on the basis of strict criteria (some of them mentioned in the above text) and based on the products and services used by customers. As most used criteria for risk assessment for money, laundering and financing terrorism are:

- risk from the country of origin;
- risk from a profile of a client and
- risk of a product or service.[12]

Risk from country of origin

As a separate category for risk assessment is determined the geographical risk, i.e. risk from country of origin.

The evaluation of the risk from country of origin is performed according to the following:

- *For natural persons:* the residence country and
- *For legal entities:* the country in which is the legal entity's seat.

Countries with high risk, from money laundering and financing terrorism point of view, are those countries with high corruption index, unsecure economical and political systems, inefficient legal system or small number of requirements for the documentation needed for opening businesses, countries known for production, processing and trafficking drugs and weapons.

As additional factors that would influence the decision whether some country represents a risk, could be:

- States under sanctions, embargos or similar measures, issued, for example, from the United Nations;
- States identified, by credibility sources[13], as states having incompatible regulation for prevention of money laundering and financing terrorism with the international regulation from this area;

---

[11] *http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate);*

[12] *https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_013.htm.*

[13] *"Credibility sources" are the World Bank, the International Monetary Fund, the Organization for Economic Cooperation and Development, FATF and the EGMONT Group of FIU's, as well as important national governmental and nongovernmental organizations;*

•States identified, by credibility sources, as states financing and supporting terrorism.[14]

Risk from profile of a client

Clients with high risk, from money laundering and financing terrorism point of view, are clients whose activities can cause higher risk i.e. within which can be encountered one or more of the following criteria:

•significant and unexplainable geographic distance between the entity who should perform the activity and the place of residence or the seat of the client;

•frequent and unexplainable movements of assets between accounts in various financial institutions;

•frequent and unexplainable cash flows between financial institutions in different geographic areas;

•clients for which is difficult to identify the real owner (off-shore companies);

•cash activities that include or originate from:

-activities that offer money services (remittances, exchange of foreign-exchangeable operations, services for fast money transfer, as well as other activities offering money transfer);

-casinos, betting shops and other activities related to the games of chance;

-activities which in regular business operations are not in cash, and which generate large amounts of cash for certain transactions;

-charity organizations and other "non-profit" organizations which are not subject of a control (especially the ones acting across borders);

-bank accounts of accountants, lawyers or other professionals who act in the name of their clients, who by the financial institutions are treated as VIP clients;

•clients using non-resident accounts, especially as an opportunity for assets transfer across borders;

•using mediators within the business relationship which are not subject to the regulation for prevention of money laundering and financing terrorism and is not supervised;

•using corporate mediators or other structures in order to unnecessarily increase the complexity and decrease the transparency;

•clients who are politically exposed, and others.

Risk from products/services

The overall risk assessment should also contain assessment performed according to the third category of risk, i.e. according to the risks of money laundering and financing terrorism, which can appear in using certain products or services offered by the entities. From this point of view, the entities should take into account, both, the new products and the services, not directly offered by them, because they play the role as mediators, i.e. their services are used to deliver the product.[15]

While determining the risks of money laundering and financing terrorism by products and services categorized according to riskiness, we should take into account the following

[14] *http://www.int-comp.org/careers/a-career-in-aml/what-is-cdd/.*
[15] *http://www.syndicatebank.com/downloads/Banks-Policy-on-KYC-and-AML.pdf.*

factors:

- *Products with low risk,* from money laundering and financing terrorism point of view, are: products that the bank makes them easy available, i.e. in the cases of financing, loans or mortgages with long lasting business relationship between the bank and the client;
- *Products with high risk,* from money laundering and financing terrorism point of view, are the ones that include high level of anonymity or are referring to cash transactions. Services and products which can be categorized as potentially risky, associated with money laundering or financing terrorism, are:

-international correspondent banking services which include transactions, i.e. commercial payments for persons who are not clients of the bank-mediator;

-services including transactions' realizations through use of non-resident accounts;

-private banking services;

-services including or enabling cash usage;

-services related to trading with precious and noble metals;

-services related to the new technologies or developing technologies preferring client's anonymity, for example, electronic banking etc.

The entities who after the performed risk assessment have determined high risk, should implement appropriate measures and control in order to reduce the potential risk. Parts of the measures that can be undertaken by the entities are following:

- increasing the awareness for their own high risk clients and transactions;
- reinforcement of the measures for knowing the client and reinforced analysis of the client (CDD);
- increasing the requirements for account approval and establishing business relationship with the client;
- increased monitoring and analysing of the transactions;
- increased level of continuous control of the business relationship with the client;
- and other.

Conclusion

There is no single profile!

We start with the above mentioned conclusion, because each case is separate and apart from the previous or next one. Determining the criteria for risk profiling of customers is very important. Profiling of risky customers is the starting point for identifying suspicious customers or suspicious transactions. The refusal of establishing a business relationship with high-risk customers' financial institutions protects its reputation in order not to be involved in criminal networks. Also, the identification of high-risk customers within the business relationship will help the bank to allocate its resources to the rightful place.

Cooperation between the private and the public sector must be high. Always on time! Why? - Because financial institutions are the first wall that terrorists should be skipped in the process of transferring money from the source to the end user, without causing suspiciousness. In this case, the bank officers must be properly trained in process of detecting and identifying suspicious customers and suspicious transactions. Also, the financial

institutions need to constantly invest in their IT capabilities that will enable easy searching and detecting of the suspicious customers and transactions.

References:

1. *Banks' management of high money – laundering risk situations How banks deal with high-risk customers (including politically exposed persons), correspondent banking relationships and wire transfers, Financial Services Authority, June 2011;*
2. *Biersteker and Eckert, Countering the Financing of Terrorism, 8; Michael Freeman, "Sources of Terrorist Financing: Theory and Typologies" in Financing of Terrorism.*
3. *Biersteker and Eckert, Countering the Financing of Terrorism. 9; Passas, "Terrorist Financing Mechanism and Policy Dilemmas".*
4. *Chadha Vivek, "Lifeblood of Terrorism: Countering Terrorism Finance", Bloomsbury Publishing India, 2015.*
5. *Customer due diligence for banks, Basel Committee on Banking Supervision, October 2011.*
6. *Financial Action Task Forces (FATF), "Financing of terrorism", February 2008. http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf*
7. *FATF (2008), "Financing of Terrorism" FATF+GAFI, Paris, www.fatf-gafi.org;*
8. *Яанев Р. ,,Противодействие на изпирането на пари, София, 2011.*
9. *METAVANTE WHITE PAPER - Customer Risk Assessment, Metavante – Risk and compliance Solutions, 2008.*
10. *THE BANKING SECTOR – Guidance for a risk – based approach, FINANCIAL ACTION TASK FORCE (FATF), Oktober 2014;*
11. *http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate);*
12. *https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_013.htm.*
13. *http://www.int-comp.org/careers/a-career-in-aml/what-is-cdd/.*
14. *http://www.syndicatebank.com/downloads/Banks-Policy-on-KYC-and-AML.pdf.*